A PHENOMENOLOGICAL STUDY OF INFORMATION SECURITY INCIDENTS EXPERIENCED BY INFORMATION SECURITY PROFESSIONALS PROVIDING CORPORATE INFORMATION SECURITY INCIDENT MANAGEMENT

by

Randy L. Burkhead

BERNARD J. SHARUM, PhD, Faculty Mentor and Chair

STEVEN A. BROWN, PhD, Committee Member

SHARON L. GAGNON, PhD, Committee Member

Sue Talley, EdD, Dean, School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

October 2014

Abstract

The security of digital information is paramount to the success of private organizations. Violating that security is a multi-billion-dollar criminal business and exploiting these vulnerabilities creates a single point of failure for operations. Thus, understanding the detection, identification, and response to information security incidents is critical to protecting all levels of infrastructure. The lived experiences of current professionals indicate 10 unique themes in regards to how information security incidents are addressed in private organizations. These unique themes led the researcher to offer several conclusions related to the importance of planning, communication, offensive capabilities, and integration with third-party organizations. Information security incident management is accomplished as an escalation process with multiple decision points leading to a restoration of services or security. The source of the incident is not often sought beyond the first external IP address but their purpose and intent are essential to information security incident management. The key lessons learned from professionals include the importance of having a plan, training the plan, and incorporating the human elements of security into information security incident response. Penetration testing as well a knowledge about threat and attack patterns are important to information security incident management for detection, containment, and remediation. External organizations play a major role in the management of information security incidents as fear, incompetence, and jurisdictional issues keep the private sector from working with government, military, and law enforcement organizations. These themes have wide reaching implications for practical application and future research projects.

Dedication

This work is dedicated to George, Katherine, Ranger Bob, and Patrick. I dream twice as big for those who did not have the chance at full lives. I also dedicate this work to my dog Faith the Vampire Slayer as she was my constant companion throughout my PhD journey during long nights and busy weekends. She never wavered in her support and was there to remind me that sometimes I needed to take her outside for a bit of fun.

Acknowledgments

I would like to thank my mentor and committee for their support and contributions to this project. Their guidance helped me to complete a work that few have the strength, will, and determination to achieve. I would also like to thank my participants. Without their support this project would not have been possible. Keep up the fight.

Table of Contents

List of Tables

CHAPTER 1. INTRODUCTION

Introduction to the Problem

Information technology (IT) has grown over the last century from room-sized military computers to pocket-sized civilian companions. IT has become incorporated into nearly all aspects of modern life from entertainment to life sustainment. However, certain threats, including warfare and crime, have risen to take advantage of these connections. Targeted malicious cyber attacks have risen 42% between 2011 and 2012 with an average of 116 targeted attacks per day (Stegmaier & Bartnick, 2013). These attacks were conducted for various purposes causing information security incidents in a variety of organizations. This presents a unique set of challenges for corporate organizations. Verizon (2012) reported that 55% of attackers in recorded incidents against organizations were organized crime groups and 21% were state affiliated in 2012. The impacts of war and crime are not restricted to military and law enforcement agencies. Private organizations are often the target of malicious cyber attacks including digital acts of war and crime (Etzioni, 2011). These statistics indicate a highly aggressive threat to the assets of private organizations. These threats are addressed by information security professionals.

Information security has developed over time to address these various threats. Information security is the identification of technology assets and targets, the processes of defending or attacking those technology assets and targets, and the social constructs influencing attackers and defenders (Pieters, 2011; Thomas & Dhillon, 2012; Vorobiev & Bekmamedova, 2010; Vuorinen & Tetri, 2012). The study of information security addresses both sides of the conflict: defense and attack. Organizations respond to information security attacks using defensive measures. Information security incident management is a set of defensive measures for identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents (Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Werlinger, Muldner, Hawkey, & Beznosov, 2010). The management of information security incidents helps organizations to minimize the damages caused by attackers. Information security incident management is a unique marriage of the elements of offensive information security and defense strategy.

However, the elements of offensive information security are not well established. Attacks may be conducted as part of military operations. IT has built upon the foundation of modern war theory through the application of automated and semi-automated technologies in network-centric warfare (Taddeo, 2012). This has revolutionized modern warfare but very little has been published about the methods and merits of these types of attacks and even less is understood about their defense. Recent publications in this field indicate a disagreement regarding the nature and potential of the military application of IT (Lobel, 2012; Rid, 2011). This split in existing literature is just one indication of the many gaps in the literature regarding information security incidents. Attacks may also be conducted as part of criminal operations. Criminal enterprises use technology for criminal activities due to the high potential for profit with minimal risk of prosecution and punishment (Guitton, 2012). This has been a highly effective partnership for criminal enterprises. However, technology changes at a fast pace making it difficult for law enforcement, lawmakers, and researchers to keep pace with criminal enterprises. This is yet another gap in the literature on elements of information security incidents. Therefore, because the identification of these offensive elements indicating who, what, and why an attack takes place is incomplete, it is difficult to establish an existing framework for information security incident management in order to defend against these attacks.

Although there were previous studies on corporate information security management in corporate organizations they were largely fragmented. This is of particular interest to the researcher as an information security professional with experience in information security incident management. The extremely high and growing volume of information security incidents must be addressed by scholar-practitioners in order to discover the nature of the phenomenon and stem the tide of this increasing dilemma. There is a lack of empirical research demonstrating holistic organizational response to information security incidents (Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Werlinger et al., 2010). Because of the fragmented nature of the literature, there is value in hearing from individuals about their experiences with information security incident management. This research will add to the body of knowledge regarding elements of information security incidents through the exploration of this gap. Therefore, it is essential that the experiences of corporate IT security professionals be understood in order to improve information security incident management. This understanding will contribute to ongoing research in information security by expanding upon the known and recently discovered aspects of information security incidents.

Background of the Study

Due to the lack of research in information security incident response methods and the fast pace of change in the field of information security it is difficult to identify any seminal reference materials for this topic. Many reference materials published more than five years ago are of little use in evaluating today's information security environment. Unlike IT, which despite improvements is still based on concepts established long ago, information security is dynamic and fluid. New risks, threats, and vulnerabilities are discovered every year (Symantec, 2013; Verizon, 2012, 2013). This information is often reported through industry reports rather than academic research. There are many practical guides to information security but no work is central to the concept of information security incident management.

Information security incidents come in many forms including cyber attacks that are performed for war or criminal purposes. Lin, Allhoff, and Rowe (2012) noted that “cyber weapons could be used to attack anonymously at a distance while still causing much mayhem on targets ranging from banks to media to military organizations” (p. 24). While many government and military systems are protected by advanced security systems and personnel trained in cyber warfare, civilian organizations such as utilities, banks, and hospitals are vulnerable. These organizations all have minimum standards to meet to uphold national regulations and industry best practices, but they are not equipped to address acts of war.

Cyber warfare is not a theoretical concept. Israel has been fighting a protracted insurgency in south Lebanon against Hezbollah for over half a century. Muhammad al-Masri, as cited in Al-Rizzo (2008), defined the Hezbollah cyber strategy: “It is no longer necessary to have rockets to destroy an electrical facility. Instead, penetrating the enemy’s networks and planting your code will get a better result and avoid human losses” (p. 393). This is just one of many cyber war doctrines. China has also developed a cyber war doctrine. Stapleton and Woodcock (2011) described the goal of the Chinese doctrine as “to dispirit an adversary’s civilian population reduce their productivity and cause them (the population) to withdraw economic, and eventually moral, support from their county’s engagement in the conflict” (p. 53). This philosophy focuses on the effective use of cyberspace as a psychological weapon to destroy a nation's will to fight instead of the nation's military might.

Information security incidents also come in the form of criminal activities directed against an organization's assets. There are many potential criminal actions that can be performed with the assistance of IT or that can be directed against IT (Brenner, 2004). As potential victims of cyber crime, corporate organizations have a moral responsibility to protect their assets from criminal activities. These types of information security incidents occur frequently in today's world. Annual industry reports clearly note the rising rates of information security incidents attributed to cyber crime (Filshtinskiy, 2013; Symantec, 2013; Verizon, 2012, 2013). The damages caused by successful cyber crime are incalculable. Criminal actions are just one of many potential purposes behind information security incidents.

While cyber war and cyber crime are both high-risk types of information security incidents that may lead to devastating consequences, there are other reasons why information security incidents occur in organizations. An accidental attacker may not even be aware of the damage he or she is doing (Hua & Bapna, 2013). However, many attackers are blatantly malicious. Protecting against internal threats is one of the more challenging aspects of information security. However, not all attacks against systems can be bad. Incorporating information security tests, such as penetration testing, into information security management programs is a good practice (Geers, 2010). All of these information security incidents, cyber war and cyber crime as well as accidental and purposeful, are occurring in today's world. Although information security incidents are at least partly explored in the literature these studies were fragmented and incomplete. A logical precondition to examining the relationship between these variables related to information security incident management is a richer and more robust understanding of the lived experiences of information security professionals who have responded to such incidents.

Statement of the Problem

Although there are articles regarding various elements of information security, there is a gap regarding holistic response frameworks for information security incidents. The literature related to information security incident management in corporate organizations is fragmented and there is a lack of empirical research demonstrating holistic organizational response to information security incidents (Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Werlinger et al., 2010). Current research in this field is often limited to preventive information security measures rather than defensive measures for holistic incident management. These limited scopes leave many unanswered questions that only the IT security professionals making decisions could answer. Information security professional responses to information security incidents in private organizations are not fully known. Therefore, the research problem of this study focused on the lived experiences of information security professionals who have responded to information security incidents in private organizations.

Purpose of the Study

These information security incidents are likely to develop as a result of targeted actions against sensitive resources. Symantec estimated that over $110 billion a year is lost to malicious cyber actions (Filshtinskiy, 2013). This number is only expected to grow. In addition to these types of monetary losses, there is an increasing culture of fear that military applications of technology could have a profound impact on modern life in the event of a military conflict

(Butts, Rice, & Shenoi, 2012). As technology continues to grow and become integrated into modern life the threat from information security incidents becomes increasingly dire. Organizations can benefit from a better understanding of the experience of identifying and responding to these information security incidents as a means for supporting future professionals.

The purpose of this phenomenological study was to understand the experiences of corporate-based IT security professionals providing information security incident management services and to use those experiences to contribute to the body of scientific knowledge in the science in warfare, criminology, and IT. Phenomenological analysis was used to answer the research question using semi-structured interviews to identify the lived experience of information security professionals. The participants in this study were encouraged to share the meanings they derived from their experiences managing information security incidents and how these experiences shaped current response procedures for information security incident management. The meanings shared by the participants provided insights into the influence these incidents had on information security professionals and what they gained from their experiences. The results of this study contribute to the scientific knowledge of this phenomenon and provide future researchers with points of departure for future explorations into issues directly related to information security incidents. The essences of these experiences discovered in this study may serve as a springboard for additional research.

Rationale

There is a significant gap in the literature related to information security incident management for corporate organizations. Authors such as Filshtinskiy (2013) have specifically identified a need to explore these elements. Corporate professionals face unique dilemmas and little is understood about the conflicts they face and their processes for resolving these conflicts. Recent literature has contributed to the field in a variety of ways, but the primary focus has been on military and law enforcement organizations using defensive measures (Denning & Denning, 2010). A phenomenological study was appropriate in order to address this gap. Phenomenological methods enabled the researcher to explore the experiences of information security professionals as a means of gaining a deeper understanding of these unique issues. This approach allowed the topic to be explored openly.

Research Questions

The research into information security indicated that there is a gap in the literature. While there is a body of literature that addresses the management of information security incidents the literature is fragmented. This gap in the literature indicated a lack of knowledge about the practical application of information security elements and technology decision making. Therefore, the main research question explored in this study was:

RQ1: What are the lived experiences of information security professionals in private organizations responding to information security incidents?

The research subquestions are as follows:

RQ1a. How does the identification of the source, purpose, and intent during an information security incident influence the responses of information security professionals?

RQ1b. How do information security incidents influence information security professionals preparing for future challenges?

RQ1c. In what way(s) do information security incidents influence the thinking of information security professionals with regard to information security attack frameworks?

RQ1d. How do external information security programs impact the response of information security professionals in private organizations with regard to information security incidents?

Significance of the Study

While there is some fragmented literature addressing components of incident management for law enforcement and military organizations, there is a paucity of research addressing the management of information security incidents in private organizations from the experiences of corporate IT security professionals. The literature that does address information security incident management is typically focused on law enforcement and military solutions rather than holistic responses by private organizations (Lobel, 2012). Corporate responses to information security incidents from a holistic perspective are poorly represented in the literature. The researcher attempted to address that gap in the current literature. Just as qualitative and quantitative explorations have shed light on various elements of information security, the results of this study aimed to answer a specific question. Answering this question was only one part of a much larger puzzle. Constructing a rich description of this particular phenomenon is valuable to this field.

The practical implications of this study are potentially broad. By contributing to the research on information security incident management this dissertation may provide security experts with some insight into the nature of information security incidents. This insight may lead to improving reactions to information security incidents in private organizations. Contributions to this research topic may also provide law enforcement officials and military strategists with insight into the needs of private organizations in the defense of their networks. This insight may inform the development of support for IT security professionals in corporate organizations during national policy planning. Therefore, understating the lived experiences of information security professionals responding to information security incidents is relevant for information security management, technology management, business continuity, military organizations, and law enforcement.

Definition of Terms

Asset: There are many different targets that attackers may select during an information security incident. An asset can be a technology system or application, digital information, or the people associated with these elements (Pieters, 2011; Vuorinen & Tetri, 2012). All of these assets can be targeted and should be protected from attack.

Cyber crime: Cyber crime is one potential classification of an information security incident. An information security incident is termed cyber crime when it is a combination of illegal actions such as those defined in Section 18 of the United States Code, part 1030, but the effects are less than the threshold of cyber war (Brenner, 2004). This definition encompasses a wide range of potential information security incidents.

Cyber war: Cyber warfare is another potential classification of an information security incident. An information security incident is termed cyber warfare if “the reasonably foreseeable consequences resemble the consequences of a conventional attack” (Gervais, 2012, p. 539). This principle of equivalency addresses the threshold of armed attack per Article 51 of the United Nations Charter regarding the right to self-defense.

Defensive information security: Defending information security covers a wide area of preventive and reactive tasks that contribute to the security of information. Defensive information security consists of the preventive management of risk as well as the reactive management of information security incidents (Fenz, Ekelhart, & Neubauer, 2011; Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Schuesster, 2013; Tohidi, 2011; Werlinger et al., 2010). These defensive categorizations of processes and procedures each cover a wide variety of tasks directly related to the security of information.

Information security: The larger field of information security contains many important elements that influence information security incident management. Information security is the identification of technology assets and targets, the processes of defending or attacking those technology assets and targets, and the social constructs influencing attackers and defenders (Pieters, 2011; Thomas & Dhillon, 2012; Vorobiev & Bekmamedova, 2010; Vuorinen & Tetri, 2012). These elements inform all aspects of information security as a common ontological framework.

Information security incident: Information security incidents come in many forms. An incident, an event that adversely affects technology systems or services, must relate to the elements of information security, including the identification of assets, processes for attack and defense, and human attackers and defenders, in order to be considered an information security incident (Ayyagari, 2012; Drtil, 2013). Incidents that meet these criteria can be termed information security incidents.

Information security incident management: The management of these incidents is the primary phenomenon under investigation. Information security incident management is identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents (Kadlec & Shropshire, 2010;

Rajakumar & Shanthi, 2014; Werlinger et al., 2010). The management of these incidents occurs at the intersection of offensive and defensive information security concepts.

Offensive information security: Offensive information security is just as broad as defensive information security. Offensive information security is the identification of targets, the processes of attacking those targets, and the social constructs influencing attackers (Bowles, 2012; Chan, Hyung, & Hoon, 2013; Geers, 2010). These elements are not well established but have an impact on information security incident management.

Perception: Perception and identification are important concepts in the decision-making process for information security incident management. Heuer (1999) described a process of intelligence analysis in which the analyst, through self-awareness, removes his or her worldviews and biases from the assessment of situations. The perception and identification of information security incidents leads to subsequent actions. The perception and identification of events is a central concept of this inquiry.

Risk management: Risk management covers the implementation of information security in practice. Risk management is how information security is performed in modern organizations through the analysis and evaluation of vulnerabilities against threats to determine risk and the mitigation of that risk based on organizational priorities (Fenz et al., 2011; Schuesster, 2013; Tohidi, 2011). This is primarily a preventive framework designed to prevent information security incidents from occurring in secure networks.

Source and intent: Identifying the source and intent of an information security incident may provide valuable information for the management of the information security incident. The source and intent of an information security incident is any combination of internal or external actors with purposeful or accidental intentions be they malicious or benign (Halfond, Choudhary,

& Orso, 2011; Hua & Bapna, 2013). This identification provides a high-level indication of the attacker’s source and intentions.

Assumptions and Limitations

The methodology of this phenomenological study was subjective in that the information obtained was provided through semi-structured interviews with information security professionals. As with any qualitative study there were limitations and assumptions that directly affected the study. These assumptions and limitations were mitigated in order to increase the validity of the study and prevent undue bias on the part of the researcher.

Assumptions

This research study proceeded on the basis of the following research assumptions. First, it was assumed that any commitment to a theoretical perspective would violate part of the phenomenological approach. Phenomenology is unique in that committing to a theoretical construct prior to the study would violate part of the phenomenological method (Van Manen, 2014). Therefore the researcher strived not to use theoretical assumptions when considering the data in this study. The researcher’s expectations were set aside in a process commonly known as the epoche as recommended by Van Manen. By acknowledging these preconceived expectations, this researcher was able to consciously set aside these expectations during data collection and analysis. Second, it was assumed that corporate IT security professionals providing information security services face information security incidents and that these experiences are different than those experienced by individuals serving in the military or in law enforcement. This difference is attributed to the difference in resources, organizational culture, organizational mission, and organizational purpose, as demonstrated in existing literature. Third, it is assumed that participants spoke openly and honestly. In order to ensure that information was protected mechanisms to ensure the confidentiality of information were in place to protect participants.

Limitations

This research study was subject to the following limitations. First, the key constructs and phenomena in this study were difficult to articulate as they are subjective to the perceptions of participants. However, this limitation is also a strength of the phenomenological design, as these subjective perceptions hold the answer to the research question. Second, the target population was limited to private organization security practices. This limitation was important to control the scope of this research study. Third, the sample in this study was limited to information security professionals in the Pacific Northwest region of the United States. This limitation was important to controlling the scope, but alternate regions may have different methods or concerns. Finally, the information security professionals' perceptions of the experiences may have been impacted by variables other than those included in the scope of this study. However, this limitation is addressed in the flexible nature of the semi-structured interview process in order to allow for the collection of alternative variables.

Nature of the Study

A qualitative phenomenological study was utilized to explore the lived experiences of IT security professionals working in information security incident management serving private organizations. The primary data collection instrument in this study was a collection of open-ended interview questions. These questions were reviewed and approved by industry experts in a field test prior to the start of data collection. The study was intended to be conducted by interviewing 20 IT security professionals providing information security incident management services to corporate organizations. Participants were recruited from the Pacific Northwest's rich culture of private technology firms. An additional 10 participants were to be recruited if saturation was not reached within the first 20 interviews. However, this addition was not necessary.

Criterion sampling is a process of selecting a research population based on the development of specific criteria (Suri, 2011). This is a purposive, non-random sampling method. Criterion sampling was used to ensure that data would be produced from specific lived experiences in order to contribute to answering the research question. Participants met at least one of three qualification sets. Set one participants were IT security professionals with at least 10 years of experience in information security and no recent experience within the past five years directly supporting military, government, or law enforcement agencies. Set two participants were IT security professionals with at least five years of experience in information security, a bachelor's degree or higher, and no recent experience within the past five years directly supporting military, government, or law enforcement agencies. Set three participants were IT security professionals with at least five years of experience in information security, a professional security certification, and no recent experience within the past five years directly supporting military, government, or law enforcement agencies.

The researcher explored this topic using open-ended questions during semi-structured interviews. These procedures are effective at obtaining appropriate information for a phenomenological study (Flood, 2010). As the analysis of this data was subjective, it was important that preconceived perceptions and biases be bracketed through the epoche as a means to improve credibility and address researcher bias. The analysis process in phenomenology is iterative in nature in order to obtain meaning from the review process (Gill, 2014). The iterative analysis was important to establishing a strong foundation for additional assessments. As data was collected and reviewed, it was grouped into clusters and analyzed. The identification of units of meaning indicates a structure that reflects the essences of the experiences of participants (Van Manen, 2014). These essences were the answers to the research question.

This study advanced the scientific knowledge base by exploring the experiences of IT security professionals providing corporate information security incident management services. Following an extensive literature review, as documented in chapter 2 of this study, a gap in the knowledge base was discovered. There has been some exploration of corporate information security incident management, but it is fragmented. However, the literature that exists on information security is primarily passive in nature. Corporate organizations have fewer dedicated resources for security than military and law enforcement agencies (Symantec, 2013). They are not empowered to perform the same actions as law enforcement or military personnel. Corporate information security incident management presents unique challenges to staff which were explored. An exploration of this issue enabled organizations to better understand the experiences of staff. This research can serve as a springboard for future researchers seeking to develop appropriate information security incident management methods for IT security professionals.

Organization of the Remainder of the Study

This report is organized into five chapters. While this first chapter describes the research problem and lists the research question along with a brief overview of theoretical concepts, the remainder of the study is organized to respond to the research questions asked in this section, in order to address the research problem. In chapter 2, the literature review begins with a discussion of information security ontology. Due to the connected nature of IT, establishing the boundaries of this particular field is important in order to limit this study to its most relevant components. The second section of the literature review expands upon the ontology of information security by establishing how information security is implemented in organizations to prevent information security incidents. However, the third section of the literature review addresses what happens when these protections fail and how these incidents are managed. The fourth section explores the breadth of knowledge about the elements of information system attacks and attackers. These various elements represent a holistic view of information security and information security incident management. The final section of the literature review explores literature related to the dissertation methodology, approach, instruments, measures, and methods.

Chapter 3 contains the explanation of the method used to conduct this study. The focus of this chapter is on the phenomenology methodology, study sample, data collection methods, and data analysis tasks. The study was comprised of semi-structured interviews conducted with information security professionals. These interviews were conducted by this researcher and coded in order to identify the essences of information security incident management. These themes were analyzed using the methods detailed in chapter 3. The methods and procedures described in this chapter were the recipe for how data was collected for the study and later analyzed by the researcher.

The analysis of the results is detailed in chapter 4 as generated from the analysis of the data collected. The results of the study were examined and deconstructed in accordance with the methods documented in chapter 3. It is through this phenomenological examination that emerging themes were discussed. Finally, chapter 5 begins with a discussion of the themes documented in chapter 4 in order to respond to the research question. The results of this research were then used to recommend future research opportunities.

CHAPTER 2. LITERATURE REVIEW

In chapter 1 the research topic is outlined at a high level in relation to the study to be conducted; however, in this chapter the goal is to discuss and define information security. Upon completion of this review covering the ontology of information security the discussion will switch to the discussion of information security defense and attack. This should provide a good understanding of the field of information security as a whole. As stated previously, cyberspace has grown from a small-scale defense research project to a world wide web of digital connections that is deeply integrated into various aspects of modern life. This growth, while wonderful, has also brought attention to the field of information security. The ontology of information security is a developing subject composed of technology, processes, and people in the defense and attack of systems. Despite defensive measures information security incidents can still occur in organizations.

Information security incidents occur when security has failed. To summarize from chapter 1, the information security incident management issue addressed in this research entailed the following: identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents. Information security in corporate organizations is primarily focused on preventive measures that are passive in nature; however, information security incident management is reactive (Etzioni, 2011; Pusey & Sadera, 2012). These characteristics are important to understanding the current state of defensive measures commonly deployed for information security. Understanding the technology, processes, and people involved in this complex topic area required a deeper dive into the existing literature on information security.

The following four fields were central to providing a theoretical framework for the research area described above: information security ontology, information security prevention, information security defense, and information security attack. In the next section information security ontology is explored in order to establish a broad theoretical framework for subsequent topics. The second section moves to focus on corporate information security in practice. This builds upon the theoretical framework to establish how information security is used by organizations and covers preventive measures such as risk management. The third section emphasizes information security defense and builds upon the established theoretical framework to establish the boundaries of what may be considered a security incident and to identify how they are managed within organizations. The final field of significance relates to information security attack. As is highlighted throughout this review, information security is both the defense of assets and the attack on assets. Therefore, in order to establish a holistic theoretical framework that covers all of information security, it is helpful to understand both the defensive and offensive aspects of information security. The final section of this chapter addresses the literature on research methods relevant to this study.

Information Security: Ontology

Information security has its own unique ontology consisting of technology, processes, and people. Vuorinen and Tetri (2012) conducted a grounded theory study in order to identify the ontology of information security; they concluded simply that information security is a system of systems, with the dual function of inhibiting entry and exit to a system of machines. In this context the security machine is technology and is a separate entity to both information and users. Defense in depth is a security strategy created by layers of protective systems where data exists in territories and access to the data is controlled by the information security systems of systems (Vuorinen & Tetri, 2012). The ontology of information security in this instance indicates that information security exists independently of other concepts, but when these concepts and security are combined, complex systems of systems develop. This complex system of systems, such as the relationships between anti-virus applications and computers, is the foundation of information security. However, these observations on the ontology of information security only cover technical elements of information systems and exclude other components such as processes and people. In order to develop a more complete understanding of the ontology of information security additional concepts must also be considered.

The evolution of technology from isolated systems into large computing networks means information security must be more than just a perimeter. Pieters (2011) conducted a study expanding on the ontology of information security and concluded that the distribution of data across various points has changed the nature of information security from perimeter security to data security in order to focus on the confidentiality and integrity of information. The distribution of data to multiple locations, both internal and external, to organizations has increased the permeability of perimeters and decreased their importance to the security of information. Cloud computing services allow data to be stored in a third-party system in order to be accessed and manipulated from around the world. This demonstrates that information can no longer be contained in isolated networks with large walls. The changing nature of technology has eroded the idea of security through perimeter defense, and new concepts indicate that information security should be performed as close to the data as possible. Therefore, because data no longer exists in isolation, the changing nature of technology requires a shift in the ontology of information security to include information as a technology asset. This change is an important improvement upon the defense in-depth system of machines by extending the protection to the information level in order to protect information in a mobile world. These two security concepts represent which technology is part of information security: systems, including computers, devices, and other information-based technology, and information itself.

Technology is only one of the elements of information security ontology and represents what needs to be protected but processes represent how data is to be protected. Thomas and Dhillon (2012) presented a case study demonstrating the interplay between the deeper technology structures and the representational security procedural models in which they demonstrate the importance of understanding this relationship on effective information security practices. Security procedures indicate how deeper technology structures are to be configured to provide protections for system and information assets; therefore, understanding this interaction is important to establishing an understanding of information security. The information security procedure for establishing password complexity is a representational model for the technological configurations that enforce the use of complex passwords. The deeper structures of security represent the technology configurations to enable protections and the procedures indicate how systems and data are to be protected. Technology interacts with procedures to create a secure environment. This interplay is important to understanding the ontology of information security as more than the placement of static technology. The relationship between technology and procedures is one that must be effectively managed to generate a secure environment.

Procedures are related to the technology they work with and this relationship is further expanded upon through additional procedural groupings. Vorobiev and Bekmamedova (2010) presented a study on what they term the security asset-vulnerability ontology, which is presented as the overall interrelation between the sub-ontologies of security function, security algorithm-standard, security attack, and security defense, in which these authors conclude that these groupings represent a common ontology for security processes. These security ontology groupings represent high-level security concept processes. These concepts represent the high-level security elements for processes and are often related through system security plans for organizations that focus on the process of security. The security function and algorithm-standard groupings represent the highest level concepts of information security such as access control, cryptology, and privacy while the attack and defense processes represent the active use of security concepts such as performing or defending against a denial of service attack. Technology is not static and is a complex system of systems which are managed by related processes. These high-level ideals provide conceptual groupings for performing information security tasks including the specific tasks of attack and defense. While these processes represent how information security is achieved for the technology that requires protection they provide only some indication as to why information security is necessary.

The final ontological element of information security is the most dynamic and therefore the most challenging to clearly identify: people. In addition to identifying a need for data level security Pieters (2011) further explored people as an element of information security and discovered that they are a dynamic force that plays a central role in the security of information systems including both attackers and defenders. People are dynamic and unpredictable elements that cause various changes and bring unique situations to bear on technology systems that influence information security. As defenders people implement security procedures to protect systems and information; while, as attackers, people work to identify weaknesses to exploit systems and information. As part of information security the social constructs including motivations for attack and defense are important elements in the understanding of information security as the existence of attack indicates the need for defense. In this sense, addressing only security technology and security processes is flawed as the social elements of information security are essential to further understanding security. The establishment of these dual concepts is important to understanding why security is important and each of these situations is as dynamic and diverse as the people performing these actions. People are why information security is necessary and are therefore important to understanding information security.

The ontology of information security consists of technology, processes, and people. Systems and information are technology assets that need protection and are protected in accordance with various processes made necessary by the existence of people performing attacks thereby requiring defense in this complex system of systems. Technology represents the what, the processes represent the how, and the who and why of information security is represented by the people. These three elements establish a foundation for the nature of information security. Information security is dynamic and can be as large and complex or as small and compact as a situation requires. Understanding technology, processes, and people is important to establishing the ontology of information security. Information security ontology is therefore the identification of technology assets and targets, the processes of defending or attacking those technology assets and targets, and the social constructs influencing attackers and defenders. Establishing this ontology for information security provides a common frame of reference for discussion on this topic. Understanding the ontology of information security is important to analyzing the practical applications of information security.

Information Security: Prevention

Information security is used in many practical situations and has evolved over time into its current form. Elachgar, Boulafdour, Makoudi, and Regragui (2012) identified four unique developments in information security and presented a grounded theory in the application of information security based on the evolution of information security:

> First Wave: security as a technical issue addressed by technical people;
> Second Wave: security as a management issue addressed by non-technical people;
> Third Wave: security through compliance and standardization;
> Fourth Wave: security as a board level function of good corporate governance led by chief executives and enforced by government regulations. (p. 2)

The fourth wave of developments in information security represents the growing maturity of information security as a field of interest for organizations. The incorporation of information security into corporate governance allows information security to be included in corporate risk management in order to increase value for the organization. The fourth wave represents modern information security concepts put into practice in organizations incorporating information security concepts into areas that were previously not considered relevant to information security. The integration of information security into corporate governance demonstrates process maturity in organizations through the application of the other three waves with technical experts, active security management, the use of security standards, and the support of corporate executives. Charting the development of information security, such as the changing ontology, indicates a pattern of growth in the subject area. Integrating information security at the highest levels of an organization is an important development in information security as new developments continue to take place in the field.

However, the real application of security is rarely so perfectly integrated with management. In a phenomenology study conducted by Schuesster (2013) participants revealed that information security was consistently ranked low by corporate management in a list of priorities leading Schuesster to conclude that legislators are currently paying more attention to the management of information security, as demonstrated by the increase in information security regulation, than many organizations. These interviews demonstrate the lack of priority given to information security and further indicate the importance of forced regulation on the information security industry. Despite the incorporation of regulatory requirements for information security into corporate governance major security breaches occur frequently around the world for various reasons including failure to fully implement standards. The low prioritization by management and the development of regulatory environments are examples of how the people element of the established information security ontology interacts with the practical application of information security. The forced regulation of organizations has given rise to a culture of "good enough" security concepts designed to meet regulatory requirements in order to alleviate liability but do little to impact the deeper structures of information security. The concept of liability in relation to information security is important to the practical application of information security as it is an indicator of the extent to which organizations comply with regulations to alleviate responsibility in the event of a breach. Determining the information security in organizations is a measurement of risk and reward.

The concept of risk management is a core tenet of functional information security practices. Fenz et al. (2011) conducted two qualitative case studies on European companies using a customized risk management framework designed to identify and reduce risks to acceptable levels at the lowest possible cost based on a number of factors including threat sources, vulnerabilities, and impacts. Risk management helps organizations to manage their information assets in a fiscally responsible way as it is unlikely that any security solution can be made impenetrable at a reasonable price. A technology asset that is critical to the organization, such as information on trade secrets, should be protected from various threats; but, in reality, the cost of extreme protection may outweigh the potential cost of a breach. Thus requiring a third option that incorporates the most effective and fiscally responsible measures to provide some measure of information security. Risk management implies several elements including the acceptance of the existence of vulnerabilities in systems, threat sources that want to exploit those vulnerabilities, costs to organizations, and an intersection of those concepts at an acceptable level. Information security risk management as a function of corporate governance as backed by legislative regulation is very different from the established ontology of information security. Risk management is an important concept that has both hindered and advanced the cause of information security by providing management with options between all or nothing in the protection of technology assets but by its very existence reveals the accepted nature of security vulnerabilities that can be exploited by threats. There are many risk management frameworks that organizations may use to provide guidance in identifying and protecting assets in this middle ground.

Risk management in practice is a complex preventive measure for organizational information security management. Gikas (2010) conducted a literature review on several risk management governance standards with regulatory measures in order to evaluate the effectiveness of available security methods. Gikas discovered that the National Institute for Standards and Technology (NIST) 800 series is the most comprehensive framework when compared with the Federal Information Security Management Act (FISMA), Health Information

Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and International Organization of Standards (ISO) 27000 but there are also many common control areas that overlap between these standards. There are many different frameworks for accomplishing risk management as a function of information security that, while different in some ways, share many common elements. It is difficult to identify when security frameworks are successful but easy to identify when they fail; however, all are designed to provide organizations with a method of designing at least a minimum level of security. Inside each framework are various items and elements that address potential vulnerabilities in technology, processes, and people with guidance for managers on how to address these within their organization. While these standards perpetuate the concept of "good enough" security they provide organizations with an essential guide to security concepts. The use of risk management frameworks as standards and guidelines provide organizations with a functional basis for information security. While frameworks do not address all potential security concerns at a mature level identifying a common risk framework assists organizations in performing essential security tasks.

These contemporary programs all incorporate risk life cycles into operational security and share common elements of good security program governance. There are many common elements between these various risk management frameworks, as proposed in the integrated risk management framework proposed by Tohidi (2011), which include nine steps of risk estimation and the six methods of risk reduction:

Risk Estimation Steps:

1. System Characterization

2. Identify Threats

3. Identify Vulnerabilities

4. Analyze the Controls

5. Determine the Probability

6. Analyze Effects

7. Make Risk Determination

8. Control Purchase Order

9. Documented Results

Risk Reduction Methods:

1. Assumption

2. Avoidance

3. Limitation

4. Planning

5. Acknowledgement

6. Transfer (Tohidi, 2011, pp. 883-885)

These procedures and outcomes represent the way information security is practiced in organizations that are forced to deal with vulnerabilities that cannot be eliminated from systems. A discovered vulnerability that may allow an attacker to execute remote code on a system would generally be ranked as a high-risk vulnerability due to the potential impacts and that risk can be managed by implementing mitigating controls or simply assuming the potential risk without mitigating factors. These processes and outcomes, executed as a coherent framework targeted on technology, processes, and people, represent a well-developed, holistic, and integrated platform for the management of security vulnerabilities. The ontology of information security indicated the exploitation of assets and this process is how those technical, procedural, and human vulnerabilities are managed in the face of real-world threats as commonly enforced by corporate governance. In many instances it is simply not possible to eliminate a risk due to a variety of factors and this framework provides organizations with a method for identifying and addressing these vulnerabilities. These imperfections and assumptions, among other things, allow attackers to penetrate systems.

Information security in practice is primarily a preventive function of organizations as a system of managing risks in accordance with regulatory standards and common frameworks. The fourth wave of information security, spurned by legislatures through regulatory measures, incorporates the concept of “good enough” security for liability in which organizations use standards and frameworks that accept and acknowledge that information security is about managing vulnerabilities in the prevention of information security breaches. Risk management is how information security is performed in modern organizations through the analysis and evaluation of vulnerabilities against threats to determine risk and the mitigation of that risk based on organizational priorities. Risks can be presented in technology, processes, or people with a wide variety of potential outcomes. The important element of information security in practice is that vulnerabilities exist that cannot be eliminated for various financial, regulatory, and social reasons. Therefore, the practical implementation of information security is not perfect and these imperfections are managed through risk management. Exploiting vulnerabilities in technology, processes, and people is in the nature of information security. These limitations in real-world security leave the door open for security incidents.

Information Security: Defense

When a vulnerability is exploited an information security incident has occurred in the organization. There are many potential types of information security incidents, as defined in a literature review conducted by Drtil (2013), in which it was determined based on three elements of technical information security Confidentiality, Integrity, and Availability (CIA) that nearly everything is a security incident and that preventive defensive programs are recommended to prevent information security incidents. These three broad categories are core tenets of information security in that confidentiality is designed to prevent disclosure, integrity is designed to prevent unauthorized influence, and availability is designed to make the asset available to the correct people. In that sense, any interruption to these principals is an information security incident and therefore subject to an organization's information security program. Under this description of information security incidents as natural as a winter storm or as eventual as a hardware failure can both impact availability and are therefore both information security incidents. These three important elements, CIA, are core tenets of information security but when taken out of context the scope of information security spirals out of control. Any incident including weather, denial of service, hacking, or hardware failures are all vulnerabilities that carry a level of risk to technology. When not properly mitigated these vulnerabilities become incidents in organizations but they are not all information security incidents. The description of information security provided by Drtil describes nearly any potential incident as an information security incident that is outside the scope of the established nature of information security. Security incidents can be many things but they cannot be everything.

These broad security incident categories, CIA, must be considered within the context of the established information security ontology. Ayyagari (2012) conducted an exploratory analysis using content analysis of 2,633 security incidents resulting in the compromise of information across all types of industries including government, education, health, and corporate organizations. Ayyagari discovered that the loss of portable information, followed by hacking, and then the accidental disclosure of information were the highest causes of information security incidents. The compromise of information can come from several possible situations but the end result is the loss of the confidentiality or integrity, or both aspects, of the information. The breach of a customer database is an example of a compromise of information that immediately results in the loss of confidentiality and may also result in a loss of integrity depending on the actions of attackers during the incident. A data breach is an example of an information security incident that includes targeted technology assets, processes for attack and defense, and attackers and defenders. A data breach is one example of a category of information security incident that matches both the broad categorization of incidents with the nature of information security. This categorization limits the range of information security incidents in order to focus on incidents that truly are within the realm of information security. Data breaches are only one potential categorization of information security incidents that apply within the ontology of information security.

The integrity of information can be compromised in several ways but the most damaging and disheartening is through acts such as fraud and embezzlement committed by trusted insiders. Van Gent, Lindquist, and Smith (2013) conducted a case study examining an instance of fraud and embezzlement totaling nearly six million dollars over the course of more than 20 years by a single employee of a small town bank, who used various methods including augmenting the bank's accounting software to commit and hide the fraud. This type of theft is only one of several potential methods of violating the integrity of information and also includes the abuse of authority; which, is one of the most difficult elements of the people aspect of information security to prevent or detect. A certain level of trust must be invested in members of organizations entrusted with unique duties, such as system administrators, and these trusted individuals, as was the case in this study, can abuse this trust without having to circumvent complex controls designed to protect assets from external attackers. The falsification of electronic data violated the integrity of the information making the compromised source untrustworthy in order to commit and cover a crime. The fraud investigated in this case study conforms to the information security ontology as the attacker executed vulnerabilities in technology and process controls to commit the fraud while defenders worked to discover and prevent fraud. Integrity is perhaps one of the most abused ideals within the scope of information security and without limiting potential information security incidents to clear incidents that fall within the scope of the established information security ontology it is a slippery slope to including many incidents that have no connection to information security. Fraud is only one of several potential intentions of attackers.

Another threat to integrity is digital vandalism which comes in many forms. Bartoli, Davanzo, and Medvet (2010) conducted a quasi-experimental study on the detection of cyber vandalism in the form of website defacement, the process of attackers modifying web assets resulting in a loss of consumer trust and confidence, and determined that their solution for detection, named Goldrake, was partly effective. Cyber vandalism is not as high profile as a data breach resulting in the loss of sensitive information; but, it is a low-cost and popular way for attackers to undermine trust and confidence in organizations by violating the integrity of websites. Hactivists, activist hackers, use this technique to promote their agenda by defacing opponent’s websites. There are many potential reasons why an attacker may target a website but the early detection of this loss of integrity may help organizations to quickly and promptly identify the information security incident and restore sites to their correct format. This is another example of a form of attack that includes technology assets, a process for attack and defense, and active attackers and defenders. While this type of information security incident may not generate the same type of impact to an organization as a data breach or fraud it is a valid information security concern. The integrity of assets can be challenged using many potential techniques.

The most prolific threat to the integrity of information is malware. According to a case study, which included the world's first cyber weapon Stuxnet, performed by Langer (2011) indicated that malware variations number is the hundreds of thousands and that malware is a term used to describe a variety of automated approaches to compromising the integrity of systems and information using malicious code. Malware is a broad term used to describe a number of different threats to the integrity of technology assets and is generally a means to an end. Stuxnet is a malware application designed to compromise the integrity of selected control chips and cause real-world damages resulting in loss of availability of the asset. The integrity of assets, information and technology, is important for organizations to function and these threats to the integrity of systems are dangerous and costly. Malware is a threat to the integrity of technology assets and since they use processes to exploit vulnerabilities and are created, but not guided, by a human attacker it falls within the scope of information security. This type of information security incident is widespread and therefore it is important for organizations to include protections for the integrity of assets against malware. While malware instances number in the hundreds of thousands, it is still one of many potential information security incidents within the scope of information security.

The final broad category of information security incidents is availability. Stapleton and Woodcock (2011) conducted case studies on two of the most widespread Distributed Denial of Service (DDoS) attacks in current history responsible for crippling both the nations of Georgia, contributing to a military victory during the invasion by Russian forces, and Estonia, in response to a political feud resulting in massive financial losses. The authors concluded that increased computing power and multiple communication pathways may have helped these nations defend their assets (Stapleton & Woodcock, 2011). DDoS attacks cause the disruption of services and when targeted at highly connected assets can be a devastating attack. While the concept of DDoS is demonstrated on a national scale by these authors, it can also be applied to smaller organizations or even service providers to cause massive service disruptions. The attacks in Georgia and Estonia demonstrate the potential of DDoS attacks to disrupt the availability of assets that may be critical to functions such as national defense or financial services. While the availability of assets can be jeopardized by many elements, very few are targeted at assets and executed using established processes by human attackers. IT is highly connected in multiple aspects of modern life and cutting people off from their assets can have devastating effects that will only continue to grow as humans rely more on connected technology. DDoS is a unique information security incident within the context of the CIA triad and the established information security ontology.

Information security incidents cover a wide range of possibilities, as established in the CIA triad, which include the elements of the information security ontology. While some threats within the scope of information security against elements of the CIA triad are clear many information security incidents are more complicated and may defy categorization such as a potential attack on integrity against an ISP provider as described in a study by Cobb (2011);

which, could result in compromising the availability of national security systems in the United States. Things are rarely as black and white as to be clearly defined in any one category and may fall into multiple categories based on the primary and even secondary impacts of information security incidents. The connected nature of technology means the impacts of information security incidents may not be confined to a single source such as breaching the confidentiality of information held by an organization that in turn may result in fraud in another organization. The important thing about information security incidents is that they conform to the scope of information security rather than operations, development, or other IT disciplines that each have their own standards. Information security in practice accepts vulnerabilities making information security incidents likely and each of these information security incidents must relate to the elements of information security including the identification of assets, processes for attack and defense, and human attackers and defenders in order to be considered an information security incident. Establishing this scope on information security incidents provides a frame of reference to limit the exploration of incidents to occurrences that meet the principals of information security. Identifying incidents is only the first step in a larger incident management process.

Information Security: Incident Management

There are many different types of information security incidents that may impact organizations which are detected and addressed through a process called information security incident management. The first phase of information security incident management, according to an empirical phenomenology study by Werlinger et al. (2010), is the diagnostic phase which consists of prevention, detection and identification, and analysis. The responses from the incident managers in this study provide a unique view of how information security incident management is performed and the inherent problems in current tools and processes in this phase of incident response. The prevention of information security incidents includes the previously discussed elements of risk analysis, which are focused on prevention and works, in conjunction with detection and identification, which are focused on identifying the type of anomaly and confirming that an information security incident has occurred. Finally, the analysis of the incident determines the magnitude, impact, and threat source, internal or external, to the organization. Information security starts with prevention, but when prevention fails the diagnostic phase of information security incident response is designed to identify and analyze the potential information security incident in order to indicate the correct steps to contain and recover from the information security incident. This is difficult due to limitations in current technology and processes. Identifying the elements of an information security incident can help lead to successful containment and recovery after an incident. However, the first step is detection and identification.

Part of the diagnostic phase is the detection and identification of an information security incident. While the case study conducted by Blyth and Thomas (2006) is outdated, they reviewed a unique method for identifying information security incidents based on a concept called a footprint which is used by real-time monitoring systems to identify types of threats based on various aspects including the potential attack target, method, and purpose. Information security incidents are commonly identified during monitoring activities using a variety of signatures with various elements; but, the footprint presented by Blyth and Thomas includes elements of technology, processes, and people. The elements of this particular footprint are similar to those used by the United States military intelligence for battlefield analysis (Department of the Army, 1994). For example, there are differences between the weapons, tactics, techniques, and procedures of the United States and Russian militaries and there are differences between internal and external attackers that each have different weapons, tactics, techniques, and procedures. The concepts presented by Blyth and Thomas (2006) are important as they demonstrate the value of real-time monitoring and the establishment of a good footprint for effective information security incident management. There is a limited amount of recent research in this area of information security as it deals with various attack models for the purpose of defense but the footprint presented by these authors, when used in conjunction with effective monitoring, can provide increased detection of information security incidents. The identification of an information security incident is important, as not all information security incidents require the same responses, but the identification of anomalies using effective monitoring is a key element of information security defense through effective information security incident management. The identification of an information security incident is only the first part in the larger process of information security incident management.

Once an incident has been detected and identified it must be analyzed. Wang, Guo, Wang, and Zhou (2012) conducted a study to develop a metric scoring system using a comprehensive information security ontology to coordinate between multiple threat databases in order to calculate and rank attacks based on severity and time. However, while new vulnerabilities can be grouped and ranked based on known vulnerabilities this system does not account for all attack patterns or vulnerabilities that do not exist across all databases. Analyzing information security incidents is an element of the diagnostic phase of information security incident management. By using common databases known vulnerabilities can be ranked and evaluated to prioritize response actions based on known attack patterns. Internet Explorer is a common web browsing application with known vulnerabilities and exploits and based on the severity of the vulnerability, the time passed since the vulnerability was discovered, and the number of attack patterns that match the vulnerability a ranking of known vulnerabilities can be identified in order to match information security incidents. While there are many different ways of ranking information security incidents this particular method is unique enough to coordinate between multiple databases to evaluate the severity of vulnerabilities, group patterns of attacks, evaluate weights based on time, and rank individual attacks to establish specific threat patterns. Similar to the acceptance of flaws in information security practices some information security incidents may never be resolved if the severity is not high enough. The prioritization of information security incidents is important to managing information security incidents as multiple information security incidents may occur simultaneously or certain information security incidents may not rank high enough to warrant certain actions such as forensic investigation or breach notification. Once the diagnostic phase is complete, information security incidents that warrant continued response enter the next phase of information security incident management.

The appropriate response to an information security incident is dependent upon the type of attack being performed but the next common stage in information security incident management is containment. In a study performed by Rajakumar and Shanthi (2014) on financial systems information security incident management consists of diagnosis using spectrum analysis and worm detection followed by containment using a process called IPTraceback; which, is a process developed by Rajakumar and Shanthi to trace and identify the source propagator of worm traffic and shut it down to contain the spread of the worm. The containment of an information security incident depends on the type. In the case of a worm, which can quickly spread through multiple systems, identifying and shutting down malicious traffic to stop the spread of the worm is a prudent defense strategy. In the case of a worm infecting one computer, which then infects five more computers, the process of IPTraceback can identify the source propagator and shut down traffic to halt the spread of the worm and thereby contain the information security incident. The concept of containment is important in information security incident management in order to contain the attack to the smallest possible area and minimize the impacts to the organization. While the processes used to contain a worm will be different from other information security incidents, the concept of containment is a common theme that works in conjunction with diagnosis to defend networks by managing information security incidents. Containment is one of the core common elements of information security incident management that, despite the type of attack, remains constant. Once an information security incident is contained the organization must recover from the information security incident.

The final common component of information security incident management is recovery; which, may be known as business continuity, disaster recovery, or remediation. Kadlec and Shropshire (2010) conducted studies on disaster recovery strategies, not specifically in relation to information security incident management, and despite an astonishing claim that 60% of businesses lack disaster recovery plans and that current regulations are not enough to avert disasters a series of several best practices from backup and recovery management to employee preparation are presented by these authors. While responding to information security incidents accounts for only a small part of why systems may need to be recovered, it is an essential function that many businesses are currently failing to meet at any meaningful level. During an information security incident a server may become compromised which may indicate that the data within the server may no longer be trusted. After the diagnosis and containment of the incident it is necessary to perform a recovery operation against that server to restore the integrity of the information and return the system to working order. There are many important elements to information security disaster recovery including effective planning and rehearsal; and, these actions must occur at all levels of infrastructure from individual systems to entire networks. The recovery of assets impacted during an information security incident is the final common core function of information security incident management and it is one that is also shared with other IT and business components, requiring extensive communication and cooperation; but, the lack of corporate awareness on disaster recovery and information security incidents is evidence of gaps in the study of defending networks. Hopefully, recovery plans are never actually needed by organizations but it is essential that they are in place to prevent further damage during an information security incident and other disasters. While there are only three common components to each information security incident, there are many additional tasks that may be performed in relation to an information security incident.

There is a lack of empirical evidence demonstrating a holistic response process integrating all three of these core processes. While standards do exist for conducting incident response, such as standards contained in the NIST, SANS, and ITIL frameworks, organizations have not disclosed various parts of the incident response process to researchers to empirically evaluate (Ahmad, Hadgkiss, & Ruighaver, 2012; Werlinger et al., 2010). Organizations have not revealed parts of the incident response process to researchers for multiple reasons including the sensitive nature of these incidents, the breadth of possible response techniques related to each security incident, and the variances in organizational implementation of standards. It is only through the use of non-scholarly sources that the entire framework can be seen together but elements in scholarly sources can be used to create a whole process by inferring logical steps. In the research presented on information security incident management some form of diagnosis, containment, and recovery action must occur in order to detect, stop the spread of an incident, and return systems to a secure state (Chu, Deng, & Chao, 2011; Lanter, 2011; Tammineedi, 2010). However, these parts of incident response and steps to address attacks are not represented as a holistic information security incident management process in current literature. This gap presents an incomplete picture of this sensitive and important information security process.

In addition to the core common elements of information security incident management there are several other disjointed information security incident management processes that exist as part of some, but not all, incidents. Shaw (2010) performed case studies against two of the largest data breaches in current history involving ChoicePoint and the TJX Corporation, focusing on their notification procedures as required by current consumer protection regulations, and concluded that conflicting standards, spotty enforcement, and a lack of clear preventive standards are gaps in current breach notification laws and information security practices. In relation to information security incident management certain regulations exist that compel organizations to disclose a breach affecting certain types of information under certain circumstances; but, these factors are not always clear or enforced. Upon diagnosis of certain incidents affecting certain information under certain conditions, such as consumer personal information in an unencrypted format, a breach notification is released using methods regulated by the size of the breach ranging from phone calls to television announcements based on the regulatory environment. Organizations are entrusted with various elements of consumer information that is collected for various purposes including processing online transactions and data mining. They are legally responsible for the security of that information and must notify individuals of a breach to their personal information in the interest of protecting consumer rights and privacy (Shaw, 2010). While these two case studies were not conducted to highlight information security incident response methods, the notification of a breach, while not always required during incident response, is important for keeping consumers aware of the status of their personal information entrusted to organizations. But notification is also a point of contention, as organizations work within the letter of the law, rather than the spirit of the law, to avoid or limit disclosure of information security incidents. This is one of the few semi-standard and well-documented elements of the post-diagnosis information security incident response process. This process is becoming more standardized as the regulatory environment improves.

Another element of the post-diagnosis incident response process is forensic investigation. Computer forensics, according to a study done by Sindhu and Meshram (2012), is the science of identifying, extracting, analyzing, and presenting digital evidence consisting of several phases including collection, examination, analysis, and reporting that is primarily used for law enforcement. Forensic investigation is a process of collecting data for the general purpose of meeting a legal burden of proof; however, that information can be used for various purposes in the information security incident management process in addition to establishing a chain of evidence. In the event a crime has been committed and reported information security incident responders are likely to be the first responders in an information security incident and any organization choosing to pursue a legal resolution to an information security incident will need to conduct forensic investigations in order to capture and control evidence. Forensic investigations are important for various reasons, including meeting legal burdens of proof, but can also be used to assist in the diagnosis, containment, and recovery processes; most importantly, the data can be used to learn about incidents. While there are as many type of digital forensic techniques as there are types of technology that store digital data the process of collecting that data is often incorporated into information security incident response programs for various reasons and at various levels of detail to meet the evidentiary needs of the organization. Cyber crime in today's digital world has continued to increase over the past several years and increasing awareness of forensic techniques may help organizations to be better prepared to address these threats in cooperation with law enforcement. The limited use of formal forensic investigation processes in organizations is one of many limitations of current information security incident management programs.

Information security incident management should not simply end with the restoration of services. Ahmad et al. (2012) conducted case studies on information security management in the financial industry and discovered several interesting flaws. Ahmad et al. noted (a) a lack of learning and knowledge management following incidents; (b) the reclassification of incidents under alternative definitions to escape regulatory requirements until such time as a decision is made that it would benefit the organization to respond; and (c) that many organizations are ill prepared for incident response with some forgoing evidence procedures in favor of resuming production without investigation. Not only are organizations limited by their lack of learning from incidents but the active dodging of legal requirements, and in some cases information security incident response altogether, makes it difficult to establish the size and scope of information security incidents in organizations. Failing to learn from information security incidents may lead to continued information security incidents. Not taking advantage of operational improvements while refusing to report information security incidents limits the amount of knowledge available to researchers, law enforcement, and compliance auditors. The important elements to note from this case study (Ahmad et al., 2012) are that incident management processes are not fully implemented in many organizations and some are implemented in counterproductive ways that limit the effectiveness of regulatory requirements. While a process exists to prevent information security incidents using risk management, diagnose incidents when they occur, contain and respond to incidents as needed, recover systems, notify people, and conduct investigations, the lack of learning in this model limits its effectiveness and the inconsistent and counterproductive implementations make it difficult to assess. In short, the implementation of information security incident management is often flawed. The implementation of these programs varies in many ways that often run counterproductive to other efforts.

Information security incident management addresses the reactive defenses of organizations in the event of an information security incident. This process is established in several standards and implemented in organizations in various ways; however, many of which are limited in their scope, lack reporting, and fail to learn from each incident. Information security incident processes exist but much like the concept of information security and the implementation of it in preventive risk management the implementation of information security in information security incident management is flawed and limited. Properly diagnosing, containing and responding to, recovering from, notifying, investigating, and learning from information security incidents can have positive benefits for organizations in the event of information security incidents. The elements of managing an information security incident exist including diagnosis, containment, recovery, notification, investigation, and knowledge management but current literature is fragmented regarding their application in current systems. While a limited number of organizations have established effective information security incident response programs others have established a culture of fear regarding reporting and sharing information; which, limits the information available in this field. The defense of assets, both preventive and reactive, is only one side of a two-sided process related to the ontology of information security.

Information Security: Attack

Attack and defense are not independent of one another. Understanding elements of both is required for understanding information security as well as how to allocate defensive resources. Gupta, Chaturvedi, and Mehta (2011) conducted an analysis of the relationship between attackers and defenders in relation to how attackers and defenders should logically respond based on certain conditions. They developed several propositions, such as:

> 1. If the penalty to the criminal is increased, the firm should (i) increase its infrastructure technology allocation (ii), decrease its security allocation, and (iii) increase its recovery technology allocation
>
> 2. If the penalty to the criminal is increased, the criminal should decrease its activity level.
>
> 3. If the skill set of the attacker increases, the firm should (i) increase its allocation to security technologies and decrease its allocation to recovery technologies below a threshold skill set (ii) decrease its allocation to security technologies and increase its allocation to recovery technologies above a threshold skill set.
>
> 4. If the skill set of the attacker increases, the attacker should decrease its activity level beyond a threshold skill set. (Gupta et al., 2011, pp. 289-291)

The analysis of the relationship between attackers and defenders gives an indication of how organizations may allocate resources under certain conditions. Using these unique markers organizations can allocate resources to information security areas appropriately as various elements change over time. The important element of this study is the establishment of a relationship between attack and defense. While there are few frameworks that link attackers with defenders, this unique model demonstrates a relationship between the two concepts and reinforces the importance of both attack and defense in information security. Despite establishing a relationship between attacker behavior and defense allocation the authors do not provide tests for these propositions and while criminals are not often logical these models present a starting point for establishing predictive models of behavior based on this relationship. Understanding the technology, processes, and people behind attacks is important to both organizational readiness and establishing an understanding of information security.

While there is a significant amount of literature covering many areas of preventive information security and some areas of defensive information security many organizations and researchers are only just realizing the importance of understanding the other side of information security. While hacking, the process of discovering and executing vulnerabilities in technology, processes, and people, has existed in many forms such as the 1970s Phreakers, the 1980s enthusiasts, the 1990s hacker criminals, and the millennial hacktivist, in the last decade, governments, corporations, and militaries have begun exploring these more aggressive elements, according to a review done by Bowles (2012). The development of hacking has gone through several stages that mimic the development of information security as a defense concept. Hacking can be used for a variety of reasons such as for cyber crime or penetration testing. The history of cyber attacks indicates a trending growth from groups of highly technical enthusiasts to criminals with the power to steal or destroy. While cyber attacks have existed as long as the need for defense, the exploration of attack by military, government, researchers, and corporate organizations can be seen as an extension of the four waves of information security proposed by Elachgar et al. (2012) into a fifth wave of information security as the research and implementation of information security attacks continue to grow. This fifth wave of information security is still being explored and the concepts are fragmented as many researchers continue to focus on the defensive elements of information security. While the history of hacking is unique, the present is full of mystery as the importance of information security attack is still being determined.

Cyber-attack methods are not well researched from the view of attackers. Geers (2010) performed a case study on a live fire international cyber war exercise. While the purpose of the case study was to review and offer improvements to the design of future virtual exercises, the author documented the attack method of the red team as a four-step process: declaration of war, breaching the castle wall, owning the infrastructure, and wanton destruction (Geers, 2010). The live fire exercise provided an environment for defenders to practice the defense of networks against attackers in a managed way that was capable of tracking strategies on both sides of the conflict. This type of war game is similar to traditional military exercises conducted internally or with friendly militaries to simulate real-world conditions for attack and defense against live forces and is an effective learning tool for offensive and defensive strategy. However, the case study was mostly focused on the blue-team response, as only the blue team could win the game, but the discussion of the red team's general purpose provides a framework for some types of cyber attacks. The type of research documented in this case study is typical of the limited research done in the area of information security attack methodologies as it is from a defensive viewpoint rather than discussing the science or merits behind attack methods. These defensive viewpoints limit the analysis of information security attack concepts to piecemeal compilations of ideas from various studies rather than a comprehensive review of cyber-attack methods. It is difficult to assess information in this topic area.

In order to gain information on information security attack concepts from scholarly literature the inverse of what is observed is considered. For example, Chan et al. (2013) conducted a study of live digital forensic techniques for anomaly detection in order to augment traditional security tools. Specific forensic techniques were presented as conditions that may identify when an attack has occurred:

> Condition 3-1: If the value of the “foreign address” item is within the foreign IP range (China, Taiwan, etc.)
>
> Condition 3-2: If the “name of process under execution” matches with information in the known malicious programs list.
>
> If applicable of Conditions 3-1 and 2 in Table 6, it can be judged highly probably that attacks of information leakage or hijacking the administrator right (root) are under progress by network connection of a malicious program or an attacker. (Chan et al., 2013, p. 186)

These authors demonstrated various live forensic techniques to detect real-time attacks on computer terminals but in doing so also revealed elements of how certain attacks may take place. The information in this article can easily be adapted for use in organizations through the use of available tools as a defensive measure but the implied elements of attack can also be adopted to improve detection through the study of attack methods. The important elements of this study exist in the opposite context of the intentions of Chan and his co-authors. Existing literature such as this study offer very limited pieces of information security attack concepts because the primary focus is still on defensive rather than offensive actions. The lack of information in this area makes it difficult to evaluate information security attack elements using only available literature, which impacts the study of defensive methods, as information security incident management is the marriage of defense and attack. However, this lack of scholarly information does not mean the information is not available.

While the information on the merits and details of attacks may be difficult to find in scholarly literature it is not difficult to find around the Internet. Hacker and criminal communities exist on the Internet; a simple web search using Google at the time of this writing revealed millions of wikis, videos, professional articles, news stories, blogs, and bulletin boards related to hacking computers. Even more data exists in a part of the Internet known as the dark net or deep web (O'Kelly & Trott, 2014). One of the more comprehensive resources on information security attack methods is the common attack pattern enumeration and classification database by MITRE which is a not-for-profit research organization (Zhongqiang, Yuan, & Zhongrong, 2010). This is an interesting area in information security research where a gap exists in scholarly literature but is filled by alternative sources thereby making it very difficult to conduct a literature review. In the context of information security incident management defensive actions must be taken in accordance with the type of attack being performed against the network but the merits and techniques of attacks have not been studied to the same depth as defensive measures. This field is rich with research potential. There are many different types of technology vulnerabilities and processes for attacking them with many different results; however, the one constant is the human aspect of information security.

Attack Source and Intention

There are various reasons why an attack may be executed against a target. The biggest threat to information security in organizations, according to a study done by Hua and Bapna (2013), is information security incidents from internal sources regardless of malicious intent. These authors applied game theory, a mathematical process for predicting situational outcomes, to model internal threats in order to demonstrate that insiders are extremely difficult to accurately address. Insider threats account for a majority of information security incidents in organizations and malicious insiders are difficult to defend against as many preventive measures are focused on external information security and are therefore bypassed by insiders. An insider, malicious or otherwise, may alter files, destroy information, disclose information, or even commit fraud by abusing the trust given to them by the organization to access systems. Hua and Bapna introduced several important concepts including identifying three unique types of insider threats: an accidental attacker as one creating an information security incident with a non-malicious intent without purpose; a purposeful but non-malicious attacker as one deliberately creating an information security incident without malicious intent; and a malicious insider as one creating an information security incident with malicious intent and purpose. Organizations have more control over insider information security incident response than external information security incident response. Therefore, as these aspects of source, purpose, and intent are important to classifying information security incidents it is important to the success or failure of the defense of networks. Insiders represent only one category of attackers. Despite the number of internal threats external threats can be far more dangerous.

While organizations are right to address the various insider information security threats external attackers have unique purposes and intentions. Some external attacks on organizations are purposeful but non-malicious, such as penetration testing, which, according to a study done by Halfond et al. (2011), is important to supporting information security by performing attacks to test security practices. External attacks may come in several forms including those that may use attack as a method of supporting the defense of systems rather than for malicious purposes. While these types of supportive attacks are often not used by organizations, less than 3% of organizations perform penetration testing according to Schuesster (2013), organizations or individuals may be hired to perform attacks against systems to determine the reliability of defensive measures and information security incident response through aggressive probing of externally facing network resources. These types of attacks and attackers support information defense by embracing the use of attack methods to test and improve information security. While organizations often do not embrace this support, and further research may benefit this methods contribution to defense, it is one method of testing the effectiveness of information security. The use of attack as a supportive element in the defense of systems is a unique concept that demonstrates positive value as opposed to external attacks performed for malicious reasons. While this type of attack can be beneficial, many external attacks are harmful to organizations.

External attacks may also be conducted for various malicious purposes. Kim, Wang, and Ulrich (2012) proposed a United Nations level cyber-security agreement which would emphasize measurement, responsibility, collaboration, and communication based on data gathered on cross-country cyber attacks to address the growing problem of cyber security. Cross-country cyber attacks are external attacks that originate from a variety of sources, using technology and processes both directly and indirectly controlled by human attackers who can cross borders around the world attacking targets from countries with lax security standards, allowing the attackers to avoid retaliation. Stuxnet, as previously discussed, is an example of an external attack committed by state-sponsored organizations for a malicious purpose and launched in a cross-country cyber attack. The global emphasis placed on addressing external threats in this study indicates a massive problem (Kim et al., 2012). While internal attacks may cause more information security incidents than external attacks, externally based attacks are a problem on a global scale; this problem is framed from a geo-political view rather than from an organizational viewpoint making it unclear how designating an attack source as external impacts information security for private organizations. While organizations have the authority and responsibility to address insider threats a malicious external attacker may attack an organization from anywhere in the world for a variety of reasons. Identifying an attack source as external with malicious intent is a broad category that addresses many types of source attackers that are linked to various purposes.

There are many different reasons for attacking a target. The hacktivist, as identified by Davis (2012), attacks for social or political purposes; espionage, as defined in a study by Greengard (2010), can be conducted by corporations or governments to steal secrets; and taggers, as defined by Warren and Leitch (2010), are hackers who attack to compromise the integrity of a website to alter its appearance. There are many different purposes that may be involved in an attack that are not always mutually exclusive and can be difficult to determine during an information security incident. A hactivist may tag a website in support of their agenda but the unauthorized access may be a criminal offense. Identifying the purpose of an attack can help to identify the social elements of an attack which may give defenders additional information to address an information security incident. Identifying attackers and their purpose addresses the human component of information security. Understanding these components provides insight into attack methods that may be used in support of each purpose by each attacker. This complex coding of attackers, methods, and purposes is not consistent throughout research or in practice around the world; therefore, many gaps exist in this important topic. While the source and intent address some of the human aspect, identifying the various attack purposes will continue to expand this topic.

Criminal Attacks

Cyber crime is a unique attack purpose that can be committed by both internal and external attackers. Hu, Chen, and Bose (2013) conducted a study comparing cyber-crime rates and punishments in various countries around the globe but ultimately these authors came to the conclusion that due to the vast differences in what is considered illegal activities, such as China's lack of laws against child pornography and the United States' more than 40 laws that address various computer-targeted or assisted crimes, a common legal framework does not exist for dealing with cyber crimes, criminals, and criminal organizations. Crime is determined by a legal framework but the world's legal frameworks are as different as its peoples. While an action may be a crime in the victim's location, it may not be a crime in the attacker's location. Even if they are in the same location it may be determined that the actions taken do not constitute a crime or that prosecuting the crime would add no value to society. The elements of cyber crime are too varied to list in relation to all the available legal standards that exist nationally and internationally. The lack of a common legal framework makes identifying a crime difficult and it is still an evolving topic; but, much like the conclusions reached by Kim et al. (2012), the lack of common criteria make it difficult to address crime due to the trans-national nature of connected technology. A crime is determined by the law of the land and because each land's laws differ or may not exist at all it is difficult to determine the nature of some cyber attacks as criminal actions. Since the criminality of an action is difficult to determine a framework must exist for addressing the complexities of jurisdiction and extradition.

Determining which standards are applicable to a cyber attack is complicated. Urbas (2012) conducted a review of laws in light of criminal activity in order to determine a common framework for jurisdiction and extradition since, "cyber-crime knows no borders" (p. 1). Urbas (2012) discovered two limiting issues: the anonymity of an attacker makes it difficult, if not impossible, to determine the identify of an attacker to meet the burden of proof; and, an action must be considered a crime in both jurisdictions, the victim's and the attacker's, in order to prosecute offenders for crimes committed across borders. Crime is a complex topic, made more complex by the transnational potential of cyber-criminal actions, with jurisdictional complications made more complex by the limitations of current technology to accurately determine an attacker. If an attacker performs an attack from Australia and it results in a crime in the United States, such as identity theft or child pornography, as referenced by Hu et al. (2013), and it is a crime in both jurisdictions, then it is likely that the attacker, if they can be identified, will be prosecuted by the United States if extradition is sought. However, if the attack is not a crime in Australia, it is unlikely that the attacker could be forced to face the justice system of the United States. Anonymity is one of the greatest weapons in an attacker's arsenal which prevents their identification and therefore prosecution for their actions; and, the double criminal standard makes it difficult to go after attackers in many jurisdictions. In relation to the global potential of cyber crime the best frame of reference for determining the legality of an attack is to evaluate the laws in all jurisdictions but the anonymity of skilled attackers makes their identification difficult further hindering prosecution of criminal attackers. The scope of cyber crime is global and while a global solution does not currently exist the evaluation of attacks based on a doubly illegal standard is a valid framework for classifying attacks if an attacker can be accurately identified. These issues related to the question of crime and jurisdiction are not as problematic when the attacker and the victim exist in the same geopolitical area.

However, even when limiting the review of criminal activity to the United States there are still many issues regarding identifying and prosecuting cyber criminals. Hanser (2011) conducted a study on the evolution of technology crimes in the United States committed by criminal organizations such as gangs and law enforcement efforts to collect, analyze, charge, and prosecute offenders, and he concluded that law enforcement must be prepared to handle digital evidence and evolve their investigative techniques to address the evolution of street crime to cyber crime. Criminal organizations are effectively exploiting vulnerabilities in law enforcement methods to escape punishment through the use of cyber-criminal activities as many law enforcement officials are ill equipped to process digital evidence. A criminal organization may pass secret messages through digital communication mediums such as websites, email, or mobile devices that may contain evidence of traditional criminal activities or criminal organizations may use a computer in the commission of a crime such as identity theft. While the criminal attack using technology is committed by a criminal in clear violation of laws, it is also important to note that law enforcement can also be considered a malicious attacker, from a certain point of view, in disrupting criminal activity and extracting digital evidence. There is still much to be evaluated in the area of cyber crime to address gaps in the empirical research. The purpose of an attack may be to commit a crime by criminals or to collect evidence of criminal activity by law enforcement. There are many gaps in the area of information security attacks for criminal or law enforcement purposes.

These gaps in criminal purposes for information security attacks make it difficult to relate this complex subject area to information security incidents. Hyman (2013) conducted interviews with expert information security professionals on the topic of cyber crime and many of these experts indicated that due to failures in reporting, self-selection bias, no standard mechanism for accounting, and undetected losses, a trusted non-government organization be used to conduct future research; however, some of the participants vehemently stated that this was an issue best left to the police. There are gaps that exist in the identification and reporting of criminal activity that lead to failures in accurate research into the issue but conflicting opinions raise a valid question of authority and responsibility when dealing with cyber crime. If a data breach is detected in one company it may be reported as a loss internally but not externally or it may even be determined, based on the regulatory requirements for notification, that no notification is required. Since organizations often do not report information security incidents, as previously mentioned, the collection and analysis of this data is limited to publicly disclosed information security incidents or organizations that are willing to cooperate with industry organizations performing research in this field. But despite issues in reporting disagreements exist between experts on which organizations have the authority and responsibility to coordinate in this field (Hyman, 2013). Cyber crime is a major factor in modern information security and it is important to organizations but how big a factor, how the information can be used, and who should use that information are still questions that are not clearly answered in the existing research. Cyber crime grows at a fast rate making it difficult for researchers to remain current on new developments.

Cyber crime grows at such a rate that many developments have yet to be researched in scholarly articles. In an unprecedented recent crackdown on cyber crime, as reported by CNN reporters Perez, Prokupecz, and Cohen (2014), law enforcement officials made over 90 arrests in 300 searches in 19 countries related to uses of cyber-crime remote access tool Blackshades. Criminals can purchase and deploy Blackshades with little technical skills, provide feedback to improve the product to Blackshades' paid employees, and become a part of a community of hackers improving their skills. The Blackshades software is a disturbing problem for law enforcement as it is a commercial off-the-shelf product that can be used to commit a variety of malicious computer crimes without having to have the technical skills to hack a computer. Even the crackdown by law enforcement, while unprecedented in its success, resulted in the arrests of less than one third of their targets primarily due to early warnings issued from within the Blackshades community. Remote-access tools such as Blackshades are installed via malware on unsuspecting machines and allow the attacker to capture screens, passwords, messages, and even turn on the web camera remotely. All of these actions are used in the commission of crimes such as blackmail, identity theft, and fraud. These reporters relate several important elements such as the low technical skill required to commit cyber crime that the cooperation of law enforcement is improving but still poorly equipped to address the issue that there is a business of creating and selling software to commit crimes and that hackers warn criminals of investigations via worldwide communities on the Internet. There are many gaps in how cyber crime is identified and prosecuted and these reporters relate several of these gaps as well as identify concepts missing in current scholarly literature as this topic develops faster than researchers can perform research. This real-world event demonstrates the ease of cyber crime and the presence of criminal hacker communities which both present potential future research topics. Cyber crime is one of many complex social issues related to the people element of information security.

While there are still many gaps in the field of cyber crime, some elements can be clearly identified in existing literature. Cyber crime is not a method of attack but the purpose behind an attack; however, disagreements between researchers and nations on the determination of cyber crime, which organizations have the authority and responsibility to respond to cyber crime, and how they respond to cyber crime make this a complex issue. Despite these gaps this field is still important to understanding attackers and their methods which is important to information security ontology and may yield practical benefits in both the defense of assets against cyber crime and assisting law enforcement in attacking criminal assets. For example, the techniques used to commit identity theft are unique and identity theft is generally considered a crime and identifying these techniques and therefore the purpose of the attack may assist defenders in countering an attack and focus law enforcement response. While there are still many unidentified elements about cyber crime the important element is its relationship to information security.

Therefore, it is important to identify this purpose for attacks as it may provide information for the defense of assets or the response by law enforcement. While a relationship clearly exists, the strength and value of that relationship still needs to be tested by further research. Criminal motivations are only one potential reason for attacking assets.

Cyber War

Another purpose for an information security attack is to perform an act of war. Gervais (2012) performed an extensive review of the international standard known as the law of war in relation to potential cyber war actions and determined that a technology attack must be equivalent to a traditional attack to be a cyber war attack, which is also in accordance with Article 51 of the United Nations charter; but, counter research, such as a study performed by Rid (2011), concluded that it is not possible to meet the standard of war using only technology. Current international standards set the threshold to determine the extent of a technology-only attack based on the principle of equivalency but because no cyber attacks have met this threshold as of this writing so there is some disagreement about the possibility of cyber war. As previously mentioned, Stuxnet is a computer virus created by state-sponsored organizations to attack a target in a foreign nation but despite this being labeled a cyber weapon it does not meet the standard for equivalency and therefore did not constitute an act of cyber war. The current standard for cyber attacks is based on traditional warfare and if a cyber war were ever unleashed it would currently be subject to the same rules. The concept of war is complex and the inclusion of IT into this has created a new debate regarding the potential to weaponize information platforms but it is possible to perform an attack for the purpose of making or supporting war. Equivalency is the guiding principle of current definitions of cyber war in relation to cyber-only attacks. Attacks committed and targeted at computers are only one possible application of technology in an attack.

Technology has been incorporated in nearly every aspect of modern life including modern warfare. Netcentric warfare is the term used to describe modern war's marriage of technology and traditional military weapons and strategy, such as the use of DDoS attacks during military invasions to disrupt communications, the use of technology in drones and bombs, and even the increased knowledge management for improved intelligence collection and dissemination using websites, according to a review of modern military strategy by Arquilla (2011). The inclusion of IT into warfare has changed the way wars are fought to the point of relying on and exploiting technology in support of or in conjunction with traditional military operations. During the American invasion of Iraq DDoS attacks were used to disable Iraqi communications systems to prepare for ground troops and provide digital cover for air support (Arquilla, 2011). These technology-assisted attacks are unique in that they incorporate direct physical consequences, whereas other cyber attacks are limited to the digital world. Cyber-assisted or cyber-targeted war, similar to cyber-assisted crime or cyber-targeted crime, are complex integrations of elements of the digital and physical realms that make dealing with these situations difficult at best as this hybrid phenomena is still being researched. IT has become integrated into war and this integration has created a strong need for information security in the protection of military assets and to support military actions. However, war is not limited to the military.

Military and government organizations are not always the targets of acts of war. Lobel (2012) conducted a study on the implications of cyber war on civilian organizations and critical infrastructure and determined that non-military and government targets are at a very high risk and as such should incorporate active defense to disrupt malicious signals. Non-military and non-government organizations are potential targets during traditional war, and the same seems to hold true for cyber attacks for the purpose of war, but one potential method of deterrence is to conduct active defense to disrupt malicious signals. China has been frequently accused of hacking many American systems, including government contractors, in order to steal information on advanced weapons platforms as it is easier to target the contractor than military systems (Lobel, 2012). It is important to note that these types of attacks for the purpose of war are not confined to military and government targets. Therefore, civilian organizations may be targeted during war but despite the author's suggestion of active defense it is still unclear where the authority and responsibility of information security lies in the event of a coordinated cyber attack for the purpose of war. This concept of civilian targeting is a new area that requires further research to evaluate the potential of models such as active defense theory. All types of organizations may be targeted for the purpose of war but additional research is required to determine the authority and responsibility to act in this situation.

While there are other gaps in current literature on cyber crime, there are many more gaps in the literature regarding cyber war. There has never been a cyber war at the time of this writing and therefore many aspects of the military potential of computers are unknown or at least unpublished outside of the military. It is clear that the potential exists for cyber-only attacks to be used to make war or to support war and that the integration of IT into warfare has evolved the way humans kill each other. The strategic value of controlling information in a military conflict is high and often that information may not only be controlled by the military but by the military industrial complex. As previously mentioned, Cobb (2011) indicated that attacking Internet Service Providers (ISP) would severely impact the military's ability to keep command and control. ISPs are not military commands and therefore these issues are important for more than just the purpose of military on military attacks. However, due to the limited information available in this field due both to the lack of empirical evidence and potential national security impacts very little can be said other than that it is possible and important.

Research Literature

The research method chosen for this study was qualitative phenomenology. Creswell (2012) wrote extensively about the epistemology and ontology of qualitative methods, including phenomenology, as well as the methods and procedures for qualitative research, which share several common assumptions including that some phenomena cannot be quantitatively observed and measured. While there are a multitude of qualitative methods with various strengths and weaknesses they all share a common foundation. It is not possible to measure how an information security incident is detected or why it was dealt with in a specific way but qualitative research methods allow researchers to explore a complex phenomenon and how it interacts with people. Many of the elements of qualitative research vary according to the various types and methods of qualitative research but the important elements related to method selection include the assumption that the question cannot be observed and measured. The research problem of this study indicated that a gap existed on the methods and procedures related to information security management and that these concepts cannot be measured and evaluated in a quantitative manner, so in accordance with the relevant literature on research, a qualitative method, specifically phenomenology, is appropriate for this study. The method of a research study is an important choice that must be an informed decision that fits the research problem and can answer the research question; and, in this instance, a qualitative foundation is an appropriate method.

However, there are many types of qualitative methods, including phenomenology, that were considered while reviewing the literature.

There are many types of phenomenology approaches that impact how information is processed during the study. Giorgi (2009) wrote extensively on descriptive phenomenology and its merits, processes, and procedures in relation to psychology in which several important elements of phenomenology were established including instruments, measurements, and processes, which are reinforced by more recent works such as the writing of Van Manen (2014), which were focused on the theoretical establishment of creative phenomenology methods. Phenomenology is a research process that is focused on the unique lived experiences of participants using creative methods and processes to collect and analyze data. Phenomenology as a concept can be applied to research in the collection of unique experiences in relation to a common phenomenon thus establishing relationships between people and the world around them. There is no one way to conduct phenomenology research, as described by these authors and their reference materials, but many different and creative approaches to problem solving that all share common elements such as lived experiences, establishing an epoche for the researcher, and phenomenology reduction. These various elements are uniquely suited to answering the research question and addressing the research problem as a qualitative method that allows researchers to expand upon phenomenon by evaluating the experiences of individuals as described in these reference materials. The ideas presented by these authors are important as they establish the many elements of modern phenomenology research. These concepts and other important elements in relation to methodology are covered extensively in chapter 3 of this dissertation.

Summary

In chapter 1 the research agenda for this dissertation is introduced along with an argument for considering aspects of empirical information security incident management. The literature review provides an overview of the academic research available on this topic focusing on the elements of information security. Since information security is a highly connected field this review covered a variety of topics. After reviewing the recent literature on information security the researcher determined that there were several missing elements. Based on the information security ontology the preventive defense of systems is very well researched. However, there are gaps in the literature regarding information security incident management including investigation, containment, and recovery as well as gaps in understanding the methods, sources, intentions, and purposes of attackers. Literature on research methods was also reviewed in order to establish an appropriate method for conducting research into this topic area. The remainder of this study addressed the research methods, analysis, and resulting conclusions. The next chapter contains the research methodology for addressing these gaps.

CHAPTER 3. METHODOLOGY

Introduction to the Methodology

In chapter 1 an overview of this research project was presented; which, included a brief description of the methodology. In chapter 2, the existing literature was reviewed to determine the gaps and to validate the need for additional research. Within this chapter the method of inquiry used in this study is described in detail. This qualitative study was performed using phenomenology to explore the lived experiences of information security staff. In this chapter the details of this methodology are presented including the research design, sample, sample methods, and sample procedures, data collection, instrument design, measurements, and data analysis methods. The validity and reliability as well as ethical considerations are also discussed in this chapter.

Research Design

The goal of this research was to understand the experiences of information security professionals who have responded to information security incidents in the private sector. In order to accomplish this goal a specific research design was developed. There are two major dividing lines between research methodologies based on the ontology and epistemology of each method. Ontology and epistemology are concerned with the development of theories describing forms, modes, and views of the world from various viewpoints (Herre, 2013). These concepts describe what we can know and how we can know it. The positivist quantitative methods allow researchers to address questions through objectively observable and measurable facts and figures such as statistics (Dayton, 2011). This view of reality is absent the observer. However, this approach would not be appropriate for this research design as the goal is to understand the experiences of a specific group of observers.

Qualitative methods provide a different approach. The ontology and epistemology of interpretivist qualitative research methods is in the study of the impacts of observer observations, measurements, and experiences on the human condition (Van Manen, 2014). Qualitative research methods are useful for evaluating experiences, emotions, decisions, and other non-numeric data. This view of reality is based on the observer and how they interact with the world. This type of inquiry relates to the goal of this study which was to understand the experiences of information security professionals. The research design of this study was designed to expand this field through the examination of experiences.

The methodological approach for this study was a qualitative approach. This methodology was selected as it would allow the researcher to address the proposed problem statement. However, there are many types of qualitative techniques such as case studies which are based on observations within a specific instance, grounded theory studies which derive theory from observations, and phenomenological studies which examine the lived experiences of participants (Creswell, 2012). These various types of qualitative research designs each have strengths and weaknesses. However, phenomenology is the best choice for examining the lived experiences of individuals. Thus phenomenology is the most appropriate for reaching the goal of this study.

As there is little knowledge of the lived experiences of IT security professionals performing information security incident management in corporate organizations a qualitative study was appropriate. A phenomenological research design was used to gain a better understanding of the perceptions of individuals who lived the experience. The methodology approach for this study was rooted in phenomenology as the goal was to explore the experiences of IT security professionals performing information security incident management services for private organizations. Phenomenology is centered on relating first-order effects to second-order theories through the lived experiences of participants (Van Manen, 2014). Empirical phenomenology is an appropriate methodological model for this study. Establishing the experiences of the target population allowed the researcher to provide an answer to the research question and address the gap in existing literature.

The phenomenology method was suited to answering the research question as an inductive qualitative approach by providing the researcher with a guided path in order to examine the experiences of experts in the target field; thus, achieving a deeper understanding of the phenomenon. The utilization of a creative qualitative phenomenology approach provided a mechanism for the collection and analysis of the experiences of information security professionals conducting information security incident management. There is no exact method to phenomenology (Van Manen, 2014). However, using a creative mixture of phenomenology approaches allowed the researcher to focus on the unique experiences of participants. Phenomenology is based on the assumption that reality for an individual is based on his or her unique experiences. This research design allowed the researcher to address all the major points of the research question.

Sample

The target population of this study was selected in order to answer the research question. The target population of this study was IT security professionals providing information security incident management to corporate organizations. The data obtained from these individuals during the interview process served as the primary data. The target population was very large and without additional criteria to set the sample frame the scope of this project would have been unmanageable. Criterion sampling is a process of selecting samples based on select criterion (Suri, 2011). Criterion sampling, based on the years of experience in information security as well as the other inclusion and exclusion criteria, was used to select study participants. This ensured that the most data-rich participants with a history of lived experiences were selected to become participants in the study. The sample frame consisted of three qualification sets. Set one participants were IT security professionals with at least 10 years of experience in information security and no recent experience within the past five years directly supporting military, government, or law enforcement agencies. Set two participants were IT security professionals with at least five years of experience in information security, a bachelor’s degree or higher, and no recent experience within the past five years directly supporting military, government, or law enforcement agencies. Set three participants were IT security professionals with at least five years of experience in information security, a professional security certification, and no recent experience within the past five years directly supporting military, government, or law enforcement agencies.

Individual participants were recruited from the Pacific Northwest region of the United States. This region is home to many prominent technical organizations with a history of innovative information security practices. The high volume of potential participants in this area with various experiences and approaches to information security incident management helped to ensure diversity in the study. Interviews were conducted with 20 IT security professionals within the sample frame over the course of this project. Professionals were recruited from professional websites such as LinkedIn, online bulletin boards, solicitation during professional gatherings, and bulletin boards at local establishments. The objective of the researcher was to reach data saturation on the target issue. Data saturation is the point when all relevant experiences have been considered on an issue (Walker, 2012). Additional participants were to be used only if additional experiences were required to reach the saturation point on this issue. Additional participants were to be selected as needed and the process would have continued until data saturation had been reached or there were no more available participants in this sample; however, this was not required in order to reach data saturation.

The selection procedures and sample size were consistent with the research method as well as federal and school guidelines. Utilizing a criterion selection procedure to identify participants within the sample frame allowed the researcher to directly address the target population referenced in the research question. A small sample size was appropriate for this type of study, phenomenology, in order to concentrate on the depth of experience of participants (Giorgi, 2009). The sample size reflects the intended scope and size of the research study. This sample size is comparable to recent research studies (Angwenyi, 2014; Cane, McCarthy, & Halawi, 2010; Rozendaal & Schifferstein, 2010). These processes were appropriate for this study. Because this issue had the potential to generate diverse experiences additional participants were to be recruited if saturation was not reached within 20 interviews. This sampling method used nonprobability, criterion, and convenience sampling methods. Participants were purposefully selected based on established criterion within a region convenient to the researcher.

The researcher commenced an initial recruitment effort by identifying and targeting professional information security membership organizations, online forums, and local clubs. These organizations and places were likely to be frequented by the target population and worked as an effective means of recruitment for this study. Combined, these efforts had the potential of directly reaching many individuals of whom a few hundred may have been eligible to participate in this study. Limited information regarding the nature of the study was made available to solicit interest. In each case potential participants were provided a pre-screening questionnaire.

The initial questionnaire included a statement that all questionnaire respondents' responses were to be kept confidential and that response to the questionnaire did not necessarily mean they would be selected to participate in the research study. Upon communication from a potential participant that they would like to participate in the study a pre-screening questionnaire was sent to the interested party. This questionnaire was designed to capture basic information about the potential participant to ensure that the appropriate criteria were met for this study. The pre-screening questionnaire focused on gathering important information including:

- age
- race
- gender
- employment status and history
- education level
- professional certifications
- years of experience in information security
- years of experience in government, law enforcement, or military organizations

This information was used to determine if potential participants met all requirements for inclusion in this study. Once the responses from the recruitment effort were received they were assessed for inclusion as potential participants. They were assessed based on the established inclusion and exclusion criteria of the study to ensure that they were eligible based on the sample frame.

At the conclusion of this period of recruitment eligible participants were assigned a participant identification code. Upon selection, each individual was contacted to set up an interview. The interviews were held in a variety of public places for the safety, privacy, and convenience of the researcher and participants. As an alternative to those who were not local or did not feel comfortable discussing these issues in a physical place Skype was used as an alternative. Upon selection, each individual was also provided with the informed consent document. Additional eligible participants beyond the initial 20 were to be grouped into additional ranks of ten to be used only if saturation was not reached within the initial group. However, this was not needed. The specific inclusion and exclusion criteria are listed below.

Inclusion Criteria

In order to be included in this study participants met at least one of three qualification sets. Set one participants were IT security professionals with at least 10 years of experience in information security and no recent experience within the past five years directly supporting military, government, or law enforcement agencies. Set two participants were IT security professionals with at least five years of experience in information security, a bachelor's degree or higher, and no recent experience within the past five years directly supporting military, government, or law enforcement agencies. Set three participants were IT security professionals with at least five years of experience in information security, a professional security certification, and no recent experience within the past five years directly supporting military, government, or law enforcement agencies.

To ensure that participants had at least some experiences within the subject area of the study an experience requirement was included as part of the inclusion criteria. As an alternative qualification participants could also have qualified using either a college or advanced degree or an industry security certification. This qualification was included to ensure participants had the required knowledge to communicate their experiences. Potential participants were prioritized based on the number of years of experience in information security. These requirements were important to establishing a good set of data rich participants.

Exclusion Criteria

In order to mitigate biased views of information security incident classifications the pre-screening questionnaire asked individuals about past government, military, or law enforcement experience. Those indicating an affirmative response to this question within the last five years were excluded from participation in the study. Professionals working in these environments have unique experiences that are unlike those of civilian counterparts (Dawley, 2013). Thus they likely would have had a bias toward a specific identification strategy due to their work environment. These individuals may also have sensitive information that should not be disclosed in unclassified research projects. Thus for these three reasons scope, bias, and national security, those with recent government, law enforcement, and military experiences were excluded. The researcher also excluded potential participants from her current and previous places of employment in order to avoid any potential ethical issues.

Instrument Design

Through the use of interviews the researcher explored the individual experiences of each participant in relation to the research question. Using established questions helps researchers to remain focused and not to guide the direction of the interviews (Giorgi, 2009). The framework established by the researcher for these interview questions was approved by field testing with industry experts and academic boards. These questions elicit both information and opinions. The semi-structured nature of this framework allowed the researcher to explore additional areas as necessary in each interview.

Interview Questions

Demographic questions.

- What is your gender?
- What is your age?
- What is your race?

Qualifying questions.

- Have you recently, within the past five years, worked in any capacity with government, law enforcement, or military organizations in information security?
- Do you have experience responding to information security incidents?
- Do you have experience as a penetration tester?
- What is the highest level of education you have completed?
- What is your current job title and responsibilities?
- How long have you worked in this capacity?
- What is your organization's industry? Examples include software development, manufacturing, finance, health care, etc.
- If you have worked in this capacity for less than six months what was your previous job title, responsibilities, and length of employment?
- How many years of experience do you have responding to information security incidents?
- How many years of experience do you have performing penetration testing?

- How many years of experience do you have in IT security?
- How many years of experience do you have in IT?
- Which industry certifications do you hold?

Icebreaker questions.

- On a typical work day what types of information security tasks do you perform such as scanning systems or reviewing logs?
- What are some of the challenges you face while working in this position related to information security?
- What is your role during information security incidents?
- What is your organization's procedure for identifying and addressing potential information security incidents?
- How do you define an information security incident?
- How often did you / do you need to respond to information security incidents?
- What training have you received to deal with information security incidents?

Incident question.

- How did you respond to this information security incident?
- What steps did you take to detect and identify the incident?
- What criteria did you use to classify this information security incident?
- What was your decision making process and what were some of the factors that influenced your response to this information security incident?
- Once the incident was identified how did you respond to the incident?
- What issues, if any, did you discover during the course of responding to the incident?
- At what point did you, or your supervisors, declare the information security incident closed?

- What actions did you take to remediate discovered vulnerabilities?

- What, if any, compliance standards did you discover to have been violated during incidents? Of these violations were any noted as acceptable risks to the organization?

- Did you conduct any additional procedures or investigations into the incident following its closure?

- At any time during this incident did you work with any outside organizations such as law enforcement or security firms on this incident?

Based on your experience.

- How strictly were the processes and procedures put in place by the organization prior to these incidents followed?

- How much freedom did you have to deviate from standard procedures when responding to incidents?

- Are there any changes in processes and procedures you would recommend for responding to information security incidents?

- Do you feel the processes and procedures for responding to information security incidents were effective?

- How did you feel about the incident classification procedures used during this incident?

- What kinds of support and training do you wish you had to better respond to information security incidents?

Penetration testing questions.

- What vulnerabilities did you exploit to gain access to the system?

- What actions did you take after you gained access to the systems?

- Did you take any actions to hide or mask your presence in the system?

- How did the defending team discover the incident?

- Did the scenario continue after the incident was discovered?

- Did you take any steps to hinder the incident response process during the penetration test?
- What was your decision making process and what were some of the factors that influenced your actions during this test?
- Once the intrusion was identified how did you respond?
- Did you discover any additional issues while exploiting the targeted vulnerability during this test?
- What, if any, compliance standards were discovered to have been violated during these tests? Of these violations were any noted as acceptable risks to the organization?

Data Collection

The primary data collection instrument used in this study was the set of interview questions. Data was collected over the course of three months in the second half of 2014. The interview questions were semi-structured and open ended in order to facilitate free exploration of the participant's experiences on the target issue. Interviewing as an instrument of data collection is appropriate for a phenomenology study (Creswell, 2012). A set of standard questions including questions for demographics, qualifications, experiences, and expectations were asked of each participant; but, additional questions were developed over the course of each interview. The standard set of questions was field tested prior to data collection by a panel of industry experts. Each of the field-test participants had the required qualifications for inclusion in this study but were excluded for various reasons such as geographic location or work history. The experts all agreed that the questions were appropriate for this study but recommended some structural and grammatical corrections.

The interview questions consisted of several sections including questions related to the participant's demographics, qualifications, icebreakers, information security incident experiences, information security incident observations, and penetration experiences. The demographic information collected in this study was collected in the event that certain patterns emerged based on age, gender, or race. This information was used to either clarify or to dive more deeply into a topic. In addition to demographic information qualifying information was also collected on each participant. The information in this section was collected and used primarily to establish each participant's qualifications to participate in the study. Questions included work history, education history, and certification history. These first two groups were covered with individuals during a pre-screening interview and addressed again during the in-person interview.

Before each interview, the researcher gave participants time to read consent forms and to ask any questions about the form or the process. Each interview lasted approximately 90 minutes. The interview process began in each instance after recapping the pre-screening answers with icebreaker questions. These questions were designed to explore general experiences in IT security and management and to place the participant at ease. These questions established the pace of each interview. Once each individual had answered these general questions specific information security incidents were explored. This section directly addressed the research question and the bulk of data collected was collected during this part of the interview process. Each information security incident was explored focusing on the participant's own experiences.

After each participant's collective information security incident experiences were explored some questions based on these experiences were presented to participants. While these questions were not designed to explore their lived experiences they provided interesting insights into each participant's observations and conclusions regarding the entire information security incident management process. In addition to the reactive defensive side of information security incidents participants that revealed experiences in penetration testing were also asked to explore these experiences. These experiences provided additional data on information security incidents through experiences on the other side of the looking glass. This offered a unique exploration of the dual nature of information security.

Each interview was recorded using voice recording software and encrypted for future transcription. As a backup to this method physical recordings were taken via a hand-held recording device and securely stored in the researcher’s home. Notes were also taken during the interview process. Following the conclusion of each interview the researcher compared the recording and notes of each participant. The recordings and the notes were then transcribed into a single document. Once completed the document was reviewed to ensure that sensitive information was removed in order to protect the operational integrity of organizational systems. Then the document was presented for the participant to review. Each final document was validated by each participant to ensure the accuracy of the transcript and that no confidential information remained before analysis or publication.

Instrumentation/Measures

The experiences of individuals cannot be measured quantitatively. The unit of measure for this study was the individual descriptions of information security incidents confronted by participants. The primary source of data in a phenomenology study is typically the experiences of participants (Flood, 2010). Thus, these experiences were the only source of data for this study. The experiences related to the key constructs of this study were reported by individuals with direct experience providing information security incident management services to corporate organizations during information security incidents.

These experiences and the concepts discussed by each participant, such as the process of identifying information security incidents or the procedures for addressing each information security incident, cannot be objectively measured. These concepts also cannot be physically observed ethically in a controlled environment. To cause information security incidents in order to observe reactions would compromise operational systems and the limitations of controlled lab environments cannot replicate the complexity of responding to real-world information security incidents. Real-life experiences are unique and invaluable to understanding the key constructs of this study. Participants were asked to share their experiences in information security incidents and their processes for addressing dilemmas in the field. This information was collected as the primary source of data. These experiences were analyzed using an appropriate phenomenology model.

Data Analysis

The methodological approach selected for this study was structured around principles from multiple phenomenological sources that were used to create a unique creative phenomenological method. Phenomenology has many different forms and methods and phenomenologists have many outlooks on experience and how experience can be captured and analyzed (Van Manen, 2014). Each of the various phenomenology models addresses unique aspects of the overall method of phenomenological research. Phenomenology models are designed to describe rather than explain experiences (Creswell, 2012). The focus of phenomenology is on the lived experiences of participants. The experiences, when analyzed, form a structure that reflects the essences of the phenomenon experienced. The selected phenomenological method consisted of three actions: the epoche, the phenomenological reduction, and the search for essences.

The first analysis method used in this project was the epoche as described by Van Manen and influenced by Heuer. The epoche is designed to identify and bring to light elements of the researcher (Van Manen, 2014). This identification phase provided the researcher with an opportunity to clearly identify her own experiences and views in order to set them aside during further analysis. This clear identification of the researcher's experience helps to ensure that the researcher is aware of bias when considering alternative viewpoints, cultures, and experiences (Heuer, 1999). Based on the criteria used for this study the researcher was not eligible to participate due to her recent experience in government and military service. However, her experiences in information security incident management could still have had an influence on her analysis. Documenting these issues allowed her to set them aside and then to review them to ensure that they did not influence the analysis of participant experiences. This prepared the researcher to approach the collected participant experiences with a fresh outlook and an open mind.

The second analysis phase was the phenomenological reduction. This was the primary analysis phase of the research project. The phenomenological reduction is a two-part process of deconstruction and reconstruction that is used in order to identify meaningful units and themes (Van Manen, 2014). The reduction and breakdown of unique responses into coded themes allowed for the reconstruction of the data during further analysis. Analysis of the data started by deconstructing the data and identifying discrete units of meaning related to the phenomenon being studied. Each individual participant's experiences were deconstructed and coded. These coded responses allowed the researcher to easily compare and note the similarities and differences in each participant's experiences.

These reduced elements were then reconsidered in respect to the whole. A holistic review of the data was conducted in relation to all of the experiences recorded. Reconstruction is the process of examining each individual experience in relation to the whole (Van Manen, 2014). This shift in perspective built upon the reduction performed in the first step and allowed the researcher to put each element in context in the larger data set. Themes were noted and highlighted in each individual experience in the reduction and analyzed in relation to all the experiences in the reconstruction. This researcher then synthesized the units of meaning together in order to reveal a structure that clarified the phenomenon. This two-step phenomenological reduction promotes a deeper understanding of the experiences of each individual as well as the experiences of all participants.

Finally, the data collected in the phenomenology reduction was used to generate understanding and to answer the research question. This final review of the data is termed the search for essences. The search for essences is designed to synthesize meaningful units and themes gathered during reduction into understanding unaffected by the researcher's perspectives (Giorgi, 2009). It is in this manner that the impressions and themes developed were linked to supporting data. Once these links have been forged, the researcher, following a suggestion from Van Manen (2014), returned to the raw data to look for variations in the data. The researcher reviewed these essences one final time in relation to the raw data to establish relationships between the essences and the data. These newly discovered essences directly addressed the gap in the research by identifying the common themes and actions taken by IT security professionals in information security incident management. These various iterative reviews of the data led the researcher to logical conclusions based on the real-world data.

Validity and Reliability

There are several factors that were taken into consideration to improve the validity and reliability of the research project. Factors such as researcher bias, methodological errors, analytical errors, and procedural errors were mitigated in order to protect the validity of the study. Phenomenological analysis is subjective and therefore perceptions and biases may impact the validity of any improperly conducted phenomenological study. The inclusion of the epoche as a process for bracketing these preconceptions and biases mitigated this risk to the validity of the study. The validity of a phenomenology study may also be threatened by improper procedures and mismanagement. However, the procedures and methodology in this study were reviewed and considered by many individuals to be acceptable throughout the approval process prior to performing any data collection or analysis. Descriptive validity was protected through the careful analysis of interview recordings, notes, and transcripts. Each of the items used in the analysis of collected data was reviewed by the participant to endure the validity of each transcript. Interpretive and construct validity was increased by field testing the interview questions. These concerns and mitigations all addressed potential impacts to the validity of the study and contributed to the successful completion of this research project.

The reliability of the data collected is subjective. The nature of qualitative phenomenological studies is that the researcher is dependent upon the participant to be forthcoming and honest about experiences. Due to the anonymous nature of the study it was not possible to confirm each individual's credibility and trustworthiness. This would have required validation from professional certification organizations, educational institutions, and employers which would have violated their privacy. The criterion for judging the credibility, trustworthiness, and confirmability of interview data was based on reaching a point of data saturation. Reaching the point of data saturation on the topic ensured that data not matching the larger sample was isolated. Since the validity of the study as well as the reliability of the study were high the results of this study should be a fair indication of experiences across multiple industries.

Ethical Considerations

The ethical concerns for this research were minimal. One of the ethical concerns of this study was researcher bias. Bias cannot be fully eliminated from research (Simundic, 2013). The methodology and procedures for this study were closely and heavily scrutinized by various third parties prior to performing any data collection. These extra checks provided ethical protections against any bias by the researcher. The researcher did not use any prior knowledge as an information security professional to influence any responses during the research study. The researcher was not studying any group of people over whom the researcher would be able to exert coercion or undue influence. The criteria for the sample frame was clear regarding participant selection for the study. There were no conflicts of interest in the selection of participants.

The population targeted did not consist of any protected groups or groups that were involved in national security. The researcher was respectful and responsible with participant information at all times. Participants were identified by number in all reference materials, interviews, and transcriptions. Non-disclosure agreements with all participants were signed in order to clarify the reportable elements of their experiences to protect operational security concerns. All digital materials were encrypted. As a means to ensure confidentiality and anonymity, participants' personally identifying information was kept anonymous. Identifying information such as name and address, the participant organization, or other unique identification was excluded from transcriptions if provided during the interview process to protect anonymity and confidentiality. Sensitive data, such as data indicating an open vulnerability or a clearly identifiable client, was not reported in the results. This data was scrubbed during the transcription process and further reviewed by participants to ensure that all the information was correct and publishable. This process ensured that participants were protected from misrepresentation and helped to ensure the privacy of sensitive data. All participants were treated equally. No incentives or other tangible benefits were made available to participants as a result of this study. All individuals who participated in this study did so with informed consent and on a voluntary basis. Participants had the option to withdraw at any time.

There were ethical considerations regarding the researcher's competence including considerations under the ethical principles of the American Psychological Association (APA). The APA standard directs researchers to conduct research within the boundaries of their competence (APA, 2010). This standard requires the researcher to obtain training, experience, and supervision. The researcher had completed extensive academic training and passed examination prior to conducting this research. This training also included modules on ethical considerations for various standards. The researcher was also experienced in conducting research academically and professionally using various models. The researcher worked with her mentor and a committee throughout this research project. While the researcher's work is her own she was not alone during this project.

CHAPTER 4. RESULTS

Introduction

The purpose of this phenomenological study was to understand the experiences of corporate-based IT security professionals providing information security incident management services and to use those experiences to contribute to the body of scientific knowledge in the science in warfare, criminology, and IT. In chapter 1 the researcher provided an overview of the project and why this topic deserved further review. An extensive literature review was conducted for chapter 2 in order to document the existing research in information security incident management. In chapter 3 the research methods were presented by the researcher. The intent of this chapter is to document the steps taken by the researcher to collect and analyze the research data.

The sections of this chapter include a detailed description of the researcher's role and background as the first stage of phenomenological analysis. Following the epoche a detailed description of the sample is provided including a demographic profile of participants. A summary of the data collection methods used in the study is presented followed by the phenomenological reduction of the data. The reduction of the data concludes with the establishment of the essence of the phenomenon. These essences will be used to address the research questions in chapter 5.

Restatement of the Problem

How information security staff respond to information security incidents in private organizations is not fully known. Various elements of potential response methods have been researched but a coherent holistic response process used by information security staff had not been studied. Recent research projects have focused on preventive security measures and their effectiveness as opposed to reactionary security measures that are used when information security incidents occur (Amancei, 2011). Thus there were many unanswered questions regarding the unique response elements of information security. These unanswered questions could best be answered by exploring the lived experiences of information security staff. The research problem explored in this study was how information security professionals in private organizations articulate their experiences in responding to information security incidents.

Restating the Purpose

The purpose of this phenomenological study was to understand the experiences of corporate-based IT security professionals providing information security incident management services and then to use that understanding to contribute to several scientific fields such as IT, criminology, and even warfare. Each participant in this study was interviewed in order to discover the meanings they derived from their experiences managing information security incidents and how these experiences helped to shape their current information security incident response procedures. These insights into individual experiences provided a window into the impacts these information security incidents have on information security professionals and the companies they support. These new insights offer future researchers additional information on the significance of information security incidents.

Research Questions

The research into information security indicates that there is a gap in the literature. While there is a body of literature that addresses the management of information security incidents, the literature is primarily related to a subsection of preventive actions in private companies and some offensive actions in relation to law enforcement and military organizations; thus, leaving a gap in reactionary security measures. This gap in the literature indicates a lack of knowledge about the practical application of information security elements and technology decision making. Therefore, the main research question explored by this study was:

RQ1: What are the lived experiences of information security professionals in private organizations responding to information security incidents?

The research subquestions were as follows:

RQ1a. How does the identification of the source, purpose, and intent during an information security incident influence the responses of information security professionals?

RQ1b. How do information security incidents influence information security professionals preparing for future challenges?

RQ1c. In what way(s) do information security incidents influence the thinking of information security professionals with regard to information security attack frameworks?

RQ1d. How do external information security programs impact the response of information security professionals in private organizations with regard to information security incidents?

Epoche

The researcher is herself an information security professional in the Pacific Northwest with at least five years of experience in information security. The researcher has a Master's degree in information systems engineering with a specialty in information assurance and security as well as the Certified Information Systems Security Professional (CISSP) certification.

However, the researcher has also worked for the military as a Soldier and contractor as well as for other government agencies as a contractor over the past several years. The researcher has an extensive background in information security incident management including time spent as an incident manager for the military. Given this background the researcher brings to this study extensive knowledge and expertise as it relates to information security and the unique challenges of information security incident management.

However, this background may also serve to bias the researcher's analysis. As such the first element of the phenomenology method used in this study is the epoche. The epoche, as described by Van Manen (2014) and Giorgi (2009), is a critical process used to bracket the researcher's experiences in a way that maintains the objectivity of the researcher process and results. As a researcher evaluating the lived experiences of others it is important that the researcher's experiences do not cloud her judgment. This process is reinforced by methods developed by Heuer (1999) for intelligence analysis in which procedures for raising the awareness of intelligence analysts was a core component to preventing bias during intelligence analysis. Awareness is an important method to prevent researcher bias. This is especially important when the researcher has experienced the phenomenon that is being studied.

The following is a summary of the researcher's experience. Much like the original transcripts of participants the actual epoche process is filled with confidential information and therefore cannot be published in its entirety. As an information security professional the researcher has experienced various types of information security elements in government, military, and civilian organizations. The researcher started her professional career in IT in 2007 with the military as a contractor. In early 2011 she led her first information security investigation into an information security incident which ultimately uncovered the responsible party and restored the affected systems to working order. In 2012 the researcher spent several months designing, developing, and implementing processes and procedures for event management for a military organization. Currently the researcher is performing governance, risk, and compliance consulting.

In the researcher's experiences there were several common threads. In each information security incident detection was never accomplished with technical tools. Information security incidents were reported by users or administrators witnessing anomalous activities. In general, organizations have not developed the resources to respond to any information security incidents beyond returning systems to service. The only exception to this was the military organization which had the authority, responsibility, and resources to respond to attackers rather than just the information security incident. Even in these instances forensic investigations were never performed for the collection of criminal evidence. Due to the limited resources and immature processes and procedures at most organizations, with the exception of the military, there were no lessons learned from information security incidents as the vast majority of information security incidents never resulted in major breaches of protected data.

As a student the researcher has a history of working in this subject area. She holds a Master's degree in information systems engineering with a specialty in information assurance and security. The thesis research she conducted for the capstone requirement focused on preventive risk management which is a precursor to information security incident management (Burkhead, 2009). The process developed in this research project was evaluated by industry experts as a valid risk management framework. The researcher has also previously attempted to publish an article based on active defense. Active defense is a potential response plan for information security incident management that focuses on aggressive signal disruption (Brown &

Burkhead, 2012). This concept is one of several potential threat response procedures that could impact national security. This article was accepted for publication but withdrawn due to funding issues.

Based on the researcher's experience information security incidents from internal threat actors are more common than successful information security attacks from external threat sources. The policies and procedures that govern these actions are generally described and defined in federal regulation for some organizations. Organizations spend more time and resources preventing external threats than internal threats using preventive risk management. Information security incident response in private organizations is minimal and generally no prosecution occurs. Private organizations are not aggressive about information security incident response. These essences represent the researcher's unique experiences.

Despite the researcher's similar, although not identical, background with study participants and in-depth knowledge of information security incident management she resisted entering this study as a participant. The selection of this specific sample was designed to purposefully exclude the researcher in addition to the assumption that government, military, and law enforcement experience differs from private organization experience in information security incident management. As noted by Van Manen (2014) and Giorgi (2009) phenomenology is unique in the specific exclusion of the researcher's background and the emphases on preconceived notions. Phenomenology was selected as a research method to meet these specific criteria. The focus of this work is, and should remain, on the participants.

Description of the Sample

Participants in this study were recruited and selected based on the sampling method and criterion established in chapter 3. In research studies with small sample sizes, such as phenomenology studies, it is more difficult to mask a participant's identity characteristics (Creswell, 2012). All participant data reported in this study is reported in aggregate or under a participant identification number. Each participant is identified by participant identification number and no operational security information is used. A total of 26 candidates responded to the recruitment efforts conducted over social media, professional networking sites, and online message boards, as well as word of mouth. One of these candidates was deemed ineligible for participation based on information obtained in the pre-screening questionnaire. Based on results from the initial questionnaire a total of 25 participants were selected. Seven respondents were withdrawn from this study and did not participate. Three of them withdrew voluntarily and four of them were withdrawn after a long lapse in communication. A total of 18 participant interviews were conducted and all transcripts were approved for use in this study. Saturation was reached within the first ten interviews in regards to subjects related to the research question. It was not expected that including additional interviews in this study would improve or change the results.

Table 1. Recruitment Breakdown

	Responses received	Percentage
Recruitment Messages Sent	1144	100%
No Response	724	63%
Responses to Recruitment	265	23%
Completed Eligibility Forms	26	2%
Declined	26	2%
Ineligible	144	10%
Eligible Participants	25	2%

Demographics

The first three questions of the pre-screening questionnaire were designed to collect demographic information. This information was only to be analyzed if it was determined that a pattern existed that included these elements. The predominant race of participants was White and the average age of the participants was 44. All of the participants were Caucasian males, with two exceptions for Asian males. The only females who responded to requests for this study refused participation due to concerns regarding the confidentiality of reported information.

Table 2. Demographic Breakdown: Race

Race	Number of Participants	Percentage
Caucasian	24	92%
Asian	2	8%
Total	26	100

Table 3. Demographic Breakdown: Age

Age	Number of Participants	Percentage
18-29	2	8%
30-39	7	27%
40-49	10	38%
50+	7	27%
Total	26	100

Table 4. Demographic Breakdown: Gender

Gender	Number of Participants	Percentage
Male	25	100
Female	0	0
Total	25	100

Criteria

The eligibility criteria of this study was based on years of experience and either education or certification. The qualifying questions in this study were designed to evaluate each participant's experiences to ensure that the most data-rich participants were selected in relation to the phenomenon being studied. On average participants had 21 years of experience working with IT, 16 years of experience in information security, 6 years of experience in penetration testing, and 14 years of experience in information security incident management. Sixty-one percent had academic degrees with most participants having a bachelor's degree in a technology field. Seventy-six percent of participants had certifications with most participants having a CISSP. Forty-six percent of participants had both education and certification. The job titles and responsibilities varied with each participant but they all worked in information security roles in private organizations.

Data Collection and Organization

Interviews were the only source of data collection. The primary method of data collection in phenomenological studies is through interviews (Creswell, 2012; Giorgi, 2009; Van Manen, 2014). This is consistent with the methodology of this study as described in chapter 3. All interviews were conducted between September and October of 2014. Each interview lasted on average a median total of 90 minutes. All interviews were conducted and audio recorded. The interviews were held in a variety of public places for the safety, privacy, and convenience of the researcher and participants. As an alternative to those who were not local or did not feel comfortable discussing these issues in a physical place Skype was used as an alternative.

Data was categorized and organized using an electronic file system for all digital materials based on participant number on a physical drive called the participant device. The code was kept in a separate physical device, the code device, so that the loss of either device would not provide any information on participants. Each device was encrypted in order to protect the data in the event that a device was lost. Data on the participant device was categorized into a multi-folder file system based on participant number. The original notes and recordings were kept in one folder. Sanitized and approved transcripts were maintained in a separate folder. Finally a separate folder contained the spreadsheet breakdown for analysis of the various data elements.

Data Analysis

The findings of this study were analyzed using the participants' responses to the interview questions. Each participant's responses were coded to identify the overall themes that emerged from the study. Qualitative research assistant technologies were not used to process data for this study. Data was processed manually with the limited assistance of Microsoft Excel, using the processes and procedures documented throughout the works of Creswell (2012), Van Manen (2014), and Giorgi (2009). This creative phenomenology analysis design was documented in chapter 3. This process consisted of several steps:

1. Reading and re-reading: This step began with the approval of the transcription by the participant. The researcher became immersed in the information gathered from the research. This first stage involved careful examination of the data from each interview preciously transcribed. Each interview was examined as an individual case study in the primary stage. The researcher examined the information within each

separate transcript with an open mind noting unique information using an unbiased approach to begin to be aware of themes. This step was important for the researcher to begin to understand the participant's realizations and perceptions regarding the topic. This phase ended with the conclusion of the interview review.

2. Phenomenology Reduction - Deconstruction (coding): This phase began with the conclusion of the interview review process. Upon completion of the review the data was deconstructed and coded into Microsoft Excel. This is the data entry phase. Coding was used to identify actions, situations, and various elements of each participant's unique experiences. This phase ended when the data has been coded into Microsoft Excel.
3. Phenomenology Reduction - Developing emergent themes: This phase began once data had been deconstructed and coded into Microsoft Excel. This breakdown of individual coded responses was then organized internally to each participant. There was no recipe for this process. Creativity and innovation by the researcher was the foundation for this subjective categorization of nodes. The coding allowed the researcher to group subsets of nodes related to particular topics. This phase ended when the data had been grouped internally to each participant.
4. Phenomenology Reduction - Reconstruction (searching for connections): This phase began once data had been internally grouped within each participant section. Once data had been grouped it was then reintroduced to the larger data set of other participant information to reconstruct the phenomenon. Data was once again grouped into subsets of nodes related to particular topics. This phase ended when the data had been grouped in relation to the entire data set.

5. Search for Essences –Looking for patterns across cases: This phase started upon the conclusion of the phenomenology reduction of the data. Once the data had been deconstructed and reconstructed the researcher mapped the themes in ways that led to the greatest synthesis of the information provided from the interviews. These relationships between themes and elements led to the discovery of the essences related to this phenomenon. This phase ended the data analysis phase.

Phenomenology Reduction

The phenomenology reduction process was a long and complex process of breaking down the participant responses and identifying the unique themes. Following the approval of each participant's transcript their experience was reviewed by the researcher and organized to highlight their lived experiences in a logical order. Deconstructing the interview and reconstructing it in a logical order is the first phase of the phenomenology reduction process (Van Manen, 2014). This process also allowed the researcher to familiarize herself with each individual's experiences prior to breaking them down and coding their responses.

Each participant's reconstructed interview was then reviewed to identify the unique themes in each response. For example, the first question asked of each participant was how they define an information security incident. These responses contained certain phrases and key words that were repeated throughout their experiences during their description of the incident detection and classification process. These core components were captured and logged in a central location and then compared to the responses from all participants in order to correlate the consistent themes and unique elements of the data. Table 5 lists the central concepts, dominant phrases, and percentages for each coding category.

Table 5. Phenomenology Reduction: Themes and Phrases

Concept	Phrases	Percentage
Define Information Security Incidents	Breach, unauthorized access, compromise	78%
Define Information Security Incidents	Human driven	45%
Classification of Incidents	Escalation from event to incident	67%
Incident Detection	Human detection, human oversight	83%
Incident Management	Had written policies or procedures	72%
Improvements to information security incident response	Have a plan, train the plan, educate IT staff, test chaos	72%
Preparations	Risk assessment, tabletop	60%
Penetration Testing	Helpful to incident management	55%
Threat and Attack Patterns	Helpful to security to prevent incidents	83%
Identifying the Attacker	Irrelevant, not important, not within the scope	85%
Understanding the Attack	Motivation, harm, impact	83%
Law Enforcement	Not helpful, does not care, limited, jurisdiction limitations, incompetent	56%
Third Parties	Helpful	44%
Information Sharing	Helpful to incident response, trend analysis	78%
Initial Response	Assess size and impact	46%
Secondary Investigation	Forensics, additional vulnerabilities	34%
Remediation	System disconnected	49%
Compliance	No compliance standard applicable	38%
Incident closed	Remediation	70%
After Close	No improvements or investigations	55%
After Close	Updated or created procedures	42%
Motivation	Criminal, financial	36%
Third-Party Organizations	Non-repudiation, forensic, special skills	45%

Essence of the Data

Major themes were revealed following the analysis of each individual participant's lived experiences when viewed using phenomenological analysis methods. Twelve primary themes were identified based on participants' experiences. Further consolidation of related concepts eliminated thematic redundancies and overlap ultimately resulting in 10 final themes. These themes collectively make up the essence of the phenomenon of information security incidents. Although each participant experienced the phenomenon individually and uniquely it is where patterns emerged across multiple experiences that truly represent the phenomenon. These common themes represent the most commonly related concepts between each participant's experiences in information security incident management.

It is important to note a limitation of the study at this point. Due to the sensitive nature of the research material it is not possible to relate quotes for various aspects of each theme. No incident can be directly referenced due to the potential identification of real world organizations. The quotes that are reported are attributed directly to participants based on their experiences rather than their specific lived experiences. The lived experiences regarding incidents are paraphrased throughout the data analysis section.

Theme 1: Scope. The first question asked of each participant was how they defined an information security incident and their general processes and procedures for identifying and classifying potential incidents. The answers provided were generally consistent with the definition put together during the literature review for this study. In the literature review a core common definition was compiled from reviewing various literature sources on information security incident management that also contained a description of what might constitute an information security incident. Information security incident management is identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents (Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Werlinger et al., 2010). Almost every participant referenced specific language indicating compromise, breach, attack, and attacker in their definition of an information security incident. Participant 13 reported,

> For me an information security incident is an event that happens, not a risk that could happen, in which an exposure occurs that may lead to unauthorized explore of data or compromise to systems. Officially for us it becomes an incident when we are notified that something has been escalated. It becomes an incident when a compromise has been confirmed.

Several others also referenced violations or compromises specifically of confidentiality, integrity, or availability. Throughout their experiences they referenced incidents in terms of technology, processes, and people as well as diagnosing, containing, and recovering during incidents. These statements were consistent with the definition of an information security incident in this study. However, a few participants also referenced a much broader definition of information security incidents which included natural disasters and technology failures as information security incidents due to disruptions in availability.

Two viewpoints developed over the course of this research as related by participants. The most prominent viewpoint is a path of escalation in which an event is detected, identified, and then a decision made to classify it as an information security incident. Participant 16 reported,

> Somebody has to look at them (alerts) and triage them to determine if something is really normal. If it is benign then throw it out. If it is not something that can be easily identified then it is escalated to the security engineers. Responding to an alert starts with asking if these events are really indicators of anomalies in the network and then why? That’s a whole different stage once you triage and decide that there is something there.

A more detailed and focused incident response procedure follows if it is declared an information security incident. This common viewpoint works forward in a logical process toward classifying an event. Once an incident is classified as an information security incident, a secondary investigation into the details of the event occurs, followed by another decision point, leading to remediation and event closure.

Alternatively, several participants referenced a different viewpoint which starts from an assumption of breach. When an assumption of breach is made the opposite of escalation occurs. The incident is detected, investigated, identified, and then a decision made to classify the incident as an information security incident. Participant 02 reported,

> It starts with either the user or someone telling us that there is something wrong. This can come from the public or even from legal counsel. There is some event that someone is concerned about. We may also detect an incident through compliance, risk audits, or internal monitoring tools. We have many avenues to get information that may indicate that something is wrong or that something is of interest to investigate. These potential incidents will then be classified further into either potentially a breach or hopefully just an incident without any data exposure.

If it is classified as an information security incident remediation steps occur followed by another decision point for event closure. In this viewpoint, the process starts from the assumption that a breach has occurred and works backward through the investigation process to determine the likelihood of a breach. This is a rather unique approach that takes a more aggressive view of incident management and typically these participants were more interested in identifying aspects of the attacker as opposed to establishing the scope as a primary focus of the investigation. Ultimately, each viewpoint has several common elements regardless of the order and both viewpoints follow the same path post-investigation to remediation and closure.

Another common element of information security incident management related by participants was the variations in incident response based on the strategic positioning of the incident responder. Almost immediately three different layers of incident response were identified. The first interview conducted for this study was with a participant who focused on small business clients; the second was with a participant who worked for a larger company; the third was one who worked events that had the potential to threaten the security of the Internet. These three layers of incident response and their viewpoints at the tactical, operational, and strategic level mimic the same format for military categorization and viewpoints of threats.

The participants at the tactical level were commonly far more technical and focused on immediate response elements while those participants at the operational level were commonly more focused on the scope and control of the incident. Participant 01 reported,

> It varies from day to day. Each customer has a different situation and it can vary anywhere from spyware, malware, adware, cleaning up a desktop, finding out that someone’s email has been broken into, to recovering their password. So it varies in a very large way. I’ve worked on mainframes all the way down to PC and network systems.

Participant 02 reported,

> Depending on the size and scope of the incident I may do a full incident response investigation. Regardless I will always make the final risk determination in all incidents and then report the findings to the board of directors. I also do all the breach responses.

The majority of participants in this research have experiences that fall into these two groups. While these two can operate and respond to incidents independently, people in each group frequently worked together in many situations to respond to and manage incidents. When discussing things from the operational viewpoint, tactical elements were often overseen by management as part of the response and in some smaller security teams the operational level incident responders were also the technical level incident responders.

However, the third viewpoint was dramatically different than the first two. A few participants’ lived experiences occurred at the strategic layer. The strategic layer is several echelons above the tactical and operational viewpoints. Participant 03 reported,

> I am not focused on one customer space but on responding to incidents that effect large swatches of the population. Some of the experiences I have lived through were incidents on a large enough scale where people were worried the entire internet may crash.

The scope and mission of incident response changes when addressing incidents at this layer of information technology. The strategic viewpoint addresses regional, national, and global incidents that affect large portions of the population as opposed to the operational or tactical viewpoint that addresses smaller incidents. These incidents are typically not breaches but vulnerabilities that, if exploited, would have a damaging effect on large portions of the population. However, breaches at this level of incident response have crippling effects and large-scale implications. This is the only viewpoint where a cyber-war or nation-state driven incident was referenced. While these viewpoints have different scopes and mission the processes and procedures for addressing an incident was consistent regardless of the participant's echelon.

Theme 2: Flow of the incident procedure. Incident procedures generally tended to flow in the same direction in all reported incidents based on the lived experiences of the participants. Each incident started with detection then progressed, if it was an escalation procedure, through an initial investigation generally designed to establish the scope and key critical elements. The key elements were generally the size, type, and probability of a data breach as well as the intent of the source as either malicious or benign. Once these elements are identified a decision is made regarding the next steps which may be different depending on the size and type of incident. Participant 012 reported,

> The big thing we focus on is triaging the event. If there is an active attack then we move to shut that down as quickly as possible. Once that part is mitigated we work to identify what happened and then mitigate any additional risk. Our focus is primarily on confidential data since that is the core of our business. This has been common in all the organizations I have worked with in the past. If a system has no confidential information then there is not a lot we do but if it has sensitive information we do everything we can to mitigate those issues.

In most cases it progressed from this decision point into another investigation to identify the technical source of the incident and then to remediate the vulnerability. Upon remediation the incident process closes. While some participants reported after-action process improvements these were not consistent enough to say that they occur regularly. This process deviated in the very rare case when the information security incident was believed to be malicious, criminal, or involved lawyers. While the initial procedures for incident management were generally the same the process was more detailed in the second investigation which generally involved forensic investigations into when and how the incident occurred.

The exception to this general flow of incident response is when the event starts from an assumption of breach. Detection is still the same but the incident response process proceeds through an alternate progression, covering an in-depth investigation leading to the reclassification of the incident followed by appropriate remediation steps, depending on the nature of the reclassification. In most cases the incident is reclassified from an information security incident to an event and no further incident response action is needed. These cases are typically passed back to general IT staff for remediation, if required. In cases when a breach cannot be disproven the process progressed from this decision point into notification and remediation procedures before closing the incident.

While many participants reported their experiences in a linear process it is unlikely the parts of the response took place in such a separated fashion. Elements of each part may have overlapped one another in the field and occur, at least in part, simultaneously. Some of the remediation steps may take place before and after the end of the incident. The primary investigation may bleed into the secondary investigation prior to the actual decision point regarding the organizational plan for handling the incident. As one participant put it there is static point in a working organization. There is no magic time when the world stands still to accomplish the formal niceties of plans. Sometimes it happens and sometimes it does not and more often than not these participants were handling multiple responsibilities or even multiple incidents and investigations during each of the reported incidents. Also, in each instance of an incident, it was only one person's experiences, which only represent one part of the incident response. So while on paper and in hindsight this process may look linear it would not always occur in such as timely fashion if observed.

Theme 3: Decision making. Decision making in any crisis situation is an intense combination of multiple factors. There are two primary decision points in the incident response process that were consistently noted by participants. A bit surprisingly very little decision making is involved in detection. The majority of the situations reported during this research were clearly information security incidents and were recognized as such almost immediately. Decision making in relation to incident response is primarily based around the perceived impact of the incident. Participants indicated that most events, regardless of whether or not they rise to the status of an incident, receive at least some level of investigation. Once this cursory investigation is done the responders reach their first major decision point which is about escalation or declassification.

Incidents that appear to have a low impact, such as incidents with compromised servers but no loss of confidential information, generally have a truncated incident response process consisting of the initial investigation and minimal remediation. This first decision point is focused entirely on the scope of the situation in order to determine if the event is really an information security incident. If a decision is made not to escalate to an incident or to declassify the incident to an event the process generally ends here. Remediation in these instances either consists of nothing or simply repurposing the compromised systems and there are generally no additional investigations or after-action reviews. This was generally not a bad decision when it was made by an informed decision maker and usually indicated that either the incident response plan was effective or simply that the incident was not worth pursuing for various reasons including return on investment.

If the decision is made based on the initial review of the event to either escalate it into an incident or to maintain an assumption of breach a full-scale incident response process is established to control the rest of the incident. When the impact is high, such as when money or confidential information has been lost, a full incident response process is initiated. The initial response generally focuses on establishing the scope of the incident, while a secondary response establishes forensic information on elements such as breach method and source location. In these secondary investigations a greater emphasis is placed on identifying more elements around the incident which may or may not be used afterward to develop process or technical improvements depending on the process maturity of the organization's incident response program.

The second major decision point involves the closure of a major incident. If the incident requires a full-scale incident response process then a formal decision is generally reached at the end of the secondary investigation. This decision point involved the remediation of incidents as well as any knowledge management processes. The technical context of this decision is based on the residual risk and impact of the incident. These elements, such as residual infection percentages in malware incidents or the status of technical control enhancements, are reviewed to determine if the incident has been handled appropriately. One interesting note is that participants generally separated the technical response from non-technical steps such as breach notification reporting, which occurs if it is deemed appropriate after the incident is finished.

Depending on the process maturity of the organization in incident response an after-action review may also be directed from this decision point. While this was generally an exception rather than the rule in participants' experiences, this type of review was invaluable to those that performed it after an incident. Their experiences validate the industry best practices for IT processes. This could be seen over the timeline of information security incidents that participants experienced when they conducted after-action reviews. The most experienced of the participants referenced incidents that occurred before the organization had established formal incident response policies, procedures, and methodologies in their organizations. In every instance when participants referenced these incidents they were large, damaging, and chaotic information security incidents that always led to the formation of formal incident response policies.

The context of the decision making was consistent throughout participants' responses during the interview process. However, there were variances in their experiences. These were primarily based on if the participant was involved in management at the operational tier of incident response or at the tactical level. Tactical-level participants responded that they generally received the decisions from higher up in the organization, while operational-tier participants responded that they either made the decisions themselves in small companies or, as was often the case, made the decision after reaching a consensus with a team of senior managers or their clients. While the incident manager generally had a great deal of authority they deferred in most cases to a counsel in order to determine the best decisions for the organization. The composition of this team varied from organization to organization depending on the size and type of industry. In organizations that have separate IT operations or privacy directives from security these two senior managers, along with legal counsel, typically made up the decision makers for the organization. Even in the most damaging incidents reported CEO or board level representatives were not included in the decision-making process.

Theme 4: The attacker(s). This was a unique theme that directly addresses one of the core questions of the study. In many of the incidents reported by the participants there was a very mixed response to questions about the attackers. The lived experiences shared during the interview process demonstrated two conflicting elements. Direct questions about who an attacker was in any particular instance were generally answered by stating that the information was irrelevant to the response. However, in each description of each event, even accidental events, elements of the attacker and their identity were shared. Despite being thought of as irrelevant to the investigation identifying certain elements of the attacker is an innate and often unconscious process performed by the incident responders. They naturally attributed elements of the attack to an "attacker" even if they never established a specific person or group responsible.

Even through attributing elements of an attack to an unknown attacker is a natural intuitive leap identifying the attacker is rarely, if ever, a factor. While there was almost always some information available on a potential attacker within the logs of the system such as IP addresses that were discovered during the incident response the investigation rarely proceeded further. When asked what aspects of the attacker were important such as who and why participant 015 reported,

> I've never usually cared. If they are causing an effect to the organization that is where I will spend my time. Who they are is something I will turn over to law enforcement to chase that. I will let them know what I know but being able to tell who they really are is not important to me. I want to stop the effects.

In several of incident response experiences related in this study thirty percent of attackers were international to the organization. Law enforcement problems was another theme related during the discussions about the lived experiences of these participants and it was generally believed that anything located outside the United States could not be addressed by law enforcement and therefore was never worth pursuing. Even in cases of clearly criminal behavior such as bank fraud, ransom, and blackmail, the importance of identifying a source stopped at the boundaries of the United States. Incident responders do not have the authority or responsibility to pursue attackers.

There are only two exceptions to the importance of identifying an attacker: if the source of the attack was internal or when the response process operates under the assumption of a breach. If the source of an attack appears to be internal to the organization a much greater emphasis is placed on identifying the attacker as well as means, motive, and opportunity. Internal attackers, accidental or purposefully malicious, can be administratively punished within the organization. In the majority of internal incidents reported the attack was accidental; so, in many cases nothing was ever done against the attacker. A common standard related in this study for decision making was the harm standard. If there was no harm there was generally no foul against the internal employee. However, in the few cases where the attack was purposefully malicious the insider was generally terminated from the organization.

The identity of the attacker was also important when working under the assumption of breach. In their efforts to determine if a breach was likely and the impact of that breach the experiences shared in this research project showed that identifying the attacker was a critical piece of information. This led the incident response investigations in various directions related to the attacker including motivation. The end result of these investigations helps to determine if a breach took place and the likelihood of harm. In this instance the harm standard was used to determine the likelihood of malicious use of compromised systems or data. In several instances this information was used to verify the likelihood that despite a probable breach of data there was not likely any harm and therefore not a reportable incident in terms of regulatory compliance.

When asked what elements of the attacker were important to incident response participants often answered with motivation and intent. These two elements represent the decision point in relation to the attacker and the incident response processes. The motivations related by participants commonly indicated financial or destructive motivations for purposeful attacks and ignorant or benign motivations for accidental attacks. Participant 05 reported,

> I think any breach is very important. Motive is important. What do they want? Data breaches are no joke. Motive is number one in my book the other is the impact. What are they doing? Without motive I have no way of knowing what else they may have done, and where to look. I just assume that the motive is malicious. There is no more let's just hope on the network just for fun.

The intention of an attacker was almost always purposefully malicious except when it was accidental. The accidental attacker, as described in the literature review, was a factor in some of the incidents related during this study. This human element was another core theme related in the study and often revolved around users, manager, or core IT staff either creating incidents through ignorance or enabling attackers through ignorance.

Even when no attacker is or can be directly attributed to an attack these assumptions are almost always made and attributed to an "attacker" in the incident response process. In many cases when asked about decision making during the initial response processes participants referenced assumptions regarding the motive and intent of the attacker and how those assumptions directed the incident response process. Several participants directly addressed this point by stating that, had an attack been purposefully malicious and criminal rather than purposefully malicious but benign, they would have done things differently. While it is impossible to know what might have been participants who referenced this potential noted that the difference would have been a more detailed investigation process and high priority responses from management leading to different decisions being made at the end of the incident response process.

In the rare instances one of the incident responders attempted to discover the source IP address they were often stopped from pursuing the source at the first major obstacle. One reason that this was never important outside of an internal attacker is because incident responders do not have the authority to invade machines outside their network. The internal logs may demonstrate the source of the attack against the machine; but, that may only be one step in a much larger chain. However, to uncover that chain logs must be captured from the first link and every subsequent link. Private industry does not have the authority to hack back into attacker networks that commonly include infected "bystander" systems which may or may not be government, corporate, or personal computers.

Theme 5: Fear of the law, China, and the United States. A common fear permeated these discussions. In a majority of responses during the interview when asked about working with law enforcement agencies participants responded with negative reactions. It was indicated that organization management fear law enforcement. The incident responders fear law enforcement. They fear law enforcement for several reasons including cost, secrecy, confiscation, victim blaming, and general ineptitude.

The identity of an attacker was almost never an important factor in these lived experiences. In the end the damage has already been done and the more important elements of the investigation take precedence such as establishing scope or remediation. The responses from these interviews indicated a common belief that the value of the resources it would take to pursue a criminal investigation through a trial would outweigh any benefit to the organization. Absent of a complaint it is not possible for law enforcement to pursue the incident. Yet even when they are called for their assistance in pursuing a target it was reported that they often simply came, took the information, and left, never to be heard from again. When asked if law enforcement was helpful Participant 05 simply said,

> I don’t know. You are never told the results when working with law enforcement. It’s not up to them to say anything.

Since they never provide updates to the responders or reply to requests for information from responders it was not known if law enforcement was ever able to make good use of the information. However, this shroud of secrecy destroyed the trust or respect that many of these responders had toward law enforcement and several remarked that they would not report to law enforcement in the future due to these negative experiences.

Organization management is also afraid of confiscation of equipment. In several instances participants mentioned balancing the merits of pursuing criminal action against the possibility that law enforcement could confiscate essential equipment as evidence potentially leading to major financial losses. Participant 09 reported,

> So law enforcement is a two edged sword. They can be very helpful in obtaining resources but they could also seize the server. If that is the server you rely on to do business you are out of luck. So when I am asked if law enforcement should be informed I say it has to balance out (between the risk and reward).

Armbrust et al. (2010) referenced this same fear when discussing a security concern in cloud security that resulted in a company going out of business due to the government shutting down a datacenter in which they were collocated with the law enforcement target. Despite being told about incidents involving criminal activity such as bank fraud, identity theft, blackmail, and even ransom, the participants felt that the risk of bringing in law enforcement was greater than any potential outcome.

The nature of the regulatory environment is not lost on organizational leadership based on the lived experiences of incident responders. Organizations do not wish to report certain events to law enforcement for fear of regulatory fines in addition to the various other reasons. In multiple events private corporations were being held for ransom at digital gunpoint and, rather than work with law enforcement, they paid the ransom and coordinated with third-party teams to resolve the incident. Several participants reported creative naming strategies for incidents to escape having to report security incidents and in larger organizations it was reported that there was a direct effort to keep auditors from finding these security incidents. Participant 016 reported,

> We do not use the term incident because an incident implies legal implications. So if we declare something an incident legal has to become involved and directs the process. If we label it as an issue or event we can handle it ourselves.

This response was consistent with conclusions addressed by Ahmad et al. (2012) discovered during the literature review. The common belief held by many of the participants is that it is best not to involvement law enforcement because they are more likely to come after the organization, the victim in the attack, than to pursue an attacker.

What may be even worse than all that is the prevailing belief that law enforcement just does not care about corporate computer incidents unless there are billions of dollars at stake and the attacker is in the United States. Participant 017 reported,

> Law enforcement has flat out told us they are not there to help us. They are not a cyber-national guard. The systems are ours to defend.

The feeling is that they do not care about the problems of most private organizations and they are hamstrung by a lack of resources and international laws regarding cyber crimes. The scope of this study did not include law enforcement incident response or cyber-crime investigation procedures by law enforcement so it is unknown if these beliefs are accurate. However, a small minority of participants indicated positive assistance from law enforcement. They indicated that in some instances when using aggressive response to incidents they would not have been successful without the support of law enforcement.

State-sponsored attacks were a major concern for many incident responders particularly attacks from both China and the United States. Compounding a fear of law enforcement is a fear that the United States may be one of the worst offenders of information security. How can you report violations of security to the violators? While most of the attackers were identified as coming from states that sponsor hackers, responders have a bigger fear of the known unknown which in this instance is the United States. Participant 013 reported,

> I suppose we talk these days about the difference between criminals and nation states. It really matters to us which of those vectors we are dealing with when responding to an incident. We don't tend to see the other class which I would call recreational terrorists like anonymous. We really worry about the capabilities of nation states. We consider that a bigger threat than the Russian mob and their botnets. They (the United States) may be the worst offender out there. We are sure they have all kinds of backdoors into encryption. The Chinese are another problem we don't know how to address. They are just better than us. They have whole buildings dedicated to hacking but they don't have the keys to encryption like the United States. They have to do a lot of additional work to break into things that the US does not have to do. Therefore we see the US as a bigger threat. How do we address that? How would you stop them?

This assessment is in line with the literature in the field. It is common knowledge that the United States participates in hacking for various purposes resulting in violations to the CIA of data (Langer, 2011). There is no longer any doubt that the United States at least has the potential and ability to attack organizational data. What these participants fear most is that the United States is simply better at covering their tracks than other state-sponsored attackers.

Theme 6: The basics elements of human security. The human element of security was a consistent point of discussion in every interview based on each participant's lived experiences.

Just as the humans are one of the three elements of information security as defined in this study, the lived experiences of these participants heavily feature humans. Participant 16 reported,

> The most expensive part of any security program is the people. Its eyes on the screen. They are the hardest to keep, train, and keep involved and interested. We need to keep them used efficiently.

The detection and identification of incidents is heavily reliant on human reporting or human-assisted reporting. However, just as humans can be of great assistance to incident responders, it was often reported that human ignorance was the root cause. Humans will always be a part of the equation and the almost universal recommendation from participants in this study is to train them.

A majority of the confirmed incidents referenced in the lived experiences of the participants of this study were incidents that were detected and reported by humans. The value of the human element in this area is undeniable. Participant 017 stated,

> There is not a security technology out there that has not been breached. Any incident that has been worthy of a quality response, many lesser incidents do not rise to that level, will bypass automation. I would say that for the environments that I have worked in, human reporting is far more valuable. The sophisticated attacker will go through your defenses unnoticed. Locks are meant to keep the stupid criminals out. Most of the useful advice for incident response will come from humans. Badly written software or poor social engineering will typically be caught by automated systems. However good attackers may even fix your vulnerabilities to maintain their foothold and keep you from detecting them longer. From a technology standpoint automation has less value than human reporting. I would take an aware human system over an automated tool any day.

The lived experiences of participants showed that clients, users, third parties, law enforcement, help desk, managers, and other technology administrators can all be sources for detecting incidents. When asked about the balance between human and automated reports it was often said that humans report more real incidents than automation but automation detects more events than humans. Despite a preference by several participants for automated reporting humans still need to be involved in detecting and identifying incidents.

Most of the participants in this study stated that in their experience automated detection tools are not sophisticated enough to be reliable. Even when participants referenced automated detections it was always caveated with an equally high workload in order to identify the false positives. In some of the experiences reported, overreliance on detection technology caused an incident to go unnoticed for an extended period due to failures in automation. While automated tools such as intrusion prevention systems can react to incidents without human input they were not commonly referenced by participants. Instead, when automation was referenced it was often in the form of anomalous events that were then reviewed and either escalated or addressed by technology administrators. In the experiences reported during this research, even when relying on technology, that technology still relies on humans.

Yet humans are also the single greatest threat to securing technology. This is not the threat of the attacker but the threat of ignorance. In several of the incidents that were reported through the lived experiences of participants the root cause for an incident was poor judgment made in ignorance of basic information security principles from users, IT staff, or management. Participant 07 reported,

> The less reliance on human involvement the better. Humans are unreliable for the very reason that they create incidents. So the more automation the better. However, you can't get away from that. You don't want to completely exclude people because they can detect strange things on systems. The tools are not that sophisticated yet.

Simple planning and a little security awareness would have gone a long way in incidents where the default usernames and passwords were on machines, firewalls were disabled, essential fixes were overwritten, or data was accidentally disclosed, transmitted, or lost. Simply following basic compliance and security guidelines identified in any framework would have prevented many of the incidents or at least made it significantly harder for the attacker to exploit the network in the same way. When discussing the lived experiences of participants in heavily regulated industries this is less of a problem; but, when discussing the lived experiences of participants in small or medium-sized businesses that are not as regulated, all that can be said is security common sense is not common.

Many participants had the same recommendation when it came to improvements for incident response processes and procedures or the support that they would like to have for incident response: Train people on incident response. In several of the individual events reported by participants this was one of the process improvements implemented following the incident. A frequent comment from the experiences of the participants of this study is that security awareness is critical for users, IT staff, and management. Participant 06 reported,

> One of my bigger challenges right now is that the end user or IT teams are not cognizant of information security incidents as opposed to IT incidents. They have a tendency to obfuscate or obliterate information that would be helpful for incident response. So I recommend a lot more awareness.

These recommendations made by participants included that training on detecting and reporting anomalies is critical for improving incident detection and should be provided to all staff, rather than something that is only practiced by a handful of security professionals. It also included that training security outside of basic user awareness training for technology administrators is critical. They configure these systems and must have a solid understand of why security controls are required. Further, and perhaps the most important, recommendation made by several users was that training for incident response should include going up the chain of management as management is responsible for senior level decision making regarding the incident response program, processes, and methodology at the organizational level. Participants reported that many of the incidents would have been greatly mitigated or perhaps would not have happened if security were truly everyone’s responsibility.

Theme 7: Planning and preparation. What is the most common thing to go wrong in information security incident response and management? According to the lived experiences and recommendations of the participants in this study incident management fails before the incident has even started. Without effective policies and procedures that people know how to implement, information can be lost or damaged during the initial triage state for incident response crippling any ability to follow up with formal actions such as involving law enforcement. After the incident improving and refining these processes and technical controls is key to improving both response time and preventive security. The most common things to be discovered during a major incident is the value of a plan, the importance of training, and the necessity of improving preventive security.

One of the frequent recommendations based on the lived experiences of participants was simply to have a plan for incident management. Some of the participants had experiences that spanned the creation and maturation of an information security incident response program; the benefits were observed through increased response times, effective management, and decreased losses as these programs became more mature. When asked about improvements o incident response Participant 03 reported,

> The biggest thing is getting over the hurdle of getting a process. Most people do not have a process to begin with. Processes are normally not very mature if they are even there at all. Some places have a very mature process but others do not even have a rudimentary process. Pretty much no one has a process. The ones that do, such as the ones I have been a part of, have them because they have been kicked in the teeth several times over the years.

Large organizations or those that are heavily regulated typically have more robust programs from being high-priority targets for attackers and auditors. While in many cases these plans were not perfect they were at least present in some form during an incident. However, organizations frequently had no plan in place to address security incidents. Commonly it was small- and medium-sized organizations that did not consider the importance of incident response until it was too late. The participants in this study who conducted incident response as a third party noted that in their experiences, of those organizations they consulted with, ones that were experiencing a major incident had no incident response plan or capability.

Having a plan may be as simple as identifying a third-party support organization to call for incident response or as complex as including multiple internal layers of management. The common plan elements that participants related in their lived experiences and recommendations based on their experiences were detection, escalation, decision making, and response steps. Identifying potential detection methods can make anyone into an intrusion detection systems without having to be a technical expert. Once an incident is detected establishing escalation paths helped participants to control the flow of the incident management process around key points limiting who is involved and when they become involved. Despite adding additional people to the incident response process as an incident escalates it is also important to establish a single incident manager in the response plan to make decisions. These plans were not only designed to ensure consistent responses to incidents but to protect complex environments where fixing one problem may create several others. These elements together are needed to create a basic incident response plan. Interestingly enough, despite the need for a plan based on the lived experiences and recommendations of participants, it should also be noted that despite having a plan most responders rely on their instincts and experiences. While this is necessary to address situations and incidents that are not covered in policies and procedures another frequent comment was that if the plan is not trained it will never be used.

As a result of not having a plan one of the most frequent comments from the lived experiences of incident responders is to have a plan and to train on the plan as often as is reasonable throughout the entire organization, not just in the IT security department. Participant 017 reported,

> Drills. Exercise. Non-stop. If you don’t exercise the plan you can’t do it when incidents happen. This should be more than once or twice a year. Incident response should be muscle memory.

Tabletop and simulations were commonly referenced as ways participants used to prepare for incidents before they happen. The most effective of these exercises, according to participants, include adding people outside the IT security department and implementing chaos. While the core security team may be well aware of procedures in incident response, preparing other departments and including lawyers, marketing, human resources, and other mid-level managers through the organization, can help to ensure preparedness if these individuals are called on during an incident. This also adds an element of chaos to the scenario as these individuals may not be normally involved in this process; but, the most common element of chaos that is injected in these exercises, according to participants, is to remove key players from the board. In a few of the real incidents reported the key decision makers were not available for part of the incident. Identifying alternative decision makers and how they can respond in the absence of senior leadership can make a good plan much stronger.

Despite the nature of incident response being a reactive field most incident responders noted a surprising viewpoint. They noted that prevention is the core of information security and that incident response ultimately serves to support the preventive function of information security. It was rare that participants reported after-action reviews or postmortems but they were essential elements of incident response to those that did. Participant 012 reported,

> Beyond that the biggest recommendation I would have is to conduct post mortems about incidents that have occurred. In my experience most incidents are near misses. If something different had happened it would have been a very big deal and devastating to

> the organization. Those are opportunities to identify processes and controls that have broken down and to make them better. That is tremendously helpful.

The process and procedure improvements, lessons learned, and other knowledge management that comes from incident response is redirected to the preventive defense of the network. Because the focus of investigations in private organization is not controlling the breach from the outside, which would involve focusing on the attacker and the distribution or use of the breached information, but on remediating vulnerabilities and identifying the scope of the breach the focus of this reactive operational security process is preventive medicine.

Theme 8: Third-party collaboration. Many of the participants' lived experiences involved third-party organizations to the compromised party. Sometimes the participants themselves were the third party hired to investigate aspects of the incident. This may be done for any number of reasons but the most common was non-repudiation, lack of internal skills, and lack of internal planning. Participant 08 reported,

> Yes I do believe it is helpful if not mandatory. Organizations are generally stretched thin to begin with so the third party has to, and should, do most of the leg work in incident response.

The value of a third party was critical in many of the incidents reported even for large regulated organizations. However, in some instances third-party organizations were not helpful. Sometimes they complicated issues and withheld information for payment but the majority of experiences reported during this research project were positive when third parties were brought in to assist in some aspect of information security incident response management.

Theme 9: Information sharing. The importance of information sharing was a common recurring theme within the lived experiences of the research participants. The participants in this research study generally indicated that information sharing was extremely important to incident response in various ways. In some cases participants were only made aware of an information security incident through the exchange of information. Information such as information about recent attacks, trends, malicious sources, and common motivations were important to the incident response methodologies of several participants. Information sharing between organizations, professionals, law enforcement, and third-party security firms were all mentioned as sources of valuable information throughout the study.

Identifying recent attacks and trend information allows organizations across various industry verticals to work together and proactively address vulnerabilities. While the preventive elements of information security are separate from the actual management of an incident these elements helped participants to work with their clients or organizations to manage information security before an incident occurs. In several instances sharing information about malicious sources led to the discovery of compromised systems and data. When discussing this issues and the difficulty of getting participants to share information with Participant 03 he said,

> I would say (information sharing is) critical. That (not sharing information) is asinine. The attackers share information. Some of these attack tools have technical support. You buy a kit and if you have problems with it they will support you.

This facilitates the detection and identification of an incident that in some cases would have continued to go unnoticed. Finally, sharing information about common attacker motivations and active attackers helped participants in several instances in secondary investigations and determinations about breaches. While the majority of participants were not concerned with who an attacker was they were concerned with their motivation and in several instances this affected how they responded to incidents. The attacker's motivation, which was often determined based on information shared on current trends and activity logs, was a major decision point for responders as to how the incident response process should proceed.

However, while no participant said that information sharing was not helpful, many did put caveats on the disclosure of information. In several interviews participants remarked that they were only comfortable sharing information security incidents that were already public knowledge. Participant 011 reported,

> For sharing the information outside the organization it should only be after the incident has been completed and only the lessoned learned. Everyone can learn from everyone's missteps and challenges. The information needs to be vetted to ensure that it can be shared. When I presented one of our incidents at a conference it was after it was completed and we vetted the information to ensure it was appropriate and would be helpful to the information security community. Sharing lessons learned is critical but you most certainly would not want to share information in the middle of the incident. It has to be at the right time. You would not want to share information about an incident during an incident.

A vast majority of the incidents reported in this study are more than two years old. Participants also noted that information sharing can be difficult due to a lack of common reporting criteria, fear of the police, and fear of reputational damages. This is consistent with reports discovered during the literature review (Ahmad et al., 2012; Armbrust et al., 2010; Wang et al., 2012). Yet despite all of these issues in reporting, the value of information sharing was an important common essence throughout each participant's experiences and often a top recommendation for improving information security incident management.

Theme 10: Attack frameworks. Each participant was asked several questions based on their lived experiences including questions about penetration testing as well as knowledge of threat and attack patterns. The responses to these questions were generally positive, indicating that knowledge about how to attack a machine as well as current threat and attack patterns is important for an information security professional. Participant 010 reported,

> It helps to know which tools and applications to watch and what types of logs these create on the backend. It helps to determine that an attack is happening. Having knowledge of how things go and how to work through the mind of a hacker is helpful.

Participants supported the importance of knowing attack frameworks and they indicated that it was extremely helpful to incident response. In several of the experiences provided by participants this information was important to establishing the scope and identifying the root cause of the attack. Certain threats behave in certain ways which indicate general attack patterns that allow incident responders to counter specific threats when responding to incidents.

However, some of the participants indicated a different opinion. Some participants indicated that this knowledge was not helpful in incident response. Knowledge about these attack frameworks was indicated to be of value to incident prevention rather than incident management. Knowing about the threats that are out there and how attackers may try to attack a system gives a security engineer additional knowledge to put strong controls in place to prevent those threat vectors. In either case the knowledge about how to attack a machine and the current threat landscape gave these responders a leg up when detecting and analyzing the incident.

Chapter 4 Summary

In this chapter the researcher presented the data as it was collected and then analyzed into multiple themes representing the essences of the research phenomenon. The participant information was documented and described to demonstrate their qualifications for inclusion in this study. Their collected experiences were then analyzed by breaking them down into their core components and coding each major theme to identify major connecting elements. These interconnecting essences represent the phenomenon under investigation. 10 themes were identified as core elements of information security incident management concepts. These themes are the answers to the research questions presented in this study. Ultimately this study is only the first step into a complex field. In the next chapter the major themes of this research are collated with the research questions to provide some much needed answers.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Introduction

In the previous chapter the collected data was organized and analyzed. It is appropriate now to discuss how these results fit into the overall intended purpose of the study. The purpose of this study, as laid out in chapter 1, was to understand the experiences of corporate-based IT security professionals providing information security incident management services and to use those experiences to contribute to the body of scientific knowledge in the science in warfare, criminology, and IT. The detection, identification, investigation, eradication, recovery, and management from both sides, attack and defense, were key areas of exploration. Information security experts with experience in various aspects of information security incidents were interviewed regarding their personal experiences with information security incidents.

There have been many research articles published in the past centering upon information security. However, as presented in chapter 2, very little research has been done to explore holistic information security incident management. The most current literature continues to concentrate mainly on preventive information security techniques designed to prevent incidents rather than respond to them. Data was collected to address this gap using specific methods for collection and analysis as presented in chapter 3. These instructions were carried out and the results were presented in chapter 4.

Finally, a discussion of the results will be found in the next section that will be synthesized with prior research. The remainder of this chapter will proceed through a discussion of the results, answering the research question, presenting the limitations of the study, and discussing the implications of the results. This chapter concludes with several recommendations for further research followed by a conclusion to the study.

Discussion of the Results

The essences of the participants' lived experiences led to several conclusions. The 10 themes were each demonstrated in the responses of these 18 participants. While the analysis of these themes demonstrated the majority of experiences, it also revealed some experiences that countered the majority. The study results will be presented to reflect their pertinence to the research questions: (1) What are the lived experiences of information security professionals in private organizations responding to information security incidents?; (1a) How does the identification of the source, purpose, and intent during an information security incident influence the responses of information security professionals?; (1b) How do information security incidents influence information security professionals preparing for future challenges?; (1c) In what way(s) do information security incidents influence the thinking of information security professionals with regard to information security attack frameworks?; and (1d) How do external information security programs impact the response of information security professionals in private organizations with regard to information security incidents?

Research Question 1. The primary research question in this study asks: What are the lived experiences of information security professionals in private organizations responding to information security incidents? This question was designed to allow the researcher to ask a broad spectrum of questions during this research project around how they have experienced information security incidents. While all of the themes and results address this central question several elements deserve special attention. Themes 1, 2, and 3 each address how incidents are detected and managed in the field. These three themes together create a balance and a holistic picture of how incidents are scoped and managed and how decisions are made in these crisis situations.

Theme 1 specifically addresses the scope. The scope of an information security incident, based on these results, can be defined using specific language including compromise, breach, attack, and attacker in the definition of an information security incident. Information security incidents are referenced in terms of technology, processes, and people. The results of this theme confirm the definition presented for information security based on the literature review. Information security incident management is identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents (Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Werlinger et al., 2010). The keywords attack, violate, asset, process, and people are all present in this central theme. This theme gives the primary research question shape and established the boundaries for the types of incidents discussed in these lived experiences.

Theme 2 specifically addresses the flow of incident response procedures in private organizations. Each incident starts with detection and progresses through an escalation procedure through an initial investigation designed to establish the scope and key critical elements. The key elements of incidents are the size, type, and probability of a data breach as well as the intention of the attacker as either malicious or benign. Once these elements are identified a decision is made regarding the next steps which may be different depending on the size and type of the incident. In larger incidents the process progresses from this decision point into another investigation focused on identifying the technical source of the incident and then remediating the vulnerability. Upon remediation the incident process closes. This process is similar to the disjointed aspects of information security discovered during the literature review process. These results reinforce four of the core components identified in the literature review process: detection and identification phase (Blyth & Thomas, 2006), the diagnostic phase (Werlinger et al., 2010), the forensic analysis phase (Sindhu & Meshram, 2012), and the recovery phase (Kadlec & Shropshire, 2010). These four components of incident response management are ordered and put into context in the view of the entire incident management process in this theme. This process directly addressed the primary research question by establishing how information security incidents are handled in the field.

Theme 3 addresses the major decision points in incident response. This first decision point takes place after an initial investigation and is focused entirely on the scope of the situation in order to determine if the event is really an information security incident. A decision is made based on the initial review of the event to either escalate it into an incident or maintain it as an event. The technical context of this decision is based on the scope and impact of the event. The second major decision point involves the closure of a major incident. A formal decision is generally reached at the end of the secondary investigation. The technical context of this decision is based on the residual risk and impact of the incident. The results of the analysis of this theme demonstrate the context of decision making in incident response. This theme directly addresses the primary research question through identifying the trigger points for how decisions are made in these crisis situations. Together these three themes provide a holistic view of the core components of information security incident management.

Research Question 1a. The first research subquestion in this study asks: How does the identification of the source, purpose, and intent during an information security incident influence the responses of information security professionals? This question was designed to address the various aspects of the attacker, if that knowledge was important to investigations, and how it affected incident response. Theme 4 addresses this question directly through the analysis of how these factors are addressed and managed in the field. The results of this analysis indicate the importance of establishing who, what, and why to the incident response process.

The first element addressed in this subquestion is the source. Direct questions about who an attacker was in any particular instance were generally answered by stating that the information was irrelevant to the response. Incident response will generally proceed according to the pattern established in the results for the primary research question. However, in each description of each event, even accidental events, elements of the attacker and their identity are present. Despite being thought of as irrelevant to the investigation identifying certain elements of the attacker is an innate and often unconscious process performed by the incident responders. They naturally attributed elements of the attack to an "attacker," even if they never established a specific person or group responsible for the incident. Thus the results indicate that the source had no conscious effect on incident response.

The second element addressed in this subquestion is the purpose. The purpose of an attack addresses the impact in terms of criminal, espionage, or other overt effects of an information security incident. This is a critical piece of information addressed at the first decision-making point in the incident response process and helps to establish the scope of the incident. Incidents that do or may result in nefarious endings are escalated, while more benign incidents are addressed without a full incident response. This element of the attacker is similar to the intent.

The third element addressed in this subquestion is the intent. The intention of an attacker was considered in broad strokes focusing only on if the attack was malicious or accidental. This is also a critical piece of information addressed at the first decision-making point in the incident response process and helps to establish the scope of the incident. The determination of a malicious intention is rarely an important or difficult decision but in the rare instances when the attack was accidental it becomes a critical element to the investigation and ultimate determination of administrative response actions. These results show that accidental attacks are internal and therefore the organization has the authority and responsibility to address the issue on a human resources level. The accidental attacker universally was someone who made an unintentional decision ignorant of security best practices. The determination of an accidental action resulting in an information security incident results in less severe actions than an action by a malicious insider. These results address the research question to identify that the purpose and intention are the two primary elements that are important to investigations in terms of the attacker.

Research Question 1b. The second subquestion in this study asks: How do information security incidents influence information security professionals preparing for future challenges? This question was designed to allow the researcher to ask a broad spectrum of questions about each participant's lived experiences outside of specific instances as well as highlight elements of knowledge management programs. Themes 6 and 7 each address recommendations based on the lived experiences of the participants in regards to improvements to incident response. These two themes together provide a direction for improvement in information security incident response operations based on past experiences.

Theme 6 addresses the human element, which will always be a part of the equation, and the almost universal recommendation from participants in this study is to train humans. The results of the analysis of these lived experiences indicate a simple solution: Train people on incident response. Events are reported by users, management, and general IT staff internal to the organization and the initial incident response can be compromised by any of these people making poor decisions. Training on detecting and reporting anomalies is critical for improving incident detection and should be provided to all staff not just security professionals. Technology administrators configure systems and must have a solid understanding of why security controls are required. Further, perhaps the most important result indicates that training for incident response should include going up the chain of management as management is responsible for senior-level decision making regarding the incident response program, processes, and methodology at the organizational level. This critical lesson learned by the experiences of these incident responders forms the foundation for their current views on incident response and is a great recommendation for any program.

Theme 7 addresses another simple component that is often missing from incident response based on the lived experiences of these participants. These results indicate the importance of having a plan for incident management. Some of the participants had experiences that spanned the creation and maturation of an information security incident response program and the benefits were observed through increased response times, better management decisions, and decreased losses as these programs became more mature. However, organizations frequently have no plan in place to address security incidents. This is a critical failure based on the lived experiences of incident responders that form their current incident response practices. The plan should also be trained and tested. Tabletop exercises and simulations are ways to prepare for incidents before they happen by testing the plan and the participants. The most effective of these exercises, according to the lived experiences of participants, include adding people outside the IT security department and implementing chaos. These two themes address the subquestion as both of these recommendations based on the lived experiences of participants influence their current incident response practices.

Research Question 1c. The third research subquestion in this study asks: In what way(s) do information security incidents influence the thinking of information security professionals with regard to information security attack frameworks? This question was designed to address the importance of the offensive side of information security. However, this question is one sided and does not represent something that can be directly addressed in its current format. Based on the responses of the participants, which did indicate a common theme in regards to attack frameworks, this question should be addressed as: How does knowledge of attack frameworks influence decision making during information security incidents? Theme 10 addresses the perception of information about how to attack a machine and current trends in information security affect information security incident management. The results of this analysis answer the revised subquestion.

In theme 10 the importance of attack frameworks was addressed based on the lived experiences of information security professionals. The results of this analysis show that knowledge of attack frameworks is important for an information security professional. Knowledge about attack frameworks is of value to incident management. Knowing about the threats that are out there and how attackers may try to attack a system gives a security engineer additional knowledge to put strong controls in place to prevent those threat vectors as well as the knowledge to detect and contain a threat during an incident. The results of this theme directly address the research question in that attack frameworks have an important influence on incident response.

Research Question 1d. The fourth and final research subquestion in this study asks: How do external information security programs impact the response of information security professionals in private organizations with regard to information security incidents? This question was designed to allow the researcher to ask about third-party organizations and their impact on private industry incident response, specifically, how government, military, and law enforcement interaction influences incident response. Themes 5, 8, and 9 each address how third-party organizations influence incident response for better or worse. These three themes together address a complex relationship between internal and external private organization politics.

Theme 5 addresses the relationship between private organizations and third-party organizations specifically law enforcement, military, and government agencies. The results of this study indicate a negative impact on incident response in private organizations when these agencies become involved. Organization management fears law enforcement. The incident responders fear law enforcement. State-sponsored attacks are a major concern for incident responders, particularly attacks from both China and the United States. Compounding a fear of law enforcement is a fear that the United States may be one of the worst offenders of information security. Organizations believe they are better off without involving law enforcement, military, and government agencies.

Theme 8 addresses the relationship between private organizations and general third-party organizations such as forensic organizations. The results of this theme, based on the experiences of the participants, indicated a positive and almost necessary relationship for incident response. Third parties provided value to organizations during incident response by providing critical skills and when necessary they act as impartial expert witnesses. This positive experience provided value to organizations through improved incident response capabilities that would otherwise have been impossible to achieve internally. The results of this theme indicate a positive impact on incident response when working with third parties that are not military, law enforcement, or government agencies.

Theme 9 addresses the common theme of information sharing among the lived experiences of these participants. Information sharing is extremely important to incident response in various ways including detection based on information about recent attacks, trends, malicious sources, and common motivations when it is used. However, it is generally not authorized or encouraged in organizations due to fears of negative impacts to security, consumer confidence, and regulatory issues. Yet despite all of these issues in reporting, the value of information sharing was an important common theme throughout each participant's experiences and often a top recommendation for improving information security incident management. The results of this theme directly address the research subquestion and reveal a complex and often discouraged but potentially positive relationship with outside organizations sharing information. These three themes together address this research subquestion and indicate a positive relationship and impact with third-party organizations that are not government, military, or law enforcement agencies.

When the findings from this study are compared with previous research both similarities and distinct differences become apparent. Discrepancies may exist for several reasons. Qualitative research entails a certain level of subjectivity regardless of the efforts made by the researcher to remain entirely objective (Creswell, 2012). Other studies may differ simply because a different researcher approached the problem from their own unique subjective viewpoint. It may also simply be that few researchers have focused as intently on the specific situations this researcher has attempted to address in this study. Many researchers have broadly examined information security whereas this researcher only looked at holistic information security incident management. Other researchers have often sought to better understand elements of information security incidents such as investigation or detection but few have placed these elements together in any type of consistent manner (Kadlec & Shropshire, 2010; Rajakumar & Shanthi, 2014; Werlinger et al., 2010). Yet, despite the differing scope of studies, it is useful to compare and contrast the findings of this study with those that have been previously conducted in order to build a more comprehensive understanding of the holistic experiences of information security professionals.

Limitations of the Study

As with any research project there are limitations to the study stemming from the methodological approach. The limitations of this study included sampling bias and lack of generalizability. The most critical limitations of this study are the common flaws in phenomenology. Phenomenology is directed at the lived experiences regarding a central phenomenon which by its nature requires a selective sample (Van Manen, 2014). A sample frame that includes specific criteria introduces the potential for sampling bias as it is a purposive non-random sampling method. However, it was clearly necessary in order to answer the research question and control the scope of the project. Future research projects may target a broader population, including a female population, but any phenomenology study will be limited in the selection of its participants.

This study is also limited by a lack of generalizability. Phenomenology is not typically considered to be generalizable (Van Manen, 2014). Due to the specific nature of the sample in many cases it is not possible to draw conclusions on similar situations and phenomena. The lived experiences of these professionals may not be generalized to information security incidents that impact government, law enforcement, or military organizations. These experiences also cannot be generalized to a larger geographical region as other nations or cultures may perceive and respond to threats differently. The specificity of the demographics of the participants was necessary to focus on the depth and breadth of the lived experiences of these participants but future studies may target alternative groups in various regions around the world to continue to document these experiences.

However, secrecy is perhaps the biggest limitation to this study. Despite the support of the participants in this study many of the people contacted about this study responded specifically to decline due to confidentiality. 26 potential participants specifically declined to participate due to various limits on the information they are allowed to share. It is also likely that many of the professionals contacted about this study did not respond to this request for the same reason. Other authors have also mentioned this as a limitation when conducting research in the information security field (Ahmad et al., 2012; Denning & Denning, 2010; Shaw, 2010; Werlinger et al., 2010). Even among those who did participate in the interview it should be noted that on several occasions remarks were made regarding a preference to discuss only incidents that are already public knowledge. Most of the incidents reported during this research project by participants were more than two years old.

There is value in sharing information on attacks. This value is demonstrated by the lived experiences of those who have benefited and who continue to benefit from such knowledge sharing. However, as an industry there is a wall of secrecy that stops many working professionals from reaching out and working together as a community to address a global problem. It should also be noted that in two specific instances when potential participants requested permission to participate from their organizations they were expressly denied. In one instance this denial led to a company-wide message regarding participating in this research.

Due to the secretive nature of information security much of the information that was reported could not be used in this study. It would have been very beneficial to report on some of the specific experiences. The specifics of each event would have made very interesting case studies if they could be reported. Even the respondents who became participants in this study generally only wanted to discuss incidents that were several years old and public information. There is a fear among security professionals, as stated by the participants in this study, that if information around their processes and procedures were published attackers would be able to use that information to penetrate their defenses. However, there is nothing secretive about information security.

The frameworks that make the foundation of private industry response are published by governments, standards committees, and in books. The way technology works is widely known and most organizations, except those that create internal applications, are using the same technology that is available to attackers. It is a fallacy that many information security professionals cling to regarding the secrecy of information. Maintaining the secrecy of known vulnerabilities until they can be remediated may be of some value but otherwise, as an industry community, information security professionals seem to have a fear of discussing these sensitive issues and it would be beneficial to the industry if these professionals learned to productively share information as recommended by many of the participants in this study. Until that happens studies like this one will continue to be hamstrung in both the quality and quantity of available information.

Another limitation to this study was the researcher's inability to exclude participants with any military, government, or law enforcement experience. The eligibility criteria for this study simply excluded those that performed incident response for government, military, or law enforcement in the last five years. While no military, government, or law enforcement experiences were reported in this study several of the participants had prior experiences in these areas. There is no guarantee that those experiences did not shape their incident response techniques in the civilian world. So, while distinguishing between government, military, law enforcement, and civilian experiences was necessary, the researcher was not able to select candidates with absolutely no experience in these areas. However, a targeted study excluding any history of these experiences is unlikely to yield drastically different approaches.

A portion of this study was dedicated to issues such as cyber warfare or terrorism; however, no direct evidence was presented by organizations to support or deny the potential of these types of actions. Only one of the incidents reported in this study was believed to have been the work of a military or nation state for the purpose of making war against a target. The threat of terrorism was only mentioned by three participants including a situation that nearly resulted in the deaths of several people. The literature review indicated that the potential exists for civilian organizations to be targets during military operations in cyberspace. The majority of private organization incidents referenced in this study were believed to have been caused for criminal purposes but that does not mean that war type actions are not possible. The incidents reported that dealt with state-sponsored actions and the potential for human causalities show it to be a real threat. A future study may address this threat by specifically targeting the lived experiences of organizations that have experienced what they believe to be the work of nation states or terrorists conducting information security attacks against their information assets.

Implications of the Results for Practice

On the basis of these findings, the greatest contribution of this study to the field is the knowledge of the successes and failures of current practices. The results of this study indicate how information incident response generally flows as well as the importance of having a plan to address incident response. The lessons learned by participants and related through this study should be incorporated into already existing incident response plans practiced in the field as well as used to create new ones. Identifying the essential elements of an incident response plan before an incident is critical. Implementing these essential elements in the field is relatively easy and would provide organizations with increased value from their incident response and information security programs.

The results of this study also indicated the importance of training the plan, specifically, in addressing the human elements of security in relation to incident response. Humans are a major part of information security incident management from the detection of the event through the implementation of remediating controls. Training people outside of information security is not a new suggestion. It is notoriously difficult to get the average user, manager, or IT administrator to incorporate information security into their common practices. Despite the obvious benefit to improving this training it is unlikely that this will be easily implemented in the field; but, security professionals should consider incorporating additional training for incident response for organizations. Addressing these two common failures can provide incident responders in the field with additional resources and organizations with greater value in incident response.

Results of the study also reflected the complex relationship that incident responders and organizations have with third parties including other information security professionals as well as government, law enforcement, and the military. Sharing information among security professionals, academics, and even the government is perhaps the most significant hurdle to overcome in relation to understanding the various complex topics around the field of information security which includes incident management. The benefits of sharing information were demonstrated in the lived experiences of these participants and in the results of this study. The conclusions regarding sharing information will likely have little impact on the field despite their importance. There are many roadblocks to sharing this information including the negative relationship between information sharing and regulatory fines and customer confidence.

In addition to sharing information with each other it is recommended that security professionals and organizations work together with law enforcement, government, and military organizations to address the larger problem of information security incidents. This does not have to include going after attackers to bring them to trail for their crimes. The government, military, and law enforcement all have various resources that can be used to assist private industry as demonstrated by the positive experiences working with these organizations presented by the participants. In several instances when these relationships were used productively they resulted in increased value to the private organization with mutual benefit to the third party by sharing more knowledge about incidents. Even if this relationship is relegated to sharing information about malicious IP addresses it would severely curtail the amount of malicious traffic on the Internet and force organizations to work harder to compromise systems. While it is unlikely that this implication will be swiftly implemented in the field it is certainly something that organizations would benefit from considering in the future.

Recommendations for Further Research

In future research it should be possible to widen the demographic range and include a more diverse group of information security professionals from different counties. The varied insights of these groups should provide more detailed information on the lived experiences regarding information security incidents. Future research is necessary to examine the lived experiences of alternative populations such as military, government, and law enforcement professionals with experience in information security incident management. There is a lack of understanding of the experiences of these populations as their experiences are expected to be different than those of private-sector professionals.

While the experiences of these 18 professionals have indicated several trends it is recommended that a quantitative study be performed to pose questions based on these trends to a larger population. This may shed some additional insights into the subject area based on these conclusions. This study was also limited to a single region of one nation. The culture of the Pacific Northwest in the United States is largely against law enforcement, government, and criminal punishment. Potential research opportunities may also include focusing on alternative population regions which may have different views on law enforcement and aggressive measures based on their culture.

Conclusion

In conclusion, this research project was designed to address a specific research problem and set of research questions centered on the lived experiences of information security professionals and the phenomena of information security incidents. After an extensive review of the existing literature a research model was designed. The researcher systematically carried out the research design and collected data on the lived experiences of each participant using the instrument developed for this study. These experiences were then analyzed using phenomenological methods to reach the essence of the phenomenon and answer the research question. The conclusions reached in this study answered the research questions and serve to help practitioners in the field as well as researchers in future research projects. These results may assist organizations in implementing information security incident response programs and improving their capabilities over time. The lessons learned from the lived experiences of these participants are invaluable. Future research studies may test these results in a quantitative context, examine female perspectives and decision making in incident response situations, examine the working relationship between the private sector and government, military, and law enforcement in relation to incident response, as well as incident response for government, military, and law enforcement organizations.

REFERENCES

Ahmad, A., Hadgkiss, J., & Ruighaver, A. (2012). Incident response teams—Challenges in supporting the organizational security function. *Computers & Security, 31*(5), 643-652.

Al-Rizzo, H. (2008). The undeclared cyberspace war between Hezbollah and Israel. *Contemporary Arab Affairs*, *1*(3), 391-405.

Amancei, C. (2011). Practical methods for information security risk management. *Informatica Economica, 15*(1), 151-159.

American Psychological Association. (2010). *Ethical principles of psychologists and codes of conduct: 2010 amendments.* Washington, DC: Author. Retrieved from http://www.apa.org/ethics/code/index.aspx

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

Arquilla, J. (2011). From blitzkrieg to bitskrieg: The military encounter with computers. *Communications of the ACM*, *54*(10), 58-65.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, *8*(2), 33-56.

Bartoli, A., Davanzo, G., & Medvet, E. (2010). A framework for large-scale detection of web site defacements. *ACM Transactions on Internet Technology*, *10*(3), 1-37.

Blyth, A., & Thomas, P. (2006). Performing real-time threat assessment of security incidents using data fusion of IDS logs. *Journal of Computer Security, 14*(6), 513-534.

Bowles, M. (2012). The business of hacking and birth of an industry. *Bell Labs Technical Journal*, *17*(3), 5-16.

Brenner, S. W. (2004). U.S. cyber-crime law: Defining offenses. *Information Systems Frontiers*, *6*(2), 115-132.

Brown, S., & Burkhead, R. (2012). Active defense: Corporate warfare. *International Forum of Researchers Students and Academician (IFRSA)* Call for Papers, October 2012. [Accepted, but withdrawn due to lack of funds.]

Burkhead, R. (2009). *Information technology preparation of the environment* (Unpublished Master's thesis). Western International University, Phoenix AZ.

Butts, J., Rice, M., & Shenoi, S. (2012). An adversarial model for expressing attacks on control protocols. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 9*(3), 243-255.

Cane, S., McCarthy, R., & Halawi, L. (2010). Ready for battle? A phenomenological study of military simulation systems. *Journal of Computer Information Systems*, *50*(3), 33-40.

Chan, A. K., Hyung, W. P., & Hoon, D. L. (2013). A study on the live forensic techniques for anomaly detection in user terminals. *International Journal of Security & its Applications*, *7*(1), 181-188.

Chu, H., Deng, D., & Chao, H. (2011). An ontology-driven model for digital forensics investigations of computer incidents under the ubiquitous computing environments. *Wireless Personal Communications*, *56*(1), 5-19.

Cobb, J. (2011). Centralized execution, decentralized chaos. *Air & Space Power Journal*, *25*(2), 81-86.

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*. Los Angeles, CA: SAGE.

Davis, A. (2012). Hacktivism. *ITnow, 54*(2), 30-31.

Dawley, S. M. (2013). A case for a cyberspace combatant command. *Air & Space Power Journal*, *27*(1), 130-142.

Dayton, D. K. (2011). *Communicating organizational quality: A phenomenological study through the lenses of complexity leadership and organizational learning theories* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3473159)

Denning, P. J., & Denning, D. E. (2010). The profession of IT discussing cyber attack. *Communications of the ACM*, *53*(9), 29-31.

Department of the Army. (1994). *FM 34-130: Intelligence preparation of the battlefield*. Washington, DC: Department of Defense.

Drtil, J. (2013). Impact of information security incidents: Theory and reality. *Journal of Systems Integration*, *4*(1), 44-52.

Elachgar, H., Boulafdour, B., Makoudi, M., & Regragui, B. (2012). Information security, 4th wave. *Journal of Theoretical & Applied Information Technology*, *43*(1), 1-7.

Etzioni, A. (2011). Cybersecurity in the private sector. *Issues in Science & Technology, 28*(1), 58-62.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communications of the AIS*, *28,* 329-356.

Filshtinskiy, S. (2013). Cyber-crime, cyberweapons, cyber-wars: Is there too much of it in the air? *Communications of the ACM*, *56*(6), 28-30.

Flood, A. (2010). Understanding phenomenology. *Nurse Researcher, 17*(2), 7-15.

Geers, K. (2010). Live fire exercise: Preparing for cyber war. *Journal of Homeland Security and Emergency Management*, *7*(1), 1-16.

Gervais, M. (2012). Cyber attacks and the laws of war. *Berkeley Journal of International Law*, *30*(2), 525-579.

Gikas, C. (2010). A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS standards. *Information Security Journal: A Global Perspective*, *19*(3), 132-141.

Gill, M. (2014). The possibilities of phenomenology for organizational research. *Organizational Research Methods, 17*(2), 118-137.

Giorgi, A. P. (2009). *The descriptive phenomenological method in psychology: A modified Husserlian approach.* Pittsburgh, PA: Duquesne University Press.

Greengard, S. (2010). The new face of war. *Communications of the ACM, 53*(12), 20-22.

Guitton, C. (2012). Criminals and cyber attacks: The missing link between attribution and deterrence. *International Journal of Cyber Criminology, 6*(2), 1030-1043.

Gupta, M., Chaturvedi, A., & Mehta, S. (2011). Economic analysis of tradeoffs between security and disaster recovery. *Communications of the AIS, 1*, 281-316.

Halfond, W. J., Choudhary, S., & Orso, A. (2011). Improving penetration testing through static and dynamic analysis. *Software Testing: Verification & Reliability*, *21*(3), 195-214.

Hanser, R. D. (2011). Gang-related cyber and computer crimes: Legal aspects and practical points of consideration in investigations. *International Review of Law, Computers & Technology*, *25*(1), 47-55.

Herre, H. (2013). Formal ontology and the foundation of knowledge organization. *Knowledge Organization*, *40*(5), 332-339.

Heuer, R. J., Jr. (1999). *Psychology of intelligence analysis*. Langley Falls, VA: Central Intelligence Agency.

Hua, J., & Bapna, S. (2013). Who can we trust? The economic impact of insider threats. *Journal of Global Information Technology Management, 16*(4), 47-67.

Hu, Y., Chen, X., & Bose, I. (2013). Cybercrime enforcement around the globe. *Journal of Information Privacy & Security*, *9*(3), 34-52.

Hyman, P. (2013). Cybercrime: It's serious, but exactly how serious? *Communications of the ACM*, *56*(3), 18-20.

Kadlec, C., & Shropshire, J. (2010). Best practices in IT disaster recovery planning among US banks. *Journal of Internet Banking & Commerce, 15*(1), 1-11.

Kim, S., Wang, Q., & Ullrich, J. (2012). A comparative study of cyber-attacks. *Communications of the ACM, 55*(3), 66-73.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, 9*(3), 49-51.

Lanter, A. (2011). Are you ready? Getting back to business after a disaster. *Information Management Journal, 45*(6), 4.

Lin, P., Allhoff, F., & Rowe, N. (2012). Computing ethics war 2.0: Cyberweapons and ethics. *Communications of the ACM, 55*(3), 24-26.

Lobel, H. (2012). Cyber-war INC.: The law of war implications of the private sector's role in cyber conflict. *Texas International Law Journal*, *47*(3), 617-640.

O'Kelly, K., & Trott, B. (2014). The spies' guide to cyberspace. *Reference and User Service Quarterly, 53*(3), 206-208

Perez, E., Prokupecz, S., & Cohen, T. (2014, May 19). More than 90 people nabbed in global hacker crackdown. *CNN*. Retrieved from: http://edition.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/index.html?hpt=hp_t3

Pieters, W. (2011). The (social) construction of information security. *Information Society*, *27*(5), 326-335.

Pusey, P., & Sadera, W. (2012). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88.

Rajakumar, M., & Shanthi, V. (2014). Security breach in trading system countermeasure using IPTraceback. *American Journal of Applied Sciences, 11*(3), 492-498.

Rid, T. (2011). Cyber-war will not take place. *Journal of Strategic Studies, 35*(1), 5-32.

Rozendaal, M. C., & Schifferstein, H. J. (2010). Pleasantness in bodily experience: A phenomenological inquiry. *International Journal of Design*, *4*(2), 55-63.

Schuesster, J. H. (2013). Contemporary threats and countermeasures. *Journal of Information Privacy & Security*, *9*(2), 3-20.

Shaw, A. (2010). Data breach: From notification to prevention using PCI DSS. *Columbia Journal of Law & Social Problems*, *43*(4), 517-562.

Simundic, A. (2013). Bias in research. *Biochem Med, 23*(1), 12-15.

Sindhu, K. K., & Meshram, B. B. (2012). Digital forensics and cyber crime datamining. *Journal of Information Security, 3*(3), 196-201.

Stapleton, R., & Woodcock, W. (2011). National internet defense small states on the skirmish line. *Communications of the ACM, 54*(3), 50-55.

Stegmaier, G. M., & Bartnick, W. (2013). Another round in the chamber: FTC data security requirements and the fair notice doctrine. *Journal of Internet Law*, *17*(5), 1-35.

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal, 11*(2), 63-75.

Symantec. (2013). *Internet security threat report*. Mountain View, CA: Author.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology, 25*(1), 105-120.

Tammineedi, L. (2010). Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective, 1,* 36-49.

Thomas, M., & Dhillon, G. (2012). Interpreting deep structures of information systems security. *Computer Journal*, *55*(10), 1148-1156.

Tohidi, H. (2011). The role of risk management in IT systems of organizations. *Procedia Computer Science, 3*, 881-887.

Urbas, G. (2012). Cybercrime, jurisdiction and extradition: The extended reach of cross-border law enforcement. *Journal of Internet Law*, *16*(1), 1-17.

Van Gent, R. D., Lindquist, T. M., & Smith, G. (2013). The six million dollar man. *CPA Journal*, *83*(9), 70-72.

Van Manen, M. (2014). *Phenomenology of practice*. Walnut Creek, CA: Left Coast Press.

Verizon. (2012). *2012 data breach investigations report*. Basking Ridge, NJ: Author.

Verizon. (2013). *2013 data breach investigations report*. Basking Ridge, NJ: Author.

Vorobiev, A., & Bekmamedova, N. (2010). An ontology-driven approach applied to information security. *Journal of Research & Practice in Information Technology*, *42*(1), 61-76.

Vuorinen, J., & Tetri, P. (2012). The order machine: The ontology of information security. *Journal of the Association for Information Systems*, *13*(9), 695-713.

Walker, J. L. (2012). The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing*, *22*(2), 37-41.

Wang, J., Guo, M., Wang, H., & Zhou, L. (2012). Measuring and ranking attacks based on vulnerability analysis. *Information Systems & E-Business Management*, *10*(4), 455-490.

Warren, M., & Leitch, S. (2010). Hacker taggers: A new type of hackers. *Information Systems Frontiers, 12*(4), 425-431.

Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management & Computer Security, 18*(1), 26-42.

Zhongqiang, C., Yuan, Z., & Zhongrong, C. (2010). A categorization framework for common computer vulnerabilities and exposures. *Computer Journal, 53*(5), 551-580.

APPENDIX A. STATEMENT OF ORIGINAL WORK

Academic Honesty Policy

Capella University’s Academic Honesty Policy (3.01.01) holds learners accountable for the integrity of work they submit, which includes but is not limited to discussion postings, assignments, comprehensive exams, and the dissertation or capstone project.
Established in the Policy are the expectations for original work, rationale for the policy, definition of terms that pertain to academic honesty and original work, and disciplinary consequences of academic dishonesty. Also stated in the Policy is the expectation that learners will follow APA rules for citing another person’s ideas or works.

The following standards for original work and definition of *plagiarism* are discussed in the Policy:

> Learners are expected to be the sole authors of their work and to acknowledge the authorship of others’ work through proper citation and reference. Use of another person’s ideas, including another learner’s, without proper reference or citation constitutes plagiarism and academic dishonesty and is prohibited conduct. (p. 1)
>
> Plagiarism is one example of academic dishonesty. Plagiarism is presenting someone else’s ideas or work as your own. Plagiarism also includes copying verbatim or rephrasing ideas without properly acknowledging the source by author, date, and publication medium. (p. 2)

Capella University’s Research Misconduct Policy (3.03.06) holds learners accountable for research integrity. What constitutes research misconduct is discussed in the Policy:

> Research misconduct includes but is not limited to falsification, fabrication, plagiarism, misappropriation, or other practices that seriously deviate from those that are commonly accepted within the academic community for proposing, conducting, or reviewing research, or in reporting research results. (p. 1)

Learners failing to abide by these policies are subject to consequences, including but not limited to dismissal or revocation of the degree.

Statement of Original Work and Signature

I have read, understood, and abided by Capella University's Academic Honesty Policy (3.01.01) and Research Misconduct Policy (3.03.06), including the Policy Statements, Rationale, and Definitions.

I attest that this dissertation or capstone project is my own work. Where I have used the ideas or words of others, I have paraphrased, summarized, or used direct quotes following the guidelines set forth in the APA *Publication Manual*.

Learner name
and date Randy Lee Burkhead 17OCT2014

Mentor name
and school Dr. Bernard Sharum School of Business and Technology