2014

Understanding Usability-related Information Security Failures in a Healthcare Context

Edward D. Boyer
Nova Southeastern University, edboyer@bellsouth.net

NSUWorks Citation

Edward D. Boyer. 2014. *Understanding Usability-related Information Security Failures in a Healthcare Context.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (13) http://nsuworks.nova.edu/gscis_etd/13.

Understanding Usability-related Information Security Failures in a Healthcare Context

by

Edward D. Boyer

A Dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

Graduate School of Computer and Information Sciences

Nova Southeastern University

2014

We hereby certify that this dissertation, submitted by Edward Boyer, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Gurvirender P. Tejay, Ph.D. Date
Chairperson of Dissertation Committee

Ling Wang, Ph.D. Date
Dissertation Committee Member

Maxine S. Cohen, Ph.D. Date
Dissertation Committee Member

Approved:

Eric S. Ackerman, Ph.D. Date
Dean, Graduate School of Computer and Information Sciences

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Understanding Usability-related Information Security Failures in a Healthcare Context

by
Edward D. Boyer
September 2014

This research study explores how the nature and type of usability failures impact task performance in a healthcare organization. Healthcare organizations are composed of heterogeneous and disparate information systems intertwined with complex business processes that create many challenges for the users of the system. The manner in which Information Technology systems and products are implemented along with the overlapping intricate tasks the users have pose problems in the area of usability. Usability research primarily focuses on the user interface; therefore, designing a better interface often leaves security in question. When usability failures arise from the incongruence between healthcare task and the technology used in healthcare organizations, the security of information is jeopardized. Hence, the research problem is to understand the nature and types of usability-related security failures and how they can be reduced in a Healthcare Information System.

This research used a positivist single case study design with embedded units, to understand the nature and type of usability-related information systems security failures in a Healthcare context. The nature and types of usability failures were identified following a four-step data analysis process that used terms that defined (1) user failures in a large healthcare organization, (2) Task Technology Fit theory, (3) the Confidentiality Integrity and Availability triad of information protection that captured usability-related information system security failures, and (4) by conducting semi-structured interviews with users of the Healthcare Information System capturing and recording their interactions with the usability failure.

The captured reported usability-related information system security failures dated back five years within a healthcare organization consisting of a network of 128 medical centers. The evaluation of five years of data and over 8,000 problems reported by healthcare workers allowed this research to identify the misalignment of healthcare task to the technology used, and how the misalignment impacted both information security and user performance. The nature of usability failures were centered on technical controls, however, the cause of the failures was predominately information integrity failures and the unavailability of applications and systems. Usability-related information system security failures are primarily not recognized due to the nature of healthcare task along with the methods healthcare workers use to mitigate such failures by

employing workarounds to complete a task. Applying non-technical security controls within the development process provides the clearest path to addressing throughout the organization the captured usability-related information system security failures.

Acknowledgements

This journey began based on an excuse that I recognized and understood to be fear. The fear of thinking I was not smart enough or good enough to obtain a PhD was the genesis of this journey. I would like to thank God for his grace and favor that materialized throughout this process. By aligning myself with the beautiful spirits of all that guided me was essential to me learning the personal lessons that will continue to guide me. I want to thank everyone that contributed to this major undertaking. The contributions went far beyond intellectual contributions. It was the spirit, energy, and encouragement that both my friends and coworkers provided that allowed me to continue on my journey. I would first like to thank the employees of the Veterans Administration that participated in this project. Interacting with them all as they displayed their passion and dedication to support the Veterans that has kept us safe and free simply makes me proud to know them as well as work alongside them.

I also would like to thank my advisor Dr. Gurvirender P. Tejay. There is no doubt; I would not have been able to accomplish this feat without his guidance and support. I simply cannot come up with the words to describe what he meant to me throughout this process. I am ever so thankful and appreciative that we embarked upon this journey together. I would also like to thank my dissertation committee members, Dr. Maxine S. Cohen, and Dr. Ling Wang for dedicating their time ensuring I created a project I am quite proud of.

Lastly, I would like to thank my wife Quawanda and daughters Nedra and Deyla for simply believing in me, and providing the additional positive energy and support needed to reach this major milestone in our lives. This journey was indeed an affair for the family.

Table of Contents

Chapters

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

1.1 Background

The healthcare industry faces well-recognized challenges such as high cost of operations, inefficiencies, inadequate safety, and insufficient access to information. Past and present United States Presidents have mandated restructuring the healthcare industry to alleviate many of these current problems. This has led to healthcare organizations becoming more connected through Information Technology (IT) both locally and globally using heterogeneous and disparate Health Information Systems (HIS) to access and share information. These HIS consist of clinical, management, strategic decision support, and electronic network and e-health applications (Austin & Boxerman, 2003). The use of heterogeneous and disparate systems within the highly collaborative healthcare environment can become problematic, creating usability failures when applications and systems converge to retrieve, transport, and deliver information between these systems (Bardram, 2005). Usability failures become an organizational security issue when providing HIS users a means to access information in a timely and secure manner (Braz & Robert, 2006). This research focuses on understanding usability-related information systems security failures in a healthcare organization and how such failures impact IS security performance in a healthcare organization.

For this research study, usability failures affect users in phases if left untreated. The first phase is the initial failure from a user interaction (usability failure) with an application or system. The first phase consists of the user's inability to access the application or system. For this research study, a usability failure emanates from the user's inability to access an application or system with the sole purpose to obtain information to complete a task. The usability failure could be driven by not remembering a password or it could be technical in nature. The user will react to the failure and articulate the constraints that the failure has caused. If left untreated, the usability failure creates the second phase—a usability security failure. A usability security failure occurs when information from the initial usability failure is not presented from the interface in a manner that allows the user to take the necessary security precautions with the system (Sheng, Broderick, Koranda, & Hyland, 2006; Whitten & Tygar, 1999). Usability security failures are directly linked to IS security failures. For this research, an information systems security failure is the most severe security failure, and it primarily occurs when users of a system have to create alternative methods not prescribed by the organization to complete an assigned task precipitated from usability failures. The effects of the usability failure determines whether an information systems security failure exists and the responses of the users can further determine the types of security controls an organization has in place.

In the areas of usability security, researchers primarily have evaluated methods and techniques in designing secure user interfaces while improving the human interaction with a computer system (Flechais, Mascolo, & Sasse, 2007). However, usability security encompasses a great deal more, as Al-Ghatani and King (1999) and Markus (1983) claim poor usability design evokes a greater degree of user resistance. Greater user resistance, particularly in healthcare settings, means users are likely to denigrate the system, sabotage the computer equipment, tamper with the data, or abandon the new systems and continue to use the old system (Worthley, 2000). Within a healthcare context, any of these behaviors is at best undesirable and, at worst, may lead to the quality of patient care to be questioned. Whitman (2004) identified and ranked technical software failures or errors, deliberate acts of sabotage or vandalism, and technical hardware failure or errors as threats to information security. These information security threats are fallout from usability failures.

Bhattacherjee and Hikmet's (2007) research on user physician resistance reported that physicians at Cedars-Sinai hospital in Los Angeles, California, rebelled against a new computerized physician order entry system, complaining that the system distracted them from their medical duties, which ultimately led to the removal of the system. The research findings suggested the resistance was caused by the perceived threat of losing control over their work procedures. In similar healthcare usability literature, Johnson, Johnson, and Zhang (2005) stated that healthcare software developers often overlook relevant user characteristics, user tasks, user preferences, and usability issues, resulting in systems that decrease productivity or simply remain unusable. Overlooking user needs in the software development process can negatively impact the acceptance and use of a newly implemented software or hardware system.

In healthcare organizations, the processes by which patient care is provided are defined by the user task and user characteristics; therefore, productivity and system availability become huge issues. When a user suffers from a failed interaction with an application or a system interface from a poorly designed business process prevents the user from a completing a task, the user will seek other means to complete that task. Other means of completing a task are done by the user circumventing established business processes and security controls (Eckman, Bennett, Kaufman, & Tenner, 2007; Johnson & Willey, 2011). The user behavior from the failed interaction is essentially the embarkation point on the road towards a usability security failure.

A usability-related information systems security failure occurs when information is unable to be accessed, delivered, mishandled, misinterpreted, or is altered by the user from a failed interaction with an application or system. The failed interaction may cause the user to intentionally or unintentionally violate the organization's security policies to complete a task. Information that is unable to be properly protected from user interactions have been researched under the technical domain of IT security, i.e., encryption, data, software and hardware controls (Anderson, 1972; Sandhu, Coyne, Feinstein, & Youman, 1996; Schneier, 1996). This researcher argues that focusing specifically on technical aspects of security problems creates an unbalanced approach of addressing security issues within an organization; therefore, security failures must be addressed by both technical and non-technical means.

As organizations redesign and implement business processes for their Information Systems (IS), the systems development process provides organizations a method to analyze, design, test, and implement business processes to address usability-related information systems security failures (Siponen, 2001). According to Yee (2004), there is a conflict in the systems development process aligning security and usability, since “usability improvements yield compromised software, and adding security measures have made software tedious to use or hard to understand” (p.48). This is particularly true and problematic in healthcare organizations, which are characterized by non-traditional work environments that use heterogeneous HIS, where the work flows is often mobile, high-paced, chaotic, and highly collaborative (Bardram, 2005). Bardram (2005) has argued usability-related security failures associated with login mechanisms have not recognized the nature of medical work; therefore, the consequence has led to login procedures being circumvented and the security of the organization being jeopardized.

Essentially, an application or system failure and usability security failures share a symbiotic relationship. In fact, usability security failure is defined as not having reliable software that allows expected users to be made aware of the security tasks they need to perform (Sheng et al., 2006; Whitten & Tygar, 1999). A security task in the healthcare context is a business process that provides information to the user through an interface during the usability failure on the next step a user should take in the process after the failure occurs. In essence, it is a security control that protects the organization's information assets.

In a healthcare organization, usability-related information systems security failures can be fatal. The consequences of usability-related information systems security failures were highlighted in 1999 Institute of Medicine reports stating that 44,000 to 98,000 Americans die each year from preventable medical errors, and that medical errors cost the United States $37.6 billion each year. The errors were a byproduct of misaligned business processes that were created by information-handling failures in effectively diagnosing and treating patients. The information-handling failure arose from systems and communications failures that caused misinterpretation of information by patients and physicians (Dennison, 2005).

The primary focus of usability security has been on user authentication and email encryption (Payne & Edward, 2008). Thus, there has been very little identifiable research in the domain of usability security that has addressed the impact usability failures have on the accomplishment of healthcare tasks and usability-related information systems security failures. The aim of this research is to identify and enhance the understanding of usability-related security failures and how the failures impact IS security performance in a healthcare organization.

1.2 Problem Statement

The research problem for this study is to understand the nature and types of usability-related security failures and how they can be reduced in a HIS. Ka-Ping (2002) and Whitten and Tygar (1999) have stated that usability security research focuses on providing better user interfaces in the area of human computer interaction. However, usability security is much more than user interfaces; it is the information from the interaction conveyed by the user interface, the domain in which the user belongs, and the interpretation of the actions of the user that must be considered when evaluating the ramifications of usability-related security failures. Developing a method to identify and understand the nature of usability-related security failures within a HIS allows an organization's staff to effectively incorporate security controls. These security controls can help address the information systems security risk users' encounter interacting with applications and systems of an HIS.

Understanding usability-related information systems security failures encountered by users of HIS will allow for researchers and practitioners to better understand and address information systems security risks as these risks have the potential to negatively affect patient care information in the healthcare setting. Researchers have argued that there is a need to address usability security controls in the software development process (Schecter, Dhamija, Ozment, & Fischer, 2007) along with a need to add security controls throughout the software development process (Baskerville, 1988). However, there has been little evidence that organizations have adopted and succeeded at this approach. This researcher argues that, to reduce usability security failures, organizations must align security technology with tasks performed by healthcare workers and ensure such alignment does not hamper security performance in a healthcare organization.

1.3 Research Question

The first research question of the proposed study is *what are the nature and types of usability-related information systems security failures in a HIS?* HIS are comprised of heterogeneous and disparate data and systems used to deliver healthcare to patients. According to Marcus (2002), the interaction a user has with a computer creates inputs and outputs at the local and global levels. Local-level feedback consists of the information returned from peripheral devices from monitors or printers, while the global level feedback references contextual issues and task activities from applications and systems from within or outside of an organization. It is the very nature of interactions HIS users have along with the information returned from the feedback of the interactions at the local and global levels that will determine the source and type of usability-related information systems security failure existing within an organization. The source and type of usability-related information systems security failure determines the behavior of the application, system and user. In the literature review section, Jacobson, Booch, and Rumbaugh (1999) identified nine types of usability failures that can essentially create a reaction from IS users. Capturing the sources and types of usability failures along with understanding the interactions between the user, task, and application or system wherein the security failure occurs allows the organization to determine the type of interventions that are required.

The second research question is *how does usability-related information systems security failures impact task accomplishment in a healthcare setting?* The antecedent of a usability-related information systems security failure is a usability failure occurring when a user encounters a failed interaction from the application or system in use. Researchers of usability failures have analyzed improving the user experience by improving a user interface (e.g., Flechais et al., 2007) in an effort to reduce the behavior of system users in rejecting, rebelling against or misusing the system. This approach has proven to be problematic as users may experience an improvement on the interface, but security is also compromised in the design process. The outlying problem in usability security design is it is resolved at the technical level (Payne & Edward, 2008), which creates potential information risk in an organization's security program by not using a balanced approach. Usability research has also shown that a usability failure may cause users of an HIS to circumvent the system to complete a task (Johnson & Willey, 2011), create their own workarounds (Halbesleben, Wakefield, & Wakefield, 2008), or reject the system entirely. There has been very little research that has taken the perspective of evaluating the congruence of usability-related information systems security failures in relation to how the technology fits the task of the user, and how that fit impacts the performance of the user. Diagnosing task-technology-fit in reference to a usability failure creates opportunities to detect where information security failures occur.

1.4 Key Definitions

For this research study, four terms are important to shape the context of this research through the use of definitions. In order to assign a definition to information, one must follow the path information travels in order to be used by the receiver. When information is described or defined in research, it is often done using the Data-Information-Knowledge (DIK) hierarchy. DIK is grounded in IT to distinguish the differences and the roles DIK plays within an organization. Data are often viewed as being raw and simply exist without any significance. Tejay, Dhillon, and Chin (2005) assert that data are a fundamental information asset, while Dhillon and Backhouse (2001) acknowledge the primary focus of IS security is on data. When context is added to data, they are transformed into information, and that information then becomes knowledge that can be used by the receiver. The path in which data travel and transform allows this study to take on the definition of *information* per Avison and Fitzgerald (1995) as the meaning that comes from selecting, summarizing and presenting data in such a way that becomes useful to the recipient.

The term *information systems* has often been defined by researchers as the way in which computer systems provide information in support of organizational structure, business processes, and people. The information system definition is often interpreted by researchers using three levels. Iivari and Hirchheim (1996) described their three levels as the organization level, which is the host organization, the language level, encompassing the formalized rules of communicating transmitted and received information by users in the organization, and the technical level, consisting of the computer systems used in the organization. The three levels imply that information must be managed beyond technical means to account for social and organizational roles information has within an organization. For the purpose of this research, an *information system* is considered an aggregate of information-handling activities at the technical, formal and informal levels of an organization (Liebenau & Backhouse, 1990). The technical, formal, and informal levels of an information system can be visualized using the components of a hard-boiled egg as the point of reference. The technical system is the yolk consisting of the IT used in an organization, the formal system is the egg white, encompassing the rules, and policies created within an organization, and the informal system is the shell, which is viewed as the organizational culture. The three components combine to form the automation and coordination of information-handling activities along with providing guidance to the information users.

In respect to *information systems security*, it has been viewed as providing technical means to secure the infrastructure of an organization. Information systems consist of information-handling activities at the technical, formal and informal levels respectively; therefore, security controls must be addressed and balanced at all three levels to mitigate risk in an organization. In this research study, *information systems security* is defined as a well-informed sense of assurance that information risks and controls are in balance (Anderson, 2003). Information is an asset in an organization that has varying levels of value. The value of the information determines the level of controls along with the level of resources that should be committed to protect the information. The amount of resources committed to protect information should not outweigh the value of the information; therefore, a balance and “sense of assurance” is obtained when protecting information assets.

There are a host of usability definitions held by researchers in the domain of human computer interaction that centers on adding quality and value to the user’s experience. Usability is often defined based on how it is viewed along with how it should be measured (Bevan, Karakowski, & Maissel, 1991). The product-oriented view measures ergonomic attributes, the user-oriented view measures the mental effort and attitude of the user, and the user-performance view examines how the user interacts with the product, seeking to measure ease-of-use and acceptability of the product (Bevan et al., 1991). This research will adopt the definition proposed by ISO 9241-11 (1998) as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. This definition encompasses the entire user experience interacting with an IS.

1.5 Summary

Usability failures can become an organizational security issue when providing HIS users a means to access information in a timely and secure manner. In the areas of usability security, researchers have primarily evaluated methods and techniques in designing secure user interfaces while improving the human interaction with a computer system (Flechais, Mascolo, & Sasse, 2007). However, usability security encompasses a great deal more, particularly when researchers have linked usability failures to user resistance, sabotage of computer equipment, tampering with data or creating their own workarounds. This can be highly problematic within a healthcare organization; thus, the premise of this research study is to understand the nature and types of usability-related security failures and how they can be reduced in a HIS.

Chapter 2

Literature Review

2.1 Introduction

The aim of this chapter is to provide an understanding of the extant literature in the area of usability, while highlighting the gaps in the usability domain that provide opportunities to use IS security practices to improve the organizational security program. The review of usability and IS security literature was conducted following the methods of Ellis and Levy (2006). Papers were selected and examined from key researchers in the Human Computer Interaction (HCI) and IS security fields emphasizing the search criteria under the research domains of usability and IS security development. The underlined argument of this literature review is usability failures lead to IS security failures if not addressed, but can be reduced by aligning healthcare tasks with the technology within an HIS. This can be accomplished by applying the proper IS security controls.

2.2 IS Security

In this research study, the IS security context follows the views of Dhillon and Backhouse (2000), Liebenau and Backhouse (1990), and Klein and Hirschheim (1987) which consider an organization is constituted of informal, formal, and technical parts. The technical, formal, and informal parts must be addressed at each level in the form of information systems security controls that are balanced in an organization. To ensure information security controls are applied accurately, the organization’s risk management program must assess IT resources and information assets to identify threats and vulnerabilities and apply the appropriate measures to mitigate the risk.

2.2.1 *Technical Security*

The intent of technical security is to secure computer resources such as hardware, software, and the data that reside in a computer system (Dhillon, 2007). Dhillon stated that hardware, software, and data are primarily vulnerable to six threats: (a) data modification, (b) destructions, (c) disclosure, (d) interception, (e) interruption, and (f) fabrication. Data modification occurs when data held in the computer system are accessed and changed without permission. Destruction occurs when hardware, software, or data are destroyed because of malicious intent. Disclosure happens when data are made available or access to software is made available without consent. Interception occurs when an unauthorized person or software application gains access to data or computer resources, and interruption is when a computer system becomes unavailable for use. The final threat, fabrication, happens when unauthentic transactions or records are inserted or added to an organization’s database system. At the technical level, data are one of the resources that organizations seek to protect by applying technical controls.

One stream of research has dealt with controls for securing data itself, often using different types of encryption (Blythe, 2008). A second research stream has focused on the use of digital signatures to facilitate trusted transactions between parties (Blythe, 2008; Rivest, 1978; Tompkins & Handley, 2003). Software controls seek to secure infrastructures from the inside by strengthening the applications that are present on IS (August & Tunca, 2006; Shimeall &

McDermott, 1999). Finally, many studies have focused on numerous hardware solutions, including intrusion detection and firewalls (Denning, 1987; Frincke, 2000; Vigna & Kemmerer, 1999).

2.2.2 *Data Security Requirements*

Data security requirements are linked to the classic CIA (Confidentiality, Integrity, and Availability) triad of information protection (Dunkerley, & Tejay, 2009). Confidentiality is the prevention of unauthorized disclosure of information, integrity is the guarantee that the message sent is the same as the message received, and availability is the guarantee that information will be available to the user in a timely and uninterrupted manner. With the advent of networked organizations and the usage of the Internet in reference to Electronic Commerce, authentication and non-repudiation have been discussed as important security requirements based on the context of application and system use. Authentication guarantees the message is from the source it claims to be from, and non-repudiation prevents an individual or entity from denying having performed a particular action related to data (Siponen & Oinas-Kukkonen, 2007); however, for this research study, the CIA triad will be the area of focus in relation to technical security controls.

Technical security controls in relation to the CIA triad focus on protecting the resources of systems through the means of authentication and access control (Siponen & Oinas-Kukkonen, 2007). Authentication methods include passwords (Denning, 1992) and token-based authentication using special purpose devices such as smart cards (Hendry, 1997). Authenticating with a password is primarily done through passwords mechanisms such as (a) traditional passwords, (b) system-generated passwords, (c) passphrases, (d) cognitive passwords and (e) associative passwords (Zviran & Haga, 1993). The goal of access control is to guarantee that the requirements of integrity, availability, and confidentiality of security objects are not compromised. Security objects (resources) are files, directories, tuples, or relations (Sandhu, 1993). Access control includes the prevention of all unwanted flows of information between objects and subjects, including any flows of information that could be used to attain information, which needs to be secure (Siponen & Oinas-Kukkonen, 2007) Access control techniques includes access matrix (Mclean, 1990), mandatory, discretionary, and role-based access control policies (Boswell, 1995; Sandhu & Samarati, 1996). Access control matrixes are a means of establishing the type of access control policies that will be applied to an organization, while mandatory, discretionary, and role-based access control policies are applied based on the type of access control matrix that will best benefit the users and resources that are being protected in an organization.

2.2.3 *Risk Management*

Organizations apply risk management techniques using both quantitative and qualitative methods. According to Saleh and Alfantookh (2011), there are over 200 risk management methods used in industry primarily because organizations typically seek to adopt a method that is in alignment with their specific information security management program. Labuschagne and Eloff (1998) argued that most available risk management methods derive from a scientific core, thus focusing on technology that proposes technical solutions, which negates addressing human, organizational strategic or environmental factors. Most quantitative risk methods are based on using loss exposure as a function of the vulnerability of an asset to a threat multiplied by the probability of a threat becoming a reality (Rainer et al., 1991). These methods are called expected valuate analyses, which include annualized loss expectancy (ALE) (Post & Diltz, 1986), the Livermore Risk Analysis Methodology (LRAM), (Guarro, 1987) and Stochastic Dominance (Post & Diltz, 1986). Qualitative methodologies attempt to express risk in descriptive variables rather than precise dollar amounts (Ranier et al., 1991). Ranier et al. (1991) stated that qualitative risk methods are based on the assumptions that certain threats or loss of data cannot be appropriately expressed in dollars or discrete events, and that precise information may be unobtainable. Some of the qualitative methods are Scenario Analysis (Hammond, 1988; Newton & Snyder, 1987), Operational Critical Threat Asset and Vulnerability Evaluation OCTAVE (Woody, 2006), and CCTA risk analysis and management method CRAMM (Sun, Srivastava, & Mock, 2006).

Risk analysis and risk management do not lack critics highlighting their shortcoming such as lacking a scientific approach (Baskerville, 1991), lack of clarity (Alter & Sherer, 2004), and, according to Spears (2006), being based largely on guesswork. The criticisms of “lacking of a scientific approach,” to “lack of clarity,” and “guesswork” in the risk management process stems from how an organization determines the value of intangible assets such as information (Gerber & von Solms, 2005) along with determining the vulnerability of an asset along with other factors. Gerber and von Solms (2005) argued that it is difficult if not impossible to estimate the value of information, and Suh and Han (2003) stated that organizations typically consider replacement cost, but the financial loss caused by the disruption of operation is highly subjective. Lastly, the impact of a breach and the loss of customer confidence are extremely difficult to estimate (Bennett & Kailay, 1992).

According to Voster and Labuschagne (2005), the common goal of risk management methods are to prioritize and estimate the risk value and to suggest the most suitable mitigation plan to eliminate or minimize risk to an acceptable level, but other scholars (Huang, Ding, & Hu, 2008; Niekerk & Labuschagne, 2006; Zuccatto, 2004) have called for a more holistic approach to risk management that minimizes the shortcoming of risk management methods. A holistic approach to risk management focuses equally on minimizing risk in the areas of technology, information, people, and processes (Spears, 2006). One of the benefits of using a holistic approach to information security management is that it involves business users to the extent necessary to identify a comprehensive set of risk while also promoting security awareness throughout the organization (Lategan & Solms, 2006). Several researchers have created information security risk management frameworks (Huang et al., 2008; Saleh & Alfaantookh, 2011; Zuccato, 2007) to holistically address information security risk in organizations with a focus on the technology, the people, the business processes, and the environment.

2.2.4 *User Security*

User security delves into the human experience a computer user has with computer resources such as an information system within an organization. Human-related information security research covers the social aspects of security an organization is faced with as it relates to organizational members, such as usability, security culture, security awareness, training, along with the behavior of the user and other human-related issues. Current human-related information security research has been categorized into four main directions by Stanton, Stam, Mastrangelo, and Jolton (2005): (a) user interfaces of security-related systems; (b) information security management concerns for risk, business processes and finance; (c) organizational issues related to information security behavior; and (d) counterproductive computer usage. This research study touches on all four categories in that a usability failure from an interaction with an interface creates information risk based on the behavior the user will have after the usability failure. The behavior of the user can result in counterproductive computer usage. To address “human-related” information security issues is to understand the users’ point of view as it relates to information systems security. Wier, Douglas, Richardson, and Jack (2010) have observed that security is not the main goal of a user’s interaction with a computer system. Post and Kagan (2006) stated that employees in an organization are more likely to bypass security measures in order to complete a task. To further expand on the chasm between users of an information system and information security, Albrechtsen and Hovden (2009) argued that there is a digital divide between information security managers and users that has created a misalignment of the security practices levied by the organization in relation to the dynamics of the user’s workday.

A useful tool in aligning computer users in an organization with the security guidelines and rules an organization implements in relation to the use of computer resources is through the use of security policies (Ifinedo, 2012; Knapp & Marshall, 2006s). Understanding the impact a computer user’s behavior can have on information security has allowed researchers to develop concepts, theories, and research relevant to human behavior in organizations and how the behavior affects information security (Stanton et al., 2005). Two streams of information security research that address user behavior is counterproductive computer usage (Stanton, 2002; Weatherbee, 2010) and insider threat (Post & Kagan, 2006; Warkentin & Wilson, 2009). Counterproductive computer usage consists of a computer user in an organization that exposes the information assets to risk or liability or a loss of productivity time by engaging in activities that are counter to established computer resource usage policies (Mastrangelo, Everton, & Jolton, 2006). Insider threat refers to intentionally disruptive, unethical, or illegal behavior enacted by individuals who possess substantial internal access to the organization's information assets (Stanton et al., 2005).

Counterproductive computer usage and insider threats research both focus on users of information systems that primarily subvert organization security policies for their own benefit. The security controls implemented for counterproductive computer usage and insider threats do not account for the misalignment of a user task and the technology implemented in an organization. The misalignment of a user task and the technology creates a breakdown in security controls that skews the behavior of the user, particularly in a healthcare organization where the task has an impact on the outcome of human life. Evaluating misaligned task, technology, and the behavior of the user of an IS will provide valuable insight into addressing user security.

2.3 Usability

Usability falls under the research domain of HCI. HCI in IS are "concerned with the ways humans interact with information, technologies, and tasks, especially in business, managerial, organizational, and cultural contexts'' (Zhang, Benbasat, Carey, Davis, Galletta, & Strong, 2002, p. 334). Usability is derived from HCI principles, wherein designers of software application interfaces understand that systems for users should be easy to learn, useful, contain functions people really need in their work, and be easy and pleasant to use

(Bevan, 2005). The manner in which this is done is through adding the appropriate usability design techniques and usability evaluation methods that evaluate the task, the context, and behavior of the user as the user interacts with a computer application or system.

User interface literature primarily focuses on developing better interfaces (Shneiderman, Jacobs, Cohen, & Plaisant, 2009), securing the interface (Bourimi et al., 2012; Brostoff, 2004), analyzing and critiquing software tools used for interface development (Cranor & Garfinkel, 2005), and assessing usability evaluation methods (Cockton, 2008; Hartson, Andre, & Williges, 2001). User interfaces are the portal to a user’s experience with a computer system. The extant literature discusses user interfaces in the context of interactive products that are used primarily to help the user perform a task via the product’s user interface. According to Juristo, Moreno, and Sanchez-Segura (2007), the user interface can be characterized narrowly as an interface comprising the input and output devices and the software that services them, while also using broader terms characterizing a user interface that includes everything that shapes users’ experiences with computers, including documentation, training, and human support.

Usability improves the design of user interface by evaluating the organization, presentation, and interactivity of the interface (Shneiderman et al., 2009). Shneiderman (1987) provided seminal research in the area of interactive user interface design, discussing strategies for designing high-quality interactive systems by applying the syntactic and semantic model of user knowledge. The syntactic/semantic model suggests that users have both syntactic knowledge about device details and semantic knowledge about concepts, which are separated into task concepts and computer concepts. Syntactic knowledge is gained through repetitive actions and familiarity with a specific task or computer systems while semantic knowledge is gained through meaningful learning. Despite the blue print user-interface design strategies provided by Shneiderman, researchers continue to look for methods to design interfaces to reduce errors a user can encounter.

A user's interaction with an application or system when a usability failure occurs is central to determining whether security controls are aligned with an organization's business process. Blandford, Thimblebly, and Bryan-Kinns (2003) suggest users encounter interaction traps as a consequence of misunderstanding their ability to complete a task due to a system failure. The interaction trap occurs when the user encounters detours, barriers, or objectives that are unable to be achieved. According to Marcus (2002), the results created interacting with a computer include the input and output techniques, status displays, and feedback at the local and global levels. At the local level, feedback users receive are related to the behavior of the physical aspects of a computer system, such as a visual display of a computer screen or peripheral devices like the response of a printer when initiated by the user. At the global level, context issues and task activities at a larger scale are presented to users.

Context is gathered in an automated fashion using a combination of sensing and complex rules to allow applications to react to relevant changes in an organizational environment (Dey & Newberg, 2009). Context of use and the interaction of a user serve as a barometer to measure the impact a failed task from a usability failure has on the impact of performance. Crowley et al. (2002) described "context of use" for an interactive system as consisting of three key attributes: (a) users of the system who are intended to use (and/or who effectively use) the system; (b) hardware and software platform(s), that is, the computational and interaction device(s) that can be used for interacting with the system; and (c) the physical environment where the interaction can take place. The context of use attributes can be applied to hospital and clinical settings in the mere business practices used. A user in the healthcare environment can vary based on the nature of the task, from the patient to the physician, which can determine the system used and the environment in which the task will be accomplished. Hospital and clinical settings are among the many organizations that are often used for context-aware applications in their environment to take action without explicit user input (Dey & Newberg, 2009). Research in the area of context-aware applications suggest that users become frustrated when they do not understand why a system performs an action, not allowing the user the ability to fix the problem (Barkhuus & Dey, 2003).

2.3.1 *Usability Failure*

Software usability deficiencies are determined by the problems users have in carrying out a standard set of actions using software (Rubin, Chisnell, & Spool, 2008). In this research study, user problems from software usability deficiencies are synonymous with usability failures. According to Winograd and Flores (1986), usability failures often result in interaction breakdowns. Winograd and Flores and Blandford et al. (2003) have stated that breakdowns occur when a user faces enough difficulty accomplishing a task so that the user is able to identify that the user interface is the source of the problem. Jacobson et al. (1999) defined usability failure as being indicated by any of nine criteria: (a) the user articulates a goal and cannot succeed in attaining it, (b) the user explicitly gives up, (c) the user articulates a goal and has to try a different method to find a solution, (d) the user produces a result different from the task given, (e) the user expresses surprise, (f) the user expresses some negative affect or says something is a problem, (g) the user makes a design suggestion, (h) the system crashes, (i) the evaluator generalizes a group of previously detected problems into a new problem.

Jacobson et al. (1999) provided a usability failure definition as a foundation of where to begin in applying methods to address and reduce usability failures. Based on this definition, it can be concluded that a usability failure, particularly when a system fails, is essentially the same as an information systems security failure. Therefore, usability failures, and usability-related information security failures should be addressed using the same strategies organizations use to improve their overall security program.

2.3.2 *Usability Development and Design*

Usability development and design is the primary area of focus in the HCI and usability domain. In the domain of usability development, usability design principles are the basis for designing usable software applications. According to Juristo et al. (2007), with some notable exceptions, software development is primarily concerned with the inner workings of the system, while usability development focuses on the user. In the software development process, the user’s role is a manner in which the development team can elicit requirements, while in the context of usability development, also termed user-centered development, the users are the reason for designing the system (Gould & Lewis, 1985; Peslak, 2005).

The difference in usability development design perspectives highlights the challenge in the software development process; however, the development process presents a means to understand how the varying development perspectives create an opportunity to address the issues that stem from the development staff's disconnect with the users. For example, a usability error such as the failure for a user to access a system due to an authentication breakdown between two systems may not be viewed as a failure in the application that was developed. The failure may be viewed as a "memorability" or "learnability" problem by the user; however, the inability to access an application is also an IS security failure, and should be addressed accordingly. The ability to have usability-related security failures come to the fore reported by users that suffer such failures and address the security failures through adequate security controls adds security value to both the usability and information system security communities.

Usability evaluation methods (UEM) are used to measure and identify potential issues affecting usability attributes of a system or devices with respect to particular users performing a particular task in a particular context (Hilbert & Redmiles, 2000). The usability attributes are learnability, efficiency, memorability, errors, and satisfaction (Nielsen, 1993). Applying usability attributes can vary depending on the background knowledge and experience of users, the task for which the system is used, and the context in which it is used (Hilbert & Redmiles, 2000). Usability researchers have proposed several classifications of UEMs. Fernandez, Insfran, and Abrahao (2011) observed that UEMs are principally are classified into two different types: empirical methods and inspections methods. According to Fernandez et al., empirical methods are based on capturing and analyzing usage data from end users, and inspection methods are performed by expert evaluators or designers.

The most common types of UEMs are Heuristic Evaluations (Nielsen & Molich, 1990), cognitive walkthroughs (Wharton et al., 1992), goals operator methods and selection (Card et al. 1983), and cogtools (John et al., 2004). According to Reisterer and Oppermann (1993), a complete evaluation of usability must consider the user, the task, the computer, and the organization. UEMs are evaluated during the testing or implementation stages of the development process (Akers, Jeffries, Simpson, & Winograd, 2012), which leaves unanswered questions in the usability domain in relation to managing usability-related information security failures once software is released into the organization.

2.4 Healthcare Information System

There has been a great deal of literature chronicling the evolution of healthcare organizations and their ability to adopt IT. The adoption of IT within the healthcare organization has brought about a cornucopia of terms and definitions to describe the software and hardware technology used within the organization. Healthcare literature is bombarded with such terms as hospital information systems, healthcare information systems, health information systems, medical information systems, clinical information systems, patient care information systems, and nursing information systems to describe both the applications and systems that process data and produce information for the user to provide point of care to patients. Users who provide point-of-care to patients within the healthcare context are physicians, clinicians, and healthcare workers. Physicians and clinicians provide direct observation and care to patients, while healthcare workers assist in the process by carrying out orders issued by physicians and clinicians.

In addition to identifying the types of systems that process data and produce information along with the types of users in the healthcare environment, there are also applications (subsystems) that require identification. Computerized Order Entry Records

(CPOE), Electronic Health Records (EHR), Electronic Medical Record (EMR) and Computer-Based Patient Records (CBPR) are essentially subsystems or byproducts of the information system. Decisions regarding Healthcare IT (HIT) implementations are often made at the department level, with each department developing subsystems based on its needs, beliefs, practices, and expertise (Harkee, Alessi, & Collan, 2003; Kim & Unmanath, 1999). The fact that these subsystems contain multi-platform, multi-vendor application wrappers built around multivariate data sources contributes to the complexity of HIS (Orgun & Vu, 2006). The results of decisions to acquire and implement HIT are autonomous and heterogeneous systems (Devaraj & Kohli, 2000; Toussaint, Bakker, & Groeneweegen, 1992) that access and retrieve data from disparate sources, which is the healthcare environment. There is a rich stream of literature in the healthcare environment reporting problems caused by autonomous and heterogeneous systems such as user resistance, HIT implementation and project failures primarily due to interoperability and usability failures (Bhattacherjee & Hikmet; 2007; Johnson & Willey, 2011; Vega, Schieferdecker, & Din, 2010).

With the numerous terms used to describe systems in the healthcare environment along with the many subsystems used, the healthcare environment terms used in this research study will be operationalized. The subsystems described previously are the interfaces where information handling activities (interactions) take place, and the definition of an HIS is aligned with Backhouse and Liebenau (1990) as an aggregate of information-handling activities at the technical, formal and informal levels of an organization. These information-handling activities comprise subsystems composed of autonomous, heterogeneous and disparate software applications and hardware systems that interoperate to provide information to the users of the system.

2.5. Summary

Healthcare organizations are composed of heterogeneous and disparate information systems intertwined with complex business processes that create a great deal of challenges for the users of the system. The manner in which IT systems and products are implemented along with the overlapping and intricate tasks the users have pose problems in the area of usability. Usability research primarily focuses on the user interface; therefore, designing a better interface often leaves security in question. When usability failures arise from the misalignment between healthcare task and the technology used in healthcare organizations, the security of information is jeopardized. Information is jeopardized when the CIA of computer resources are rendered vulnerable from usability failures. Usability failures are a technical security issue; therefore, technical security controls must be evaluated and applied accordingly. Applying the appropriate IS security controls will reduce usability security failures while also improving the practices used to design, develop and implement user interfaces.

Chapter 3

Research Methodology

3.1 Introduction

In this chapter, the theoretical framework, research model, and research method will be discussed. This chapter begins by discussing the theoretical framework of Goodhue (1988; 1995) and Goodhue and Thompson (1995) to study the research problem. The development of the research model is then discussed. Finally, the research method is discussed.

3.2 Theoretical Framework

The theoretical framework in this research study is an extension of the work of Goodhue (1988; 1995) and Goodhue and Thompson (1995) regarding TTF theory and the Technology-to-Performance Chain (TPC) fit focus model. The TTF theory holds that, for IT to have a positive impact on individual performance, the technology must be utilized and it must be a good fit with the task it supports. The TPC model "draws on insights from two complimentary streams of research (user attitudes as predictors of utilization and task-technology fit as a predictor of performance)" (Goodhue & Thompson, p. 213). The TPC model tests user evaluation and performance impacts, which are consistent with the research model proposed by DeLone and McLean (1992) in that utilization and user attitudes lead to individual performance impacts. However, the TPC model goes beyond the IS Success model of Delone and McLean where the TPC model explains how technology leads to performance impacts, along with explicitly detailing the manner in which the TTF constructs provides the theoretical basis for evaluating the issues related to the impact of IT on performance.

Goodhue and Thompson’s (1995) TTF model is measured using eight factors that are distributed among the TTF constructs of task, technology, and individual characteristics respectively. The dimensions of TTF along with the eight factors are listed in Appendix A. The factors will be discussed at length later in this section. Goodhue and Thompson suggest decomposing the TTF theoretical model into more detailed components to facilitate the usage of TTF as a diagnostic tool to measure how well the technology of an organization fits a task, and how that task ultimately impacts performance. TTF with a “fit focus” provides that opportunity as it proposes that IS has a positive impact on performance only when there is a corresponding “fit” between their functionality and the task requirements of users. Figure 1 contains the TTF “fit focus” model preceded by an explanation of the constructs.

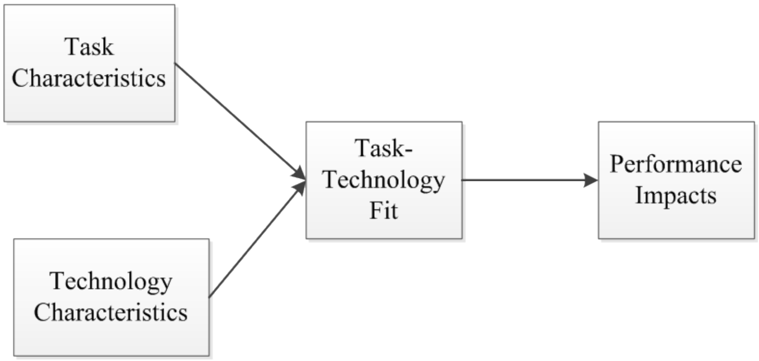


Figure 1. TTF “Fit Focus” model (Goodhue & Thompson, 1995)

Technology characteristics are tools used by individuals in carrying out their tasks. In an IS research context, the tools consist of hardware, software, data, and user support services (training and help lines, etc.) provided to assist users in their task. Task characteristics are actions carried out by individuals turning inputs into outputs. Task characteristics of interest include those that might move a user to rely heavily on certain aspects of the information technology. The example Goodhue and Thompson (1995) use is relying on the organization’s IS to process queries against a database. TTF, the degree to which a technology assists individuals in performing their portfolio of tasks, is the correspondence between task requirements, individual abilities, and the functionality of the technology.

Antecedents of TTF are the interactions between task, technology, and individual. For example, certain tasks require specific kinds of technological functionality from various organizational units, which encompasses integrated databases being accessible to all users in the organization. As the gap between task requirements and the functionality of the technology widens, TTF is reduced. Performance impact in this context is related to an accomplishment of a portfolio of tasks by an individual. Higher performance is characterized by improved efficiency, improved effectiveness, and/or higher quality. High TTF increases the likelihood of utilization, but also increases the performance impact of the system.

The task-technology fit theory allows organizational members to assess the capability of their IT systems, along with how those systems impact individual performance, while also assessing the behavior and attitudes of the individual user while interacting with an IS. The TTF model aligns very well with the healthcare environment, particularly with the constant implementation of IT products that are often driven at the department level to improve point of care for patients.

3.3. Task-technology Fit in IS Context

TTF theory has evolved from Goodhue (1988; 1995) to Goodhue and Thompson (1995). The evolution of TTF has benefited the IS community with key research studies extending the TTF theory as suggested by Goodhue (1988; 1995) and by Goodhue and Thompson (1995). For example, Zigurs and Buckland (1998) examined the TTF construct focusing on Group Support Systems (GSS) environment. Zigurs and Buckland evaluated the fit between complex tasks and how those tasks impacted group performance. The GSS literature indicates a direct correlation between the importance of the task between fit and effective GSS use. However, GSS literature has not been able to use a single method to evaluate the various GSS task characteristics i.e., simple task, single solution task, or idea-generation task. Zigurs and Buckland were able to address the issues of evaluating various task characteristics using TTF by analyzing the task using complexity dimensions instead of focusing on the components of a task. Complexity dimensions consist of four constructs that take into account the task attributes used in the GSS environment.

A second extension of TTF used in the IS domain is the TPC model, which follows the research stream of utilization and fit (Goodhue & Thompson, 1995). Goodhue (1995) and Goodhue and Thompson (1995) have stated that, when utilization can be assumed, the utilization construct of TTF is not required. This research study assumes the utilization of an HIS is mandatory; therefore, this research aligns with the fit focus model of TTF theory. Further, there has been a small number of researchers who have conducted IS research utilizing TTF theory primarily focusing on the fit conceptual model. The researchers have argued that performance impacts will result from TTF when a technology provides features that fit the requirement of a task. Benbasat et al. (1986) and Dickson et al. (1986) used the “fit focus” model to examine the impact of graphs versus tables on individual decision-making performance. The researchers used a series of laboratory experiments that reported how two types of technology characteristics directly influenced user performance based on the fit with the task.

3.4. Research Model

In order to further develop both the research model and the hypotheses to be tested, we must first operationalize the TTF constructs. The operationalized research model is presented in Figure 2 extending the TTF theory in a healthcare setting. The original task characteristics construct of TTF will be termed *healthcare task characteristics*, while the technology characteristic construct will be termed *security technology characteristics*. The TTF construct will remain unchanged, while the performance impact construct is concerned with HIS security performance impacts. These constructs are further discussed in the following paragraphs.

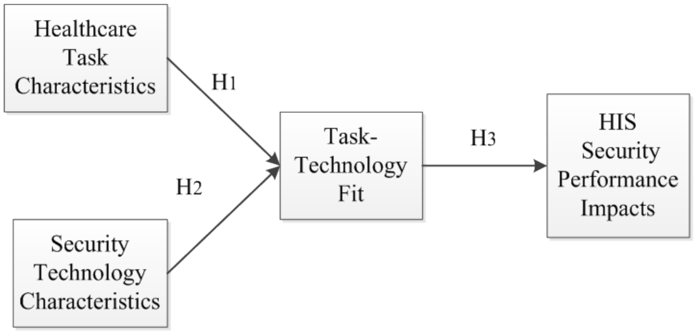

Healthcare Task Characteristics
Security Technology Characteristics
H1
H2
Task-Technology Fit
H3
HIS Security Performance Impacts

Figure 2. Research model with hypotheses testing

Healthcare task characteristics. The goal is to assess whether or not the healthcare worker is supported by the HIS to complete the task. The healthcare task will be measured by the identification of the type of task the user is engaged in, and the job role of the user with which the task is associated. The task will be categorized as routine or non-routine, along with the number and types of applications and systems that are required for task accomplishment.

Goodhue (1995) used the attributes of non-routineness and interdependence to measure task characteristics. Non-routineness is the difficulty level required to complete a task. Goodhue suggested that, since users who engage in routine and repetitive tasks are familiar with the task, users have the ability to work around the IS to complete their task with the minimum amount of interruption or frustration where non-routine task are characterized by the dependence of multiple applications, systems, and business processes used to complete the task. The second attribute interdependence is identified and measured by a user being engaged in a task that must integrate with multiple systems to access and retrieve data to allow the task to be completed. Problems often occur in this area when data are incompatible or unable to be accessed or delivered in the form expected.

Security technology characteristics. The goal is to assess the level of technical security controls that are in place when healthcare workers attempt to complete their assigned task. The security technology will be measured by identifying the type of resources, which includes hardware, software, and data that was used and rendered vulnerable when a usability failure occurred. Usability failures associated with hardware, software, and data threaten the confidentiality, integrity, and availability of these resources are is a fundamental security requirement that must be protected. Capturing and identifying the resources that were rendered vulnerable that are associated with the task the healthcare worker is engaged in, allowing this research study to further understand the nature of usability failures from the technical security perspective. This allows a linkage to form between the task and technology at the point of the technology failure, but it also provide a means to better understand what the healthcare worker was exposed to during the interaction with the technology. This will provide and shape the context of how a healthcare worker's security performance is impacted when a usability failure occurs.

Task Technology Fit. The TTF factors are linked to the task and technology characteristics respectively. TTF is measured by eight factors: (a) data quality (DQ), (b) locatability of data, (c) authorization to access data, (d) data compatibility (between systems), (e) training and ease of use, (f) production timeliness (IS meeting scheduled operations), (g) systems reliability, and (h) IS relationships with users. The first five factors of TTF have links from the healthcare task construct to TTF, while the last three have links with security technology characteristic regarding TTF. The combined eight TTF factors form the three hypotheses that will be tested by dissecting the research model into two components. Component A will focus on testing hypotheses one and two that link both the task characteristic and security technology characteristics construct to TTF, while component B will test how TTF links to HIS security performance impacts. The following is a breakdown of the hypotheses:

3.4.1 *Hypotheses Component A*

Hypothesis 1: Healthcare Task Characteristics Linkage to TTF. The factors that will be measured are directly linked with TTF are DQ, locatability of the data, authorization to access the data, data compatibility between the systems, and training and ease of use. DQ seeks to identify the currency of the data, so that the right data are maintained with the right level of detail. Locatability of the data is centered on locating the data along with the ability to easily find out the meaning of the data. Authorization is users having access to the data to complete a task. Compatibility is having access to data that are accessed and used from heterogeneous and disparate IS. Ease of use/training is providing hardware or software that is easy to use, while providing the appropriate level of training and IT support where necessary. A solid relationship among healthcare task characteristic factors signals the link between the two constructs, creating an efficient healthcare task; therefore, the following hypothesis will be tested:

H_1: Healthcare task characteristics will be associated with Task-Technology Fit.

Hypothesis 2: Security Technology Characteristic Linkage to TTF. The factors that will be measured are directly linked to TTF, which are production timeliness, system reliability, and IS relationships. Production timeliness provides the ability of a user to schedule reports or run automated tasked jobs with the expectation that the system will provide an output within the time frame required. System reliability consist of having the HIS to be available when needed without unexpected or lengthy downtimes, and the third variable of IS relationships with users consists of ensuring the IS has the flexibility to meet the changed business needs of the user of the system. The measured factors of security technology characteristics are effectively the computer resources of hardware, software and data that must be protected. A stable relationship between security technology characteristic factors in relation to computers, software, and data signals a link of TTF; therefore, the following hypotheses will be tested.

H_2: Security technology characteristics will be associated with Task-Technology Fit.

3.4.2 *Hypotheses Component B*

Hypothesis 3: HIS Security Performance Impacts. Performance impacts are affected by healthcare task and by HIS security technologies that are evaluated by the user based on the results of the TTF fit. The performance impacts should be positive, if the task fits the technology. Combining the constructs of the research model provides a means to measure the factors to determine the level of effectiveness, efficiency, and satisfaction to complete a task, with the given heterogeneous and disparate systems. If the healthcare task characteristic and HIS security technology characteristics fit, the healthcare workers will complete their task, and there will be an impact on the system, and IS security controls can be confirmed. Additionally, if the healthcare task characteristics and HIS security technology characteristics fit, TTF correlates with HIS Security Performance; therefore, the following hypothesis will be tested.

H_3: Task-Technology Fit is associated with HIS Security Performance Impact.

3.5. Research Method

This research study is exploratory in nature and used a single case design approach with embedded units as specified by Yin (2009). As Yin stated, “a case study is an empirical inquiry that investigates a contemporary phenomenon in depth within its real-life context, especially if the boundaries between phenomenon and context are not clearly evident” (p. 18). According to Yin, experiment and survey methods are limited in their approach when investigating contemporary phenomenon. Experiments typically remove a phenomenon from its context by focusing on a few variables, while survey method designers focus on having an acceptable amount of variables analyzed to ensure they have the proper amount of respondents for the study, which essentially can limit the investigation. Based on Yin’s assertions, the case study approach is a method that can be used to address a phenomenon and context in real-life situations thoroughly addressing data collection and data analysis strategies respectively.

This study was conducted using the positivist case study perspective and paradigm. According to Guba and Lincoln (1994), the positivist paradigm has three dimensions: the first is the ontological position which states that an objective reality is assumed which can be systematically and rationally investigated through empirical investigating and is driven by causal laws that apply to social behavior. The second dimension is the epistemology position wherein the researcher and the phenomenon being investigated are assumed to be independent and the research remains detached, neutral and objective. Guba and Lincoln believe that any reduction in independence is a threat to the validity of the study and should be reduced by following prescribed procedures. The third dimension noted by Guba and Lincoln is the methodological position which calls for general theories to be used to generate propositions that are operationalized as hypotheses and subjected to replicable empirical testing.

Executing a positivist case study essentially requires the researcher to understand that there is a single reality that the subjects of the study will express; therefore, the researcher must observe and measure the phenomenon adhering to the traditional validity and reliability tests used in the natural sciences (Yin, 2009). This study followed the guidelines of Yin (2009), Dube and Pare (2004) and Lee (1991) in executing this approach. In essence, this study follows a natural science approach, while applying the three-level framework of subjective understanding, interpretive understanding, and positivist understanding prescribed by Lee. The framework allows the researcher to understand how human subjects see themselves, the researcher interpreting and understanding the human subjects under study, and lastly creating the test to explain the empirical reality that is being investigated.

This case study analyzed usability failures in one healthcare organization that has 128 medical centers that utilize multiple types of clinical and HIS to share information across the United States. A usability failure develops from the user's inability to access an application or system with the sole purpose of obtaining information to complete a task. The continuous development and expansion of HIS to meet legislative mandates has, in some instances, impacted performance of the healthcare worker. The performance impact was measured in the form of usability failures, which often become an organizational security issue in an effort to provide HIS users a means to access information in a timely and secure manner (Braz & Robert, 2006).

This research study captured and identified the nature and types of reported usability failures from the 128 medical centers to determine how alignment problems between the HIS security technology and the healthcare task can have an impact on HIS security performance. The nature and types of usability failures was analyzed based on the type of task-related and technology-related usability failures respectively. Ten usability failure cases were randomly selected: five representing task-related usability failures, and five representing technology-related usability failures. The ten selected usability failures cases essentially encapsulate the single case study design with embedded unit of analysis.

3.5.1 *Unit of Analysis*

Yin (2009) stated that the selection of the unit of analysis occurs when the primary research questions are accurately specified. Selecting well-focused research questions allows for the unit of analysis to be formed, which, according to Yin, is the “case” being studied and allows for time boundaries to establish a beginning and ending point for the study. Based on these parameters, the unit of analysis for this research study is the usability failure identified and captured in a large healthcare organization by users of an HIS. The unit of analysis aligns with the research problem, the research questions, and hypotheses used to build the foundation of this research study. Furthermore, the identified and captured usability failures were decomposed into two subunits consisting of task-related and technology-related usability failures respectively. The two subunits create the embedded case study and were the focus of analysis.

3.5.2 *Participant*s

The participants in this research study are healthcare workers who reported usability failures while working to complete a task and the support staff personnel assigned to resolve the problem. The healthcare workers who reported usability failures were selected by the systematic sampling method using the "kth" record on the list. The term "kth" is defined as the number between 0 and the size of sample to be selected (Salkind, 2006). The research study participants consisted of members from 14 states and 12 medical centers. The names of the participants and the name of the medical centers will remain anonymous. Of the list of candidates interviewed, nine were IT specialists, five were nurses, three were product application specialists, two were program analysts, and one each of a human resource specialist, pharmacist, and a medical administrative specialist respectively. Based on the size of the population and the sample size of usability failures, ten cases were selected for this study. This researcher is a member of the organization that has direct access to the data under study. The process of gaining access to the organization and receiving approval to conduct the study was provided at the conclusion of the Institution Review Board process.

3.5.3 *Data Collection*

According to Bonoma (1985), collecting different types of data by different methods from different sources produces a wider scope of coverage and may result in a fuller picture of the phenomenon under study. Yin (2009) noted that the most important advantage presented by using multiple sources of evidence from data collection is the development of “converging lines of inquiry” (p.42) which is a process of triangulation and corroboration for the study. Triangulation occurred in the data collection process in two phases. The table below lists the data collection steps for this research study. The first phase consists of gathering information from the organization’s help desk database where usability failures are reported, along with collecting documentation of organizational records that reflect the practices and policies used to support the technology that is used and developed in the organization.

Structured Query Language (SQL) was used to retrieve help desk records of reported usability failures dating back five years. The query retrieved all records within the time frame of September 1, 2008, to September 31, 2013, of help desk tickets that required an intervention by the development staff. The captured help desk records followed a four-phased process that created codes and categories to identify the nature and types of usability failures. Phase two of the data collection process and another form of triangulation consisted of conducting semi-structured interviews with the case study participants. Phase two data collection process, the researcher conducted 22 semi-structured interviews guided by the theoretical framework of the study. There were 15 usability failures cases selected 9 usability failures were task-related failures, while 6 were technology-related failures. The interview data were transcribed, coded, and analyzed using the Atlas.TI qualitative analysis tool.

The data collected and analyzed from the organization along with the confidentiality of the participants was preserved throughout this research endeavor by substituting the participant names with codes. The following information further describes the two phases of the data collection process.

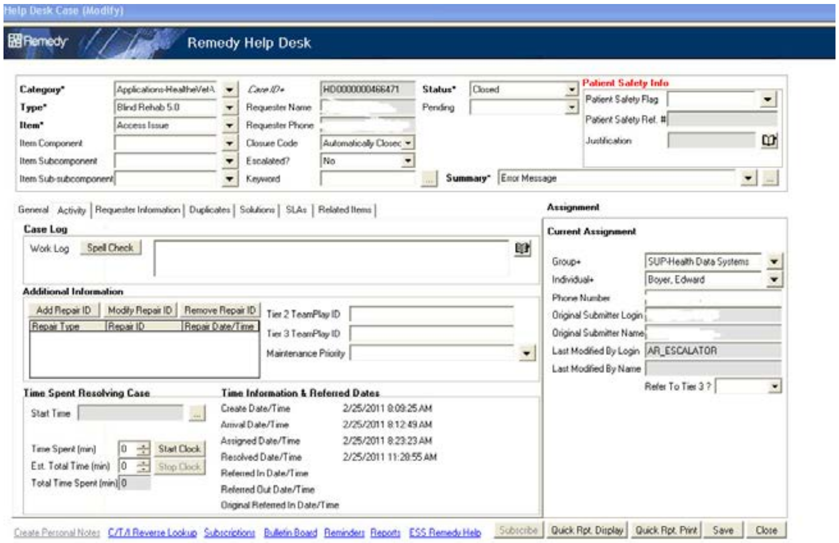
Table 1
Data Collection Technique

Data Collection Steps for this Research Study:	Yin (2009)	Pare (2004)	Sarker & Lee (2003)
Database Repository	X	X	X
Company Documents	X	X	X
Emails	X	X	X
Interviews (Formal & Informal)	X	X	X

Note. The "X" in the data collection technique table represents triangulation for this research study through construct validity, external validity, and reliability as prescribed by Yin (2009).

3.5.4 *Data Collection Phase One*

The purpose of phase one of the data collection process is to identify and capture the nature and types of reported usability failures in the healthcare organization. The healthcare organization in this study stores the data to be collected in an Enterprise Solutions Support (ESS) database in Figure 3. The ESS database is a repository of the cradle-to-grave information of all problems reported by the users in the organization along with the information of the solutions provided by the organization. The information is captured and stored in a relational database that links data elements into categories that list the task, technology, user information, and a description and summary of the usability failure. The categories in which the data are stored are the bridge that was used to create the coding structure for phase two of the data collection process. The SQL query created returned reported usability failures that required an intervention by the development staff. This researcher postulates a usability failure that required an intervention by development staff is of a serious nature and can be linked to the misalignment between a task and technology.



Category* Applications-HealtheVetA
Type* Blind Rehab 5.0
Item* Access Issue
Item Component
Item Subcomponent
Item Sub-subcomponent
Case ID+ HD0000000466471
Requester Name [redacted]
Requester Phone [redacted]
Closure Code Automatically Closec
Escalated? No
Keyword
Status* Closed
Pending
Summary* Error Message

Patient Safety Info
Patient Safety Flag
Patient Safety Ref. #
Justification

Case Log
Work Log

Additional Information

Repair Type	Repair ID	Repair Date/Time

Tier 2 TeamPlay ID
Tier 3 TeamPlay ID
Maintenance Priority

Time Spent Resolving Case
Start Time
Time Spent (min) 0
Est. Total Time (min) 0
Total Time Spent (min) 0

Time Information & Referred Dates

Create Date/Time	2/25/2011 8:09:25 AM
Arrival Date/Time	2/25/2011 8:12:49 AM
Assigned Date/Time	2/25/2011 8:23:23 AM
Resolved Date/Time	2/25/2011 11:28:55 AM
Referred In Date/Time	
Referred Out Date/Time	
Original Referred In Date/Time	

Assignment
Current Assignment
Group+ SUP-Health Data Systems
Individual+ Boyer, Edward
Phone Number
Original Submitter Login [redacted]
Original Submitter Name [redacted]
Last Modified By Login AR_ESCALATOR
Last Modified By Name
Refer To Tier 3 ?

Figure 3. Enterprise support solutions screen capture

Collecting and analyzing such data gets to the core of the studied phenomenon. The returned data lists the support case identification number, the date the problem was reported, type of usability failure, the application interface or system used, a summary and description of the problem, the name of the user that encountered the usability failure, the failed task, and the name and location of the organization.

Once the data are collected from the database, a key word search was executed in four stages focusing on the summary and description fields of the extracted data. Figure 4 list the four data collection stages that were used in phase one of the data collection process. Further, a list of key word search terms is listed in Appendix B. The first key word search stage used anecdotal terms used to describe usability and technology failures in this healthcare organization. The anecdotal terms are derived from applications, systems, and communication failures reported by members of the healthcare organization under study.

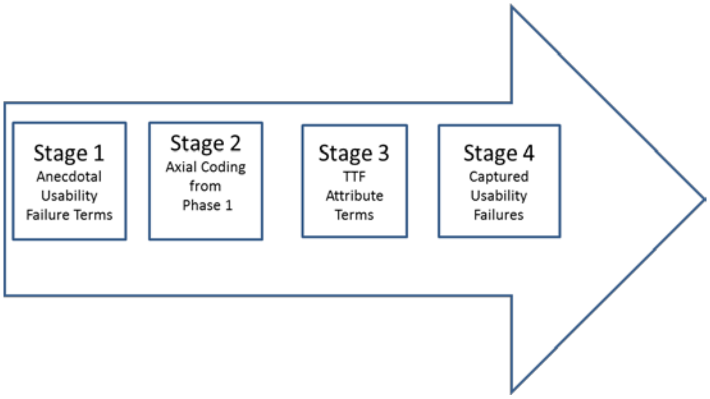

Stage 1
Anecdotal Usability Failure Terms
Stage 2
Axial Coding from Phase 1
Stage 3
TTF Attribute Terms
Stage 4
Captured Usability Failures

Figure 4. Phase one data collection stages

The second key word search stage used a form of axial coding prescribed by Strauss and Corbin (1998) to further identify additional categories of usability failures that were discovered from the first stage of the key word search. Axial coding is a process used to reassemble and capture data that were fallout from the previous stage of captured, categorized and coded data. The third key word search stage incorporated the terms used by Goodhue and Thompson (1995) to identify the attributes of the eight TTF factors. The eight TTF factor attributes can directly link usability failures to a task characteristic or a technology characteristic usability failure. The fourth and final stage is the capturing of usability failures from the key word search. The collected usability failures were analyzed to determine the nature and types of usability failures. Additionally, collected usability failures were parsed into task characteristic and technology characteristic usability failures, which essentially is the focus of the embedded case study. The task characteristic and technology characteristics usability failures went through a final review to ensure the usability failures have not been resolved by the support staff before data analysis begins. Final review required an evaluation of additional information that was added to the initial reported usability failure. The additional information provided by support staff added more detail to the reported usability failure, and in some cases, required a reclassification, and re-routing of the usability failure. Nonetheless, the additional information ensured an accurate classification of the reported usability failure.

3.5.5 *Data Collection Phase Two*

The purpose of phase two of the data collection process was to conduct semi-structured interviews to understand how usability-related information system security failures impacted task accomplishment in a healthcare setting. Yin (2009) suggested conducting a pilot study to help researchers to determine the appropriate unit of analysis, to refine the data collection instruments, and/or to familiarize the researcher with the phenomenon itself. Having a clear unit of analysis, and data collection process, along with a good understanding of the phenomenon, a pilot study was not required. Therefore, semi-structured interviews are used when the researcher knows most of the questions to ask but cannot predict the answer (Pare, 2004). Twenty two semi-structured interviews were conducted via the telephone with healthcare workers and support staff personnel who reported or supported the usability failures from the data collection process. A summary of the interview process is discussed in the phase two data collection process in Chapter 5.

The present study follows the IS research of Levina (2005) and Beaudry and Pinsonneault (2005) who conducted qualitative case study design consisting of semi-structured interviews from the range of 17 to 20 participants in less than a year’s time frame. Levina (2005) conducted a longitudinal qualitative field study of web application development projects to understand collaborative practices that unfolded from diverse members of a project team. Beaudry and Pinsonneault (2005) explored the strategies users chose in an effort to adapt to new IT introduced into a banking environment. Both research studies share features that are similar to this current study; however, the number of interviews that were conducted, ended when theoretical saturation was met. Theoretical saturation is the point at which gathering additional data about a theoretical category reveals no new properties nor yields any further theoretical insights about the emerging grounded theory (Charmaz, 2006).

According to Yin (2009), there are two jobs to be accomplished during the interview process: (a) follow the line of inquiry as reflected by the case study protocol and (b) ask (conversational) questions in an unbiased manner that also serves the needs of the line of inquiry. The interviews addressed the research questions and test the hypotheses while also evaluating TTF theory based on the answers provided. The complete list of semi-structured interview questions is listed in Appendix C. Applying both interview processes recommended by Yin created a rapport that allowed the respondents to provide the insight and answers to the phenomenon under study.

3.5.6 *Data Analysis*

Data analysis began upon the conclusion of the data collection process after the interview data have been transcribed into text. Table 2 lists the data analysis steps that fulfill internal validity through pattern matching, coding, memo writing, computer assisted tool (Miles & Huberman, 1994) and hypothetico-deductive logic (Lee, 1991). The primary data analysis technique of Miles and Huberman (1994) is used where coding of the transcribed data was completed line by line. Codes are tags or labels for assigning units of meaning to the descriptive or inferential information compiled during a study (Miles & Huberman, 1994). Each line of text analyzed from the interviews was linked to the set of codes developed for this study. Code development and reliability were established by linking specific terms from the categories of reported usability failures established by the organization to the TTF theory. The linkage provides the level of inter-code reliability and agreement by projecting a logical flow and meaning of identified and captured usability-related information systems security failures. The transcribed interviews were placed into the case study database, where each interview was coded to extricate the answers sought from the research problem of the study.

Table 2

Data Analysis Technique

Data Analysis Process for this Research Study:	Yin (2009)	Miles and Huberman (1994)	Lee (1991)
Pattern Matching	X	X	X
Hypothetico-deductive logic			X
Coding (Axial & Pattern)		X	
Memo Writing	X	X	
Computer Assisted Tool	X	X	

Note. The “X” in the data analysis technique table represents the data analysis steps to reach internal validity, along with triangulation prescribed by Yin (2009).

Through the application of hypothetico-deductive logic, as suggested by Lee (1991), data analysis tested the premise to reduce usability security failures; organizations must align security technology with tasks performed by healthcare workers and ensure that such alignment does not hamper security performance in a healthcare organization.

Following the preferred practices of Miles and Huberman (1994), the data analysis followed primarily a three-step process while also incorporating a contingency plan of revaluating the data analysis method to ensure theoretical saturation is fulfilled. The first step consists of the creation of a list of start codes before the interview phase is conducted. The initial start list codes are created from the research problem, research questions, research model, factors from the theoretical model, and hypotheses. For example, the theme of this research study is to understand the nature and types of usability failures in a healthcare setting; therefore, a start list code of "UF" which indicates a usability failure.

The second data analysis step is the development of pattern codes, explanatory or inferential codes that identify an emergent theme or explanation (Miles & Huberman, 1994). Pattern coding allows the grouping and summarizing of sub-codes, themes and constructs that are discovered from the interview process. In this data analysis process, pattern coding was conducted with the assistance of a computer-aided software tool, Atlas.TI. Atlas.TI is a tool that assists with coding and categorizing large amounts of narrative text that are often collected from open-ended interviews. The third step of data analysis is memo writing. Memo writing is the pivotal intermediate step between data collection and writing drafts of papers (Charmaz, 2006). Memo writing allows for the continued analysis of the codes and data collected throughout the research process. Memo writing was conducted at the end of each interview and after the codes and data have been assigned after the transcription process. Constant memo writing allows connections to develop, comparisons to be made, and the crystallization of questions and directions to pursue within a research study (Charmaz, 2006).

3.5.7 *Reliability and Validity*

Research design is supposed to represent a logical set of statements by which one can test and judge the quality of the design using the concepts of trustworthiness, credibility, conformability, and dependability (Yin, 2009). Yin (2009) recommended the use of construct validity, internal validity, external validity, and reliability respectively as the methods to test the quality of the case study. Construct validity was established by creating a chain of evidence. To increase reliability of a case study, Yin (2009) lists six sources of case study evidence: (a) documentation (b) archival records, (c) interviews, (d) direct observations, (e) participant observation, and (f) physical artifacts. A chain of evidence allows an outside observer to follow the trail of derived evidence from the research problem to the research questions, on to the conclusion of the case study. For this research study, construct validity was established using four out of the six sources of case evidence: the collection of documentation, archival records, interviews, and physical artifacts. The four sources of case study evidence was integrated into the case study report, case study database, and case study protocol, which further establish external validity and reliability for this study.

According to Yin (2009), internal validity seeks to establish a causal relationship where certain conditions are believed to lead to other conditions distinguishable by spurious relationships. Analyzing the data from the dialogue of healthcare workers and support staff confirms the relationships developed from usability-related information systems security failures. Following the data analysis steps suggested by several scholars (e.g., Miles & Huberman, 1994; Sarker & Lee, 2003; Yin, 2009) confirms that internal validity exists in this study.

External validity is knowing whether a study's findings are generalizable beyond the immediate case study (Yin, 2009). The ability to capture a usability failure and linking the failure to a specific task as well as the technology used to complete the task provides a means to understand the factors that created the usability failure. Once the relationship of the usability failure is established, an assessment of the failure can be determined, which allows the means to address or reduce the usability-related information systems security failure. The process used to study the nature of usability-related information systems security failures can be applied in most organizations that provide IT support to their staff. The key to obtaining generalizability is to understand when a usability failure occurs. Identifying the interaction that takes place between the task and the technology determined the effect the usability failure has on performance.

Reliability is obtained when the study can be repeated. Having a high level of repeatability provides the creation of a credible research project. Reliability can be verified by following the case study protocol developed for the case report. The case study protocol contains the instrument as well as the procedures and general rules in case study research to guide the investigator in carrying out the data collection from a single case study design (Yin, 2009).

3.6 Summary

In this chapter, the theoretical basis was discussed along with the methodology to address the research questions, and hypotheses of this study. The use of a single case study design with embedded units allows for the phenomenon of usability security failures to be identified, understood, and linked to a specific type of task and technology used in a HIS. The data collection and data analysis process provides the reliability and validity that not only provides the credibility and repeatability of this research endeavor, but it also creates the ability for many organizations and disciplines, particularly the HCI community a perspective of evaluating usability and security issues in a different vein. Lastly, a chain of evidence was provided, including the case study protocol, case study report, and case study database, which is available for outside observers.

Chapter 4

Case Study: Phase One Data Collection and Analysis

4.1 Introduction

The aim of this chapter is to describe the complete phase one data collection and data analysis process. The purpose of the phase one data collection and data analysis process was to address the first research question "What are the nature and types of usability-related information security failures in a HIS?" In the data collection phase one process, a SQL query was created to retrieve help desk records of reported usability failures dating back five years. The query retrieved all records within the time frame of September 1, 2008, to September 31, 2013, of help desk tickets that required an intervention by the development staff. Help desk tickets are stored in a database repository of cradle-to-grave dialogue of information of all problems reported by the users in the organization along with the information of the solutions provided by organizational staff. Analyzing the discourse between healthcare workers, support staff, and development teams allowed the identification and enhanced understanding of usability-related security failures and how the failures impact IS security performance within the healthcare organization.

Help desk tickets that require an intervention by the development staff are those that could not be resolved at the medical center or by the second-level national support teams. To apply the appropriate context to the problem under study, from this point forward, help desk tickets will be referred to as usability failures.

After the identification of the usability failures, *a priori* coding methods applying terms that describe and define the definition of TTF theory, the CIA triad, and the manner in which the organization under study classified and reported user problems provided the foundation of code and category development. Sub codes, codes, sub categories, and categories were the process that wove the identification, classification, theming, and understanding of usability failures in the organization. The following section describes the detailed approach to identifying and understanding the nature and types of usability failures.

4.2 Organization

The history of the current Veterans Affairs department (VA) can trace its roots back to 1626. From 1776 to 1811, to 1911, all which were prominent times in the history of the United States, specifically in times of national and international conflict, the sacrifice of American soldiers and their families was recognized by United States elected officials with the establishment and continual transformation of the VA to support the nation's veterans. The transformation consisted of providing medical and hospital treatment for all injuries and diseases of veterans, whether or not of service origin, along with the providing programs for disability compensation, insurance for service persons and veterans, and vocational rehabilitation for the disabled. The VA is organizationally structured into three main service lines: the Veterans Benefits Affairs (VBA), Veterans

Health Administration (VHA), and National Cemetery Administration (NCA). The VHA is responsible for all VA healthcare services administered by VA Medical Centers, Ambulatory Care and community-based outpatient clinics. The focus of this study has been within the VHA organization; therefore, from this point forward, only the VHA will be referenced in this study. The VHA is home to the United States' largest integrated health care system consisting of 128 medical centers, nearly 1,400 community-based outpatient clinics, community living centers, Veteran Centers and Domiciliaries. The VHA employs more than 239,000 staff at the aforementioned organizational elements, providing comprehensive care to more than 8.3 million veterans each year.

The VHA has an integrated healthcare system comprising a multitude of disparate and heterogeneous computer applications and systems. Those applications and systems are interoperable with VA system architecture composed of multiple programming languages and a diverse number of operating systems and hardware. Within the VHA, the Health Product Support (HPS) division are composed of teams of IT specialists who provide ongoing support to operational systems and are charged with analyzing the portfolios of existing products. The HPS support teams ensure prompt and effective problem resolution of organizational-deployed software, as well as ensure that such resolutions are executed in the most cost-effective manner available. HPS employees provide support to over 115 software applications. The 115 software applications along with the interactions and experiences of the users of the applications are the source of the study.

4.3 Code and Category Development

Saldana (2012) stated that a code in qualitative inquiry is most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data. Charmaz (2001) described coding as the critical link between data collection and their explanation of meaning. In the phase one data collection process, code identification was derived from the words and short phrases of users of the organization who encountered and reported usability failures. The usability failures reported by the study participants are the critical link that leads to theory testing in this study. The evolution of code identification to code creation was performed by capturing and synthesizing the words from study participants who reported usability failures to words that led to defining TTF theory and the CIA triad. The combination of TTF theory and the CIA triad is the link that identifies information system security failures. For example, when users report that they are unable to access a software application while attempting to complete a task, the phrase “unable to access” symbolizes that there was a potential task failure and a potential technical security failure. Therefore, an “unable to access” code is created. Further exploring the “unable to access” code can explain the root cause of the problem, as well as the user experience which essentially leads to testing the hypotheses in this study.

Code creation in this study follows the method prescribed by Miles and Huberman (1994). Miles and Huberman suggested creating start codes from the research problem, research questions, research model, factors from the theoretical model, and hypotheses. Following Miles and Huberman was the starting point in the code-creation process. The second step in the code-creation process was the data analysis step wherein patterns in the data are declared, termed pattern coding. Pattern codes are explanatory or inferential codes that identify an emergent theme or explanation (Miles & Huberman, 1994). Pattern coding allows the grouping and summarizing of sub-codes, themes and constructs that are discovered from the interview process.

Capturing start codes was done using the *a priori* coding method. *A priori* coding develops codes before the collected data are examined (Charmaz, 2006). In this research study, *a priori* codes were developed during first cycle coding to create start codes using the terms and conditions that caused usability failures. First cycle code review led to the extrication of 660 usability failures that ultimately developed the list of identified usability failures. The codes used to identify usability failures were organized into a hierarchy based on the TTF construct of task characteristic failures and technology characteristics failures. The hierarchical grouping were constructed iteratively through the development of sub codes transforming into codes, to codes transforming into sub categories, to sub categories transforming into categories that identified the nature and type of usability-related information systems security failures.

4.3.1 *Code Development and Analysis*

The foundation of code development was derived from the ESS screen capture (see page 44). The ESS screen capture depicts three key fields (a) Category, (b) Type, and (c) Item (CTI) that are essentially communicated to support staff personnel the nature of the usability failure. In figure 3, the *category* describes the type of system the healthcare worker attempted to use, while the *type* represents the application used, and the *item* represents the problem the healthcare worker encountered. Applying the CTI, this research study is able to develop a taxonomy of usability-related information systems security failures based on both healthcare task characterizations and security technology characteristics respectively. The process used to establish the usability-related information systems security failure taxonomy followed the phase one data collection process displayed in figure 4 (see page 45), applying the terms to each phase that is listed in Appendix B.

The combination of CTI, along with the reported problem summary and case log data created the sub code lists in Appendices D and E for both healthcare task characteristic and security technology characteristic failures. The process that classified whether the usability failure was task-related or technology-related was determined by the CTI, the problem summary, and the TTF theory defined by (Goodhue & Thompson, 1995). The initial task usability failure report in table 3 allowed the nature of the usability failures to be determined. The nature of the usability failures are essentially the root cause of usability failures. The nature of the usability failure was ultimately determined by the data from the case log, primarily because the combination of perspectives from the healthcare worker that reported the usability failure along with the support staff was required to accurately identify and classify the problem. An example of the code analysis process can be described by examining the first entry in table 3 as a reference.

The type of task was determined by reviewing the CTI and the problem summary. The first entry suggests that the healthcare worker encountered an application failure attempting to complete the task of scanning an Intravenous Order. The problem description states that there was an informational message presented that consisted of an “invalid lookup error.” The “invalid lookup error” translates to an “unable to retrieve information” usability failure. The inability of the healthcare worker to retrieve information is the nature of the failure.

A second task-related usability failure example requires highlighting the complex nature of diagnosing and troubleshooting usability-related information systems security failures. The second row entry in table 3 captured the CTI of HealtheVet-VistA. The HealtheVet-VistA CTI represents multiple disparate and heterogeneous applications and systems interacting in an effort to assist the healthcare worker complete a task. In this example, the healthcare worker was unable to obtain information using the reporting tool using the HealtheVet-VistA application and system. However, using a workaround of accessing the VistA system (alternate HIS), the needed information was pieced together to complete the task.

Table 3
Initial Task Usability Failure Report

CTI	Problem Summary	Case Log Summary
Applications-VistA Inpatient Medications 5.0 IV Orders Issue	Unable to scan IV orders	Local support, IRM, reports nurses are unable to scan particular IV orders. The nurses are receiving the following error message: Invalid lookup, do not give. The site will provide the IV order numbers. The site does have Remedy access and can grant system access if needed.
Applications HealtheVet-VistA	Multi-divisional reporting needed	The integrated data issue relates to the medical center location. It includes three locations. This was a former VISN, in which all medical centers were merged. Everyone was aware they were seeing the data from other medical centers. Everyone is aware of the sharing of patient information. Our major problem is the reporting. They cannot obtain reports for the different medical centers, which are identified. Med center has been continually using the NUMI application, but cannot separate out the RLOC data for medical center. The wards are identified with an alpha character representing each site for most reports, so people can select their MC wards, but this option is not available for RLOC and also in the Physician Advisor report.

Table 4 provides a list of security technology characteristic usability failures examples along with an explanation and interpretation of the data that allowed the classification of the failure. Technology characteristic usability failures follows the same process as healthcare task characteristic failures by combining the CTI with the problem summary to classify the nature of the usability failure. In table 4, the first example states that the Adverse Reaction Tracking application was receiving undefined errors. The interpretation of the CTI error with the problem summary suggest that the undefined error was due to data being missing that prevented both the healthcare worker from completing their task, and the software application from executing a programming step that would have created an adverse reaction report on a patient. The classification of the usability failure being technology-related was materialized by (a) missing data prevented the software from executing properly, (b) the problem was linked to a software execution failure, and (c) the healthcare worker was unable to complete the task using a workaround, hence requiring the development staff to intervene to resolve the problem.

Table 4

Initial Technology Usability Failure Report

Category Type Item	Problem Summary	Case Log Summary
Applications-Vista Adverse Reaction Tracking 4.0	Receiving Error (Undefined, Null Subscript, etc.)	58)<UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)13:43:09 ROU:PUGR1PA04 11178 55) <UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)13:41:05 ROU:PUGR1PA01 9319 54) <UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)13:39:09 ROU:PUGR1PA04 27578 53) <UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)13:37:51 ROU:PUGR1PA05 15822 52) <UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)13:36:54 ROU:PUGR1PA01 20907 50) <UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)13:27:46 ROU:PUGR1PA02 12565 46) <UNDEFINED>DSPLY+4^PSODGAL1 *GMRAL(64395)12:43:40 ROU:PUGR1PA04 24541 45) Let me know who I can send the data information to in encrypted outlook message.
Applications-HealtheVet-VistA	Enrollment Systems Redesign HL7 Messaging Issue:	We are having a problem with a patient's rated disability not showing an effective date. Our MAS Adpac says it shows in ESR but is not crossing over to our Vista system.

A second example of a security technology characteristic usability-related information security failure requires discussing the Application HealtheVet-VistA CTI in the second row of table 4. In this example, a data element is stored in the VistA system; however the data element was not transmitted over to the HealtheVet system. The programming code in the application between the VistA system and the Enrollment system should have transmitted the data element to the

HealtheVet system. In this particular example, the data element is required in order to process a Veteran's record on the HealtheVet system.

The CTI discussed earlier was not enough data to accurately classify task characteristics and technology characteristic usability-related information systems security failures. The dialogue from the summary field and case log fields listed in figure 3 (see page 44) was also required to determine the nature and type of usability failures. Table 3 lists examples of the initial failure report data from healthcare workers that framed the code analysis and essentially led to the classification of healthcare task characteristic usability failures. In essence a form of triangulation was employed to the code analysis process in order to accurately identify and analyze usability failures.

There were 660 records that followed the healthcare task characteristic and security technology characteristic code analysis process, however only a few examples are provided for understanding. Additionally, all duplicate sub codes were eliminated leaving 44 healthcare task characteristic sub codes and 53 security technology characteristic sub codes.

The sub codes were collapsed into a set of codes by grouping sub codes that were similarly related. For example, the sub codes of healthcare task characteristic usability failure of *access denied*, *access violation error*, *unable to log into the system*, *user access violation*, represents the code of *access failure*. The security technology characteristic usability failure sub codes were collapsed in the same fashion as the healthcare task characteristic usability failures. Using the sub codes from Appendix E as an example, the sub codes of *unable to transfer* *data, unable to transmit data*, *unable to upload data*, *unsolicited data merge*, *unable to receive data, system created duplicate transmission* represents the *data transmission* code.

At the conclusion of first cycle code review, the second cycle code review began. Second cycle code review was conducted to develop the categories developed from first cycle code review. According to Saldana (2012), the primary goal of second cycle code review was to develop a sense of categorical, thematic, conceptual, and/or theoretical organization from first cycle coding. The second cycle code review process allowed the transformation of sub codes into codes, and codes into sub categories, and sub categories into categories.

Additionally, during the first cycle and second cycle code review development process, the sub codes of “data” and “information” required distinct clarification to properly understand and categorize usability-related information systems security failures. This research study defined raw data as having no significance, while information was defined as coming into existence when context was added to data (Avison & Fitzgerald, 1995). To parse the difference between the two sub codes in the identified usability-related information security failures, data-related errors are presented under the group of security technology characteristics failures, while information-related errors are presented under the group of healthcare task characteristics failures. Data-related errors are errors discovered at the database and database repository level prior to the conversion of data into information, while information-related error are errors that occur after data are transmitted, received, and interpreted by the user where an action or response is expected from the interaction with information.

4.3.2 *Category Development and Analysis*

Categories were formed via the analytical coding processing. The establishment of categories in qualitative data analysis allows patterns to emerge from the data. Lincoln and Guba (1985) suggest framing categories by applying a process of classification and reasoning while using a tacit sense of intuitiveness to determine what data look alike while grouping into categories when evaluating codes to form patterns and themes. To manage, guide and refine the categories being developed, the rule of inclusion was used (Maycut & Morehouse, 1994). The rule of inclusion is a process where a category emerges followed by a proposed statement about the category along with an example of the respondent's words that contributed to the formation of the codes. Examples of the rule of inclusion used to develop pattern codes and themes are listed in Appendix F.

The category analysis process consisted of development terms that accurately represented the combination of usability failures codes developed. Combining the codes that were similarly related, to include the terms that defined TTF theory, the CIA triad; along with the analyzing the dialogue of the usability failures framed the categorical nomenclature. Additionally, the ESS repository user interface screen depicted in figure 3 (see page 44) are comprised of a combination of fields (CTI, summary field, and case log) that formed the code and category development. Analyzing the CTI along with the summary field and case log allowed this research study to classify task-related and technology-related usability failures. The healthcare task characteristic failures are comprised of the terms and attributes that describe healthcare task-related failures that healthcare workers encountered interacting with applications and systems. The security technology characteristic failures are comprised of the terms and attributes that describe security technology-related failures that healthcare workers encountered interacting with application and systems, however the distinct difference between healthcare task-related failures and security-technology related failures are that security technology failures are failures that (a) missing data prevented the software from executing properly, (b) the problem was linked to a software execution failure, and (c) the healthcare worker was unable to complete the task using a workaround, hence requiring the development staff to intervene to resolve the problem. The combination of code and categorical analysis provided the avenue for establishing a distinct difference among usability failures. The following paragraphs describe both the code and category development and analysis process.

4.3.3 *Healthcare Task Characteristic Failure Categories*

Construction of the task failure category code group was refined by grounding the sub codes, codes, and sub categories with the terms that provided clarity to the evolution of usability-related information systems security failures from a task failure in a healthcare organization. The two major categories in the task failure category group are Task Failure and Application Failure. The task failure category is the origin of encounters and interactions users of an HIS have and report within the organization under study. The encounters and interactions will provide a source of information to understand the synergy created when usability-related information systems security failures materialize while using the HIS. The application failure category was created to capture the CTI that the healthcare worker had the interaction failure. As discussed previously, the CTI represents the combination of system, application, and task that the healthcare worker was having an interaction with when the usability failure originally occurred. This application failure category allows this research study to thoroughly analyze the nature of the usability failure along with how the specific CTI affects security performance. Evaluating the historical performance factors of the CTI via the application failure category discussed in the case log entries of the usability failure provided the needed perspective to empirically investigate usability failures. The usability-related information systems security failures provide informational messages when the users encounter failures. Combining the CTI with the informational messages contributed to an enhanced understanding of the nature of the failures. The sub categories of the two major categories of the task characteristic code group will further explain the rationale in code and category choice development for this study.

Task Failure. The task failure codes of *access failures*, *interruption failures, security failures, service request, training,* and *unexpected behavior failures* are the codes that surfaced from the usability failure reports. The codes of *access failures, interruption failures, security failures,* and *unexpected behavior failures* occur during the execution of a task using the HIS. *Access failures* along with the *security failure* code errors are related to log-on issues or problem with the software handling a user’s security credentials. In essence, the user interface is where the interaction begins and ends with the software user. User interface literature primarily focuses on developing better interfaces (Shneiderman, Jacobs, Cohen, & Plaisant, 2009), and security for the interfaces (Bourimi et al., 2012; Brostoff, 2004); however, the combination of the former and latter approaches poses challenges, while leaving security in question. *Interruption failures* error codes are encountered by users when the software prevents task completion. It is commonplace that the software will provide an informational message suggesting the cause of the failure. The *unexpected behavior failures* error code is when the software performs in an unexpected manner. In those instances, the task could have been completed, but the end results were not expected which must be investigated to determine the potential risk that may exist to the HIS. *Service request* and *training* codes are requests the users of an application or system makes to support staff to improve upon the HIS or ask to learn how to appropriately use the HIS.

Application Failure. The application failure category provides an anchor to connect the type of task failure to a specific application failure down to the root cause of the healthcare task characteristic usability failure. Combining the task failure, application failure, and root cause of the problem essentially created a method to capture, identify, and understand non-technical usability-related information systems security failures. Having multiple types of information-related failures, there was a need to establish sub categories to appropriately manage codes and categories, therefore two sub categories were created. The sub categories of Information Quality (IQ) and Information Security were created. The IQ codes of *display failures*, *inaccurate failures*, *inconsistent failures*, *incompatible failures,* and *report error failures* were codes that surfaced with a high level of frequency from reported usability failures. The IQ codes were not errors generated and returned by the software application after a failure was identified by the application. Rather, IQ failure codes were detected by the users of the HIS as a result of viewing the feedback from a task that appeared to have been executed correctly. IQ has been discussed extensively in IS research literature and has been dubbed a critical success factor to an IS by Delone (2003) and Delone and McLean (1992). IQ is the fitness of the use of information, and is a multidimensional concept (Ballou, Wang, Pazer, & Kumar, 1998; Wang & Strong, 1996) with dimensions of accuracy, consistency, interpretability, timeliness, and completeness. In the healthcare context, IQ errors such as the inability of a healthcare worker to display data or a graph, as well as healthcare workers reporting they were receiving *inaccurat*e, *inconsistent*, and *incompatible* information can result in serious negative consequences. An example of received *inaccurate, inconsistent*, or *incompatible* information is the healthcare worker receiving the wrong results of a patient's blood test. The application may provide an informational message stating an error, in which the healthcare will evaluate the information by checking the blood test results against another clinical source where the inaccuracy, inconsistency, or incompatibility error confusion can be addressed with absolute certainty. The r*eport* error code also create a high level of concern, particularly when healthcare organizations conduct critical incident investigations, as healthcare workers and administrators use reports as one of the tools to evaluate medical incidents. The information gleaned from medical reports has the potential to save lives.

Information Security Failure. The information security failure codes of *misinterpretation failures, mismatch failures, missing failures,* and *unavailable failures* are codes that surfaced with a high level of frequency from the usability failure reports. The information security codes are similarly discovered as the IQ codes. They are typically not codes that are generated from the software application; they are codes discovered by the users of the HIS while attempting to complete their task. The information security codes were adopted via the in vivo coding process by using the exact words of the user who reported the failure. For example, the HIS user would have received information that he or she was unable to interpret correctly—thus stating it was "misinterpreted." Healthcare workers stated they received "mismatched" information, as well as information was "missing" or "unavailable." What distinguishes the difference between IQ failure sub category codes and information security failure sub category codes as it relates to the handling of information lie in the results and actions of the user when encountering the failure. The information security sub category seeks to understand from the participant of the study, the role and relationship a usability failure had on information security. In this study, the expectation was to have the user security practices unveiled through the steps chosen by the users when they encounter handling *misinterpreted failures, mismatched failures, missing failures,* or *unavailable* failures. This approach has been discussed by Wier, Douglas, Richardson, and Jack (2010), in that security is not the main goal of a user's interaction with a computer system; moreover, Post and Kagan (2006) asserted that employees in an organization are more likely to bypass security measures in order to complete a task. Hence, discussing and evaluating the thoughts and actions of a user after an information security failure gained new insight on how to address such failures.

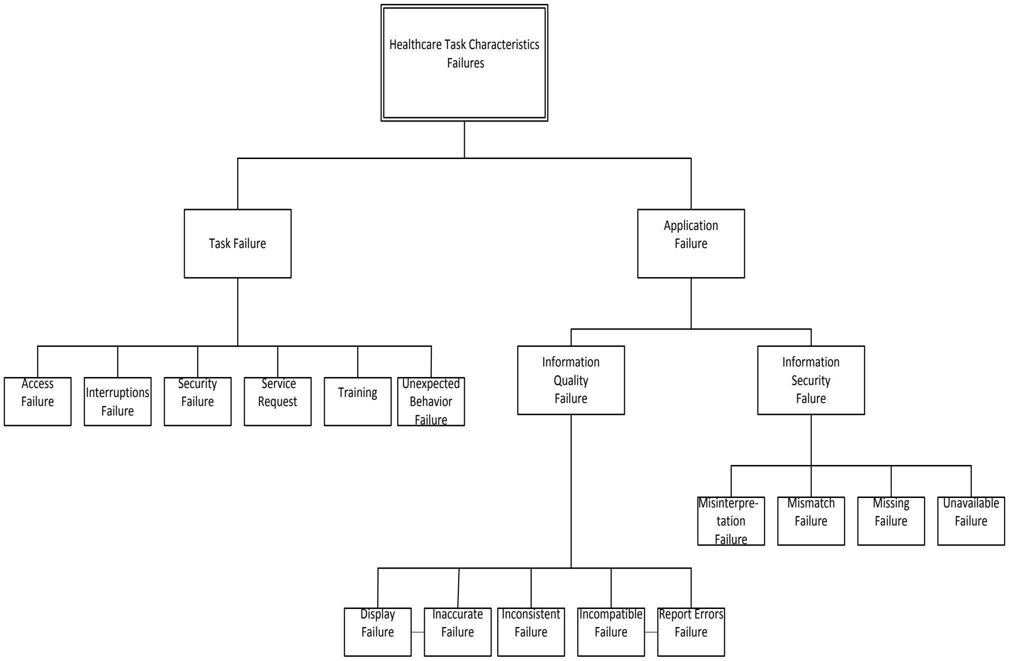


Figure 5. Healthcare task characteristic failures

4.3.4 *Technology Failure Categories*

Security Technology Characteristic Failures. The primary categories that emanated from the pattern coding process are system production failure, system reliability failure, and network connectivity failure. The codes in the technology characteristic code grouping are related to hardware components that comprise a HIS. In the healthcare environment, the HIS falls into four major categories: (a) clinical, (b) management, (c) strategic decision support, and (d) electronic networking and e-health applications (Austin & Boxerman, 2003). Clinical information systems support patient care; management information systems support non-patient care activities; decision-support systems assist senior managers in the area of strategic planning; and electronic data exchange and networking allows a healthcare organization to connect to national databases as well as to communicate with all users connected to the network. The security technology characteristic failure category grouping is shaped by both the HIS categories and Goodhue and Thompson's (1995) definition of technology characteristics: meeting the day-to-day operational needs of the users of the system. The information security context is applied and evaluated using the security requirements of confidentiality, integrity, and availability when the source of the usability failure is linked to the HIS.

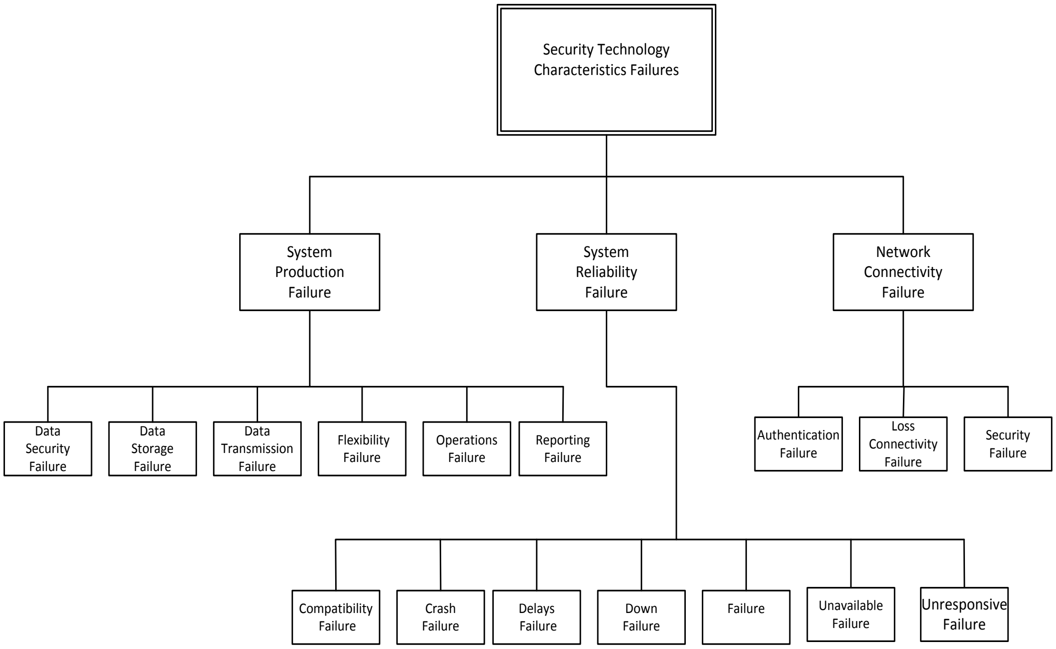


Figure 6. Security technology characteristic failures

The *system production* failure category consists of *data security failure*, *data storage failure*, *data transmission failure*, *flexibility failure*, *operations failure*, and *reporting failure* codes. The *system production* codes were discovered via in vivo coding by analyzing the reported usability failure data. *Data security failure* in this context is maintaining the integrity of information by healthcare workers as they enter data into the information system. *Data storage failure* and *data transmission failures* are the error codes reported by healthcare workers while making data request from databases or data repositories. The codes of *flexibility failures, operations failures,* and *reporting failures* are related to the feedback provided by the users as they access and use the information systems in an effort to complete their task. More specifically, as users of an HIS task and work processes change, the users will need the HIS to adapt and provide the flexibility needed to complete their task. For example, a new task request can be issued that requires the healthcare worker to run a report on a new outpatient clinic that is a division of a medical center. If the healthcare worker is unable to run a query to obtain the data, due to programming restrictions, the programming restrictions was the essence of a technical failure with the root cause being that the HIS did not have the “flexibility” required for the healthcare worker to complete the task.

System reliability failure category codes were generated using the same method and process used to identify system production codes. In vivo coding was used to capture the high-frequency pattern codes reported by the users who encountered failures. *System reliability* failure codes consist of informational messages that the HIS user will receive back from an application or system while attempting to complete a task. The failure codes are *incompatibility failure, crash failures, delay failures, down failures*, *unavailable failures,* and *unresponsive failures*. The system reliability failure codes are centered on the users' ability to connect to a HIS. The HIS within the healthcare environment are disparate, autonomous, heterogeneous systems, which can result in compatibility issues during the interoperability phase of computer systems' connecting and communicating.

Network connectivity failure category codes were generated using the same method and process that was used to identify system reliability codes. In vivo coding was used to capture the high-frequency pattern codes reported by the users that encountered failures. Network connectivity codes consist of *authentication failures, lost connectivity failures,* and *security failures*. The *authentication* error failure occurs as a user attempts to connect to an application or system while using a network connection. The most common occurrence that has been recognized in this healthcare environment is with web-based applications and with disparate, autonomous systems. With the high number of applications and systems connected to networks which are used throughout the healthcare environment, *authentication failures*, *loss of connectivity failures*, and *security failures* frequently occur when healthcare workers are unable to access software applications or systems. The *loss of connectivity* error code is network-related, while the *security failure* code is primarily related to a user's inability to transmit patient or confidential information via encrypted email or using file transfer protocols to send or receive large amounts of sensitive data.

4.4 Nature of Failures

To understand the nature of failures in this research study, the focus is on the failed interactions a user had with the HIS. The failed interaction is a healthcare task that was unable to be successfully completed or required other methods such as a workaround to obtain a satisfactory result. Ammenwerth et al. (2006) characterized the makeup of a healthcare task as comprising the wholeness of a working process to be completed (e.g., nursing documentation, order entry, etc.) by the user who is supported by the given technology. Focusing on the wholeness of the healthcare task by evaluating usability failures that required an intervention by development staff leads to understanding the nature of a failure. In the organization under study, a healthcare task and healthcare technology failures are linked to the inability of a user to accomplish his or her goal. The failure is primarily due to data or information not being delivered through technology that allows the necessary action to be taken based on established policies, standards, and working processes within the organization.

The nature of a usability failure requires the discernment of task-related and technology-related usability failures. The perception of task-related failures within a healthcare environment is slightly skewed based on the manner in which healthcare workers can mitigate their failures. Healthcare workers will use alternative means such as a workaround to survive a task failure, however that does not discount the ramifications of the task failures. The ramifications are a lack of productivity and lost time when workarounds are pursued due to task failures. Contrary to task failures, technology failures create a different reaction to healthcare workers in this study. Technology failures are caused by the tools of data, hardware, systems, and services failing as healthcare workers attempt to accomplish their tasks. Additionally, a technology failure in this research study included task failures that were unable to be circumvented via workarounds, which ultimately caused the reported usability failure to require an intervention by the development staff, leaving the reported usability failure left unresolved.

A usability failure is the inability of a user to use a healthcare product to effectively, efficiently, and satisfactorily to achieve his or her goal. Within the information security domain, an information security failure is the inability to protect the confidentiality, integrity, and availability, of the information. The combination of healthcare task failures, technology failures, usability failures, and security failures has transformed the aforementioned failures into usability-related information systems security failures (see Figure 7). Therefore, the nature and type of usability-related information system security failures consist of the attributes and characteristics of healthcare task failures, technology failures, usability failures, and information system failures respectively.

The attributes and characteristics of both healthcare task failures and security technology characteristics failures are caused by information integrity issues along with the unavailability of application and systems to healthcare workers. Information integrity errors occurred when the information transmitted was not the same as expected when it arrived to the healthcare workers and unavailability errors occurred when the information including applications and systems was not available to the healthcare workers at the time needed. Further, the terms and conditions that caused usability-related information systems security failures are the nature of the usability failure, and was the foundation used to develop a set of codes and categories that was used to evaluate and understand the nature and types of usability-related information security failures.

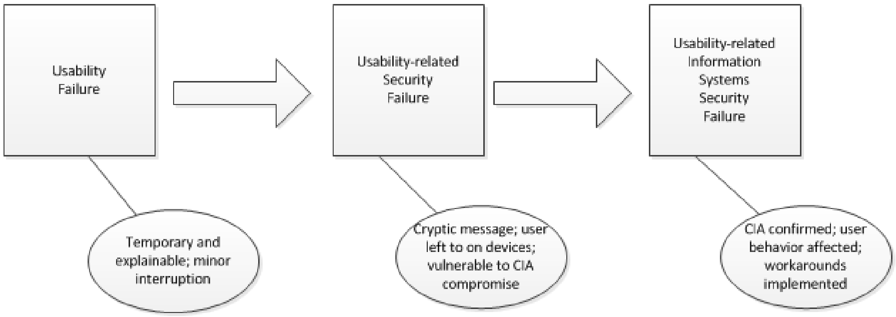

Usability Failure
Usability-related Security Failure
Usability-related Information Systems Security Failure
Temporary and explainable; minor interruption
Cryptic message; user left to on devices; vulnerable to CIA compromise
CIA confirmed; user behavior affected; workarounds implemented

Figure 7. Usability failure transition process model

4.5 Results

A total of 4,819 help desk tickets met the search criteria that captured and identified usability-related information systems security failures. The 4,819 captured failures were streamlined into 660 usability failures. The code and category connection is based on the TTF theory of (Goodhue & Thompson, 1995). The task characteristic code and category failure group linked back to the five factors of TTF: quality, locatability, authorization, compatibility, and ease of use/training. The technology characteristic code and category failure group linked to the technical factors which are production timeliness, systems reliability, and relationship with users. The usability failures were grouped into task characteristic failure groups and technology failure characteristic groups respectively. Combining the CTI from usability failures reported by healthcare workers with the summary and case log data of usability-related information system security failures allowed for an accurate identification of the nature and types of usability-related information systems security. The nature of a usability failure is the cause of a usability failure applying the definition of TTF, CIA triad, and anecdotal information provided by the ESS repository. The cause of usability failures are linked directly to information integrity and the unavailability of applications and systems. The combination of codes for the task characteristic group, and the technology characteristic group addressed the first research question "*What are the nature and types of usability-related information security failures in a HIS?*" In essence, the data collection and data analysis cycle was fulfilled following Miles, Huberman, and Saldana (2013), Charmaz (2006), and Miles and Huberman (1994).

4.6 Summary

This chapter described the complete phase one data collection and data analysis process to capture the nature and types of usability-related information systems security failures. There were 4, 819 help desk tickets captured through a SQL query that evolved from usability failures into usability-related information systems security failures. Usability-related information systems security failures were determined by the combination of healthcare task failures, technology failures, usability failures, and information security failures. Defining the combination of failures using TTF theory, the CIA triad, and the reported usability failures led to identifying the nature and types of usability-related information systems security failures in the organization. The code development process advanced the construction of a coding scheme for both task characteristic failures and technology failures respectively. The coding scheme will aid in phase two of the data collection and data analysis process.

Chapter 5

Case Study: Phase Two Data Collection and Analysis

5.1 Introduction

The aim of this chapter is to describe the complete phase two data collection and data analysis process. The purpose of the phase two data collection and data analysis process is to address the second research question "How does usability-related information systems security failures impact task accomplishment in a healthcare setting?" In the phase two data collection process, the researcher conducted semi-structured interviews guided by the theoretical framework of the study. The interview data were transcribed, coded, and analyzed using the Atlas.TI qualitative analysis tool. In addition to addressing the second research question, the analyzed data tested the hypotheses in figure 2 of this study. The following paragraphs will describe the details of the phase two data collection and data analysis process.

5.2 Data Collection Process

Participant selection for data collection was based on systematic sampling (Salkind, 2006). The query used to extract usability failures returned 660 potential usability failure cases. The systematic sampling process was started with the first usability failure cases returned, and, from that point forward, every 4th usability failure case was selected in an effort to obtain ten usability failure cases. The original goal was to analyze five task cases and five technology cases totaling 20 interview participants; however, the participant pool decreased when approval was not granted to solicit participants from one of the departments, as well as potential subjects declining to participate in the study. Based on the decrease in the participant pool, from the 660 cases, the research study increased the usability case analysis from 10 to 15. There were nine task usability-related information security failure cases, and six technology usability-related information security failure cases. The total number of participants in the study increased from the projected 20 to 22.

Although the case study increased along with the number of participants, data saturation was determined by cross case analysis (Miles, Huberman, & Saldana, 2013). Cross case analysis is primarily used when multiple case studies are analyzed. As explained by Miles et al. (2013), cross case analysis can be used to deepen understanding and explanation, while also pinning down data quickly that allows understanding how general categories of data are related. By analyzing usability failure cases separately first, data saturation was obtained at 15 usability cases, and 22 participants when it was determined that there were no new data being unveiled.

This research established the candidate pool by soliciting participation from organizational users who directly experienced the phenomenon under study. The research study participants consisted of members from 14 states and 12 medical centers. The names of the participants and the name of the medical centers will remain anonymous. The term *participants* and *respondents* will be used interchangeably when discussing the interviewee. The participants were tracked by referencing the task or technology failure, the case number being investigated, along with identifying the respondent by number. For example, if the first task case failure was being investigated, and the first respondent of the case was being interviewed, then the case was coded as TSKC1R1. The task is displayed as (TSK), the case number is displayed as (C1), and the respondent is displayed as (R1). Following the same scenario with a technology failure, the technology failure was coded as TECHC1R1. In nine out of the 15 cases studied, the researcher was able to get the perspective of two participants which enhanced the analysis of the usability-related information systems security failures. In the instances two participants were unable to be identified for a case; organizational documents, archived records, and observing the participant reproduce the usability-related information systems security failure provided research data to further analyze the case. Of the list of candidates interviewed, nine were IT specialists, five were nurses, three were clinical application coordinators, two were program analysts, and one each of a human resource specialist, pharmacist, and a medical administrative specialist respectively. The combined group of participants had a total of 316 years of experience working in the organization.

5.3 Data Analysis Process

Phase one code and category development was guided by the TTF theory. Code development guided by the theory used in this study is essentially theoretical coding, a sophisticated level of focused coding that specifies the possible relationships between categories developed during focused coding (Charmaz, 2006). Glaser (1978) argues that theoretical codes preclude a need for axial coding because they “weave the fractured story back together” (p.72).

Using the definition provided by Goodhue and Thompson (1995) for TTF, task characteristics construct is the actions carried out by individuals in turning inputs to outputs, while the technology characteristic is viewed as tools used by individuals in carrying out their task. Technology in this context is hardware, software, data, and user support services. Category emergence will be discussed later in this chapter.

5.3.1 *Interview Process*

The interview process for all participants was conducted by telephone, where the researcher captured the data by taking notes. The interview process lasted between 45 and 120 minutes, primarily due to the method used to collect the interview data. Appendix G list the case study interview record. The interview process consisted of the participant answering the interview question and providing an opportunity for the interviewer to recite the answer as it was stated to include an acknowledgement period whereby the participant agreed that the answers were recorded accurately. During the interview process, special attention was given to voice inflections of the participant to ensure the proper context of the answer was recorded. Further, any emotions displayed by the participants were questioned for understanding, allowing for an authentic analysis and reporting of the answers provided. Ten semi-structured interview questions in Appendix C were developed based on the theoretical framework to specifically address the second research question and the hypotheses; however, additional questions were asked to elicit the full meaning and understanding of the participants, while fully addressing the research questions and testing the hypotheses.

In conjunction with asking additional questions for clarity, two specific questions were added to the interview that further enhanced the data analysis process. The first question called for the participant to describe the originally reported problem. The question allowed the participant to recount his or her experience of the original interaction which ultimately added to the context that the researcher was attempting to capture. In addition to capturing the participant's interaction, asking the question allowed the researcher to accurately classify the cases under study with the appropriate usability-related information systems security failure type. After confirming the identified problems under study, the nine task characteristics usability-related information security failures are listed in Table 5.

Table 5
Task Characteristic Usability-related Information Systems Security Failure Cases

Case ID	Nature of Failure	Category	Sub Category	Code	Sub Code
TSKC1	Unable to add information	Task Failure		Unexpected Behavior	Unable to add information
TSKC2	Solicited information unreturned	Task Failure		Unexpected Behavior	Solicited information unreturned
TSKC3	Wrong information returned	Application Failure	Information Quality	Inaccurate	Wrong information returned
TSKC4	Information not displaying as expected	Application Failure	Information Quality	Display	Missing Information
TSKC5	Wrong information returned	Application Failure	Information Quality	Inaccurate	Wrong information returned
TSKC6	Unable to access information	Application Failure	Information Security	Unavailable	Unable to access system
TSKC7	Unable to update record	Task Failure		Unexpected Behavior	Unable to complete task
TSKC8	Unsolicited information displaying	Application Failure	Information Quality	Display	Incorrect information
TSKC9	Unable to enter accurate information	Task Failure		Unexpected Behavior	Unable to enter accurate information

Of the nine types of task characteristic usability-related information systems security failure cases, four of the failures types align with the task failure category, while the remaining five cases align with application failure category. Within the task failure category, the usability-related information systems security failure cases are linked to the unexpected behavior code. The unexpected behavior code is characterized by the user's inability to manage information due to the software providing an unexpected informational output preventing the task from being completed. The sub category of IQ usability-related information systems security failure cases have codes that are linked to display errors, and receiving inaccurate solicited and unsolicited information.

The technology characteristic usability-related information security failure lists five cases in table 6 that are aligned with the system production category, while the sixth case is aligned with the system reliability category. Within the system production category, four of the cases are linked to the operations failure code, one flexibility failure code, and one unavailability failure code respectively. The technology characteristic usability-related information systems security failure codes are characterized by users of the HIS inability to meet day-to-day operational needs of the users of the system. The flexibility code corresponds to adapting to the needs of the user, and the unavailable failure code represents hardware, software, data, and support services are unavailable (Goodhue & Thompson, 1995).

Table 6

Technology Characteristic Usability-related Information Systems Security Failure Cases

Case ID	Nature of Failure	Category	Code	Sub Code
TECHC1	Unable to update Database	System Production	Flexibility Failure	Unable to update data
TECHC2	Invalid Data Display	System Production	Operations Failure	Data Inconsistencies
TECHC3	Incorrect Data Stored in Database	System Production	Operations Failure	Data Storage Failure
TECHC4	Data Inconsistencies	System Production	Operations Failure	Data Transmission Failure
TECHC5	Missing Data	System Production	Operations Failure	Data Storage Failure
TECHC6	Data Unavailable	System Reliability	Unavailable Failure	Data Unavailable

5.3.2 *Pattern Coding and Theme Emergence*

A separate set of codes and categories were developed to extricate patterns and themes that were discussed by the participants during the interview process. These codes are essentially the transition point from the nature and types of usability-related information security failures that were discovered through the coding process to the information discovery process that will answer research question two, and test the hypotheses of this study, while using TTF theory to guide the analysis. The 20 codes generated during the code development process were reduced to 11 after further code analysis created three major theme categories. Applying in vivo coding from the interview transcripts were the process used to generate the code set. According to Miles et al. (2013) in vivo coding is appropriate for virtually all qualitative studies, but particularly for beginning qualitative researchers learning how to code data, and studies that prioritize and honor the participant’s voice. Figure 8 displays the hierarchy of patterns and themes developed which was prescribed by Charmaz (2001) and Saldana (2012). The information security threat theme is the domain that house and describe the pattern codes that were discovered during the data collection and analysis process. The pattern codes are the area of focus within the domain and theme of information security threat. In other words, the interview process unveiled the information security threat of *information integrity failures*, *inadequate security policies*, and *user security actions*.

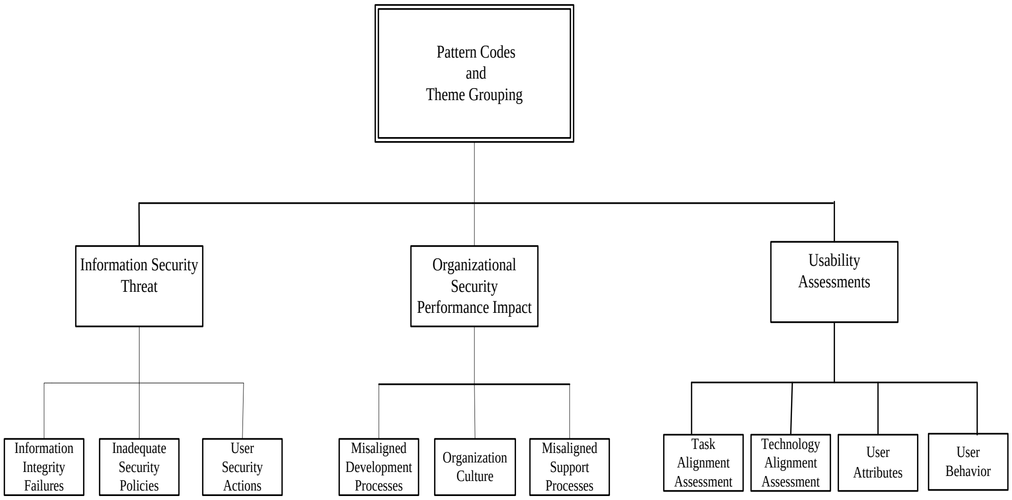

Pattern Codes and Theme Grouping
Information Security Threat
Organizational Security Performance Impact
Usability Assessments
Information Integrity Failures
Inadequate Security Policies
User Security Actions
Misaligned Development Processes
Organization Culture
Misaligned Support Processes
Task Alignment Assessment
Technology Alignment Assessment
User Attributes
User Behavior

Figure 8. Pattern code and theme grouping

After the interviews concluded, the collected interview data were analyzed based on the usability information systems security failure case groups and the interview questions. For instance, all task characteristic usability information systems security failures were grouped and separated by question, and all technology characteristic usability information systems security failures followed the same analysis pattern. In addition to analyzing each usability failure case groupings, a comparison was done between the task characteristic group and the technology characteristic groups to discover additional patterns and themes in the data. The following sections describe the major themes along with the information gleaned from feedback from the respondents under study.

5.3.3 *Information Security Threat Theme*

The first theme emerged from pattern coding was the information security threat theme. The pattern codes emerged as the participants described their interaction with their respective software application and system. There were six cases and 11 participants that provided data by which to analyze hypothesis two. Four interview questions were developed to test the hypothesis. The predominant code count consisted of *information integrity failure* (6), *organization culture* (6), *inadequate security polices* (10), *technology alignment assessment* (11), and *user security actions* (10). The less dominate codes were *development challenges* (3), and *support challenges* (3). With respect to the dominate codes, *inadequate security policies*, *technology alignment assessment*, and *user security actions* were analyzed and determined to be the catalyst to the information security threat in this study. When analyzing the interview data, the pattern codes of *information integrity failures*, *inadequate security policies*, and *user security actions* arose as the participants described the processes used to protect sensitive information that had to be shared to solicit individuals in the organization that could provide adequate support. Sensitive information was often extracted from their respective applications and systems and transmitted via encrypted email. The manner in which the respondents described how they managed sensitive and confidential information were described by both respondents from task case 3, one respondent from task case 6, along with tech case 2 respondent, where TSKC3R1 states: “I had to send the support staff the patient information via email. I sent the information using an outlook encrypted email message."

> TECHC3R2 comment was: "We use test patients. We blanked out patient names and ssns. We make sure no one can see screen names, and went through all the security prevention steps, such as locking the computer screen. Also use encrypted messages when patient data is sent via outlook mail."

> TECHC2R2 stated: "When we identify problem, we need information to talk about the problem, it does include patient information. I sent tier 2 an encrypted email message. Anytime we look at the error trap, it contains sensitive information, we have to be very careful to how we display or send the information."

> TSKC6R1 said: "I never had to give patient health information in this case. What I have done in the past, I would send encrypted information with screen shots of the data, or I would black out personal information as I provided a screen capture."

The respondents for both task and technology failures described how they were in compliance with organization security policy in relation to handling patient identifiable information. As the respondents discussed their reported usability failure, it was clear that 99% of participants were aware of security practices based on the dialogue. By the participants discussing their security practices whether or not they had to handle sensitive information, they were providing valuable insight that linked the inadequate security policy pattern code to the information security threat theme. There was one outlier security policy comment that questions how following the organization's security policies can also obstruct users from accomplishing their task as respondent from task case 1 shared by stating:

> "I send personal identifiable information via PKI; however what I have found is working with contractors pose a problem. The contractors that support the EDIS servers, does not have PKI, therefore I have found it difficult to share

> the information needed to troubleshoot some of the problems. Contractors are not held to the same standards as regular employees."

Task case 1 response reflect that although the respondent was cognizant of the organizational security policies, there was a clear level of frustration in how the organization supports its support staff personnel by employing contract personnel to develop and maintain applications. Contract personnel are not vetted for employment in the same fashion as VA employees, primarily due to contract personnel are hired to fulfill a task or job in a negotiated contract from a vendor. The contract may not have fully considered the individual ability to obtain the security clearance required to interact with confidential or private information. The respondent was essentially highlighting how applying one dimensional security controls (technical security) present additional challenges. Having contract personnel that organizational staff cannot share confidential information to provide accurate and timely support to healthcare workers negatively impacts patient care, and highlights how information security threats arise when organizational staff members are following organizational security policies. The researcher postulates that organizational security policies are inadequate and should be addressed when task accomplishment is negatively impacted when members of the organization follow organizational security policies. Additionally, the observation of this respondent also speaks to how software is currently being developed within the organization.

In this study, healthcare workers threat to information security did not occur from the actions the healthcare worker used to handle sensitive information. The threat appeared from the misalignment of the healthcare task and technology used by the healthcare worker. The threat to security was linked to the inability of healthcare workers to update data, data inconsistencies, data storage, and data transmission complications. To assess the length and degree of the information security threat related to the alignment of healthcare task characteristics with the security technology characteristics, the participants were asked questions about their ability to access the applications and systems used, to include the accuracy of the information the users were receiving while utilizing the HIS. The dialogue in which the healthcare workers expressed healthcare task-related and security technology-related failures came from four participants that reported both task-related and technology-related failures. TSKC3R1 comments were: "Yes the system is readily available. I can retrieve my information using the CPRS toolbar as well as using roll and scroll VistA."

> TECHC2R2 said: "Yes the system is readily available. We also have system monitors that tells us about system availability."
>
> TECHC1R2 said: "No the system is not providing accurate data. Since it is a calculated extract data field element that we are trying to fix, it is not currently accurate."
>
> TECHC1R1 said: "Yes it provides accurate and current information. It is integrated and pulls information from various applications. It stays current."

There are interesting contradictions in how users of an HIS perceive the performance of their HIS. The contradictions are captured in analyzing the responses from the participants as they described system availability and performance. To highlight the contradictions, the reported usability failures that were linked to information integrity and unavailability failures are listed along with the respondents that was interviewed that were involved with the same reported usability failure. The case scenario below, TSKC1, discussed the nature of usability failure which was classified as a healthcare worker unable to add information:

> "This was a national problem with the worksheet. The application would not allow emergency room staff to put a patient in the room, assign a nurse or give an acuity, until they assign a provider."

Following the reported usability failure, the two respondents that encountered and supported the usability failure had different points of views by saying: TSKC1R1 stated "yes, the system is readily available."

The second respondent (TSKC1R2), an IT specialist that provides national support to multiple applications and systems said: "There is a problem where data is being lost, based on how the architecture is setup. Network latency has created the loss of a patient data from the emergency room board."

The above case was a national problem that affected 128 medical centers. The first respondent stated that the system is "readily available," however what is not reflective in this answer that was evident during the interview, was the comfort and experience level the medical center employees had with the use of the application. This particular medical center participated in the testing of the application during the development process; therefore the medical center had a level of knowledge and experience to manage task and technology failures that simply did not exist for other medical centers. Respondent 2's perspective was from a national perspective, thus the evaluation of the system being "readily available" stemmed from viewing all 128 medical centers. This failure was an information security failure, in that the integrity of information was called into question, along with the application and system not being available. In the case described, the data discussed by the two respondents provided varying perspectives of the state of the application; however both respondents were consistent in the their answers as they reflected on their role by broaching topics on *information integrity failure*, *organization culture*, and *technology alignment assessment* that emerged from the information security threat theme.

A second example of contradictory responses in the failure description is seen below, with TECHC3 when the healthcare worker reported:

> We enter patient scores into the application. Once I put the data in, I had the option of putting start goals, and finishing or following up scores. Those are essential for us to do bench marking. If the type, start, goal, or finish date is not entered, the application should not allow me to continue adding data in the system. The application should not accept the case without having one of those not entered. The care type for the episode of care is important, but with the missing dates, the system was still working. That was wrong.

In the usability failure described above, there were four respondents that provide their perspective to the failure below:

> TECHC3R1, a registered nurse said, "yes, it is a user friendly application."
>
> TECHC3R2, an IT specialist said, "yes, the system is readily available. I have direct access to the systems, so whenever users in the field start having access problems, or notice delays, someone out in the field either calls me or send me an email message asking me what is wrong with the system."
>
> TECHC1R, a registered nurse said, "yes it provides accurate and current information. It is integrated and pulls information from various applications. It stays current."
>
> TECHC1R2, an IT specialist said, "for individual patients yes. Aggregate patients have issues. You sometimes cannot get the information you need quickly, and you sometimes have to double check the information to make sure it's right."

The task and technology data gets to the core of the information security threat theme healthcare workers have in common in this study. Healthcare workers understand the importance of protecting patient information, therefore following organizational security policies as it relates to sensitive information translates well to employees. However, healthcare workers have a strong desire to complete tasks that require them to protect patients, hence workarounds and alternative tasks that may circumvent organizational security policies. Therefore information security is more complicated in the healthcare environment with the methods available to users to mitigate information integrity failures and the unavailability of an application or system–thus a healthcare worker perspective differs based on the amount of obstacles that are present that prevents or delays task accomplishment. The question that is posed from the healthcare environment in relation to the information security threat, is to how to reduce the methods healthcare workers apply to mitigate information integrity failures along with the unavailability of data, hardware, software, and support services? This researcher postulates by evaluating *inadequate security policies* to address *user security actions* have when healthcare tasks are not aligned with the technology promotes security awareness and improves organizational security culture.

Based on the healthcare worker's perspective, the understanding of how information security was viewed was related to the codes of *information integrity failures, organization culture, inadequate security policies, technology alignment assessment*, and *user security actions*. Usability security failures along with the impact of IS security performance was influenced by information integrity, and the unavailability of applications and systems used by healthcare workers. When usability failures occur, the security of information is placed into jeopardy based on the organization predominantly using technical security controls, along with the healthcare worker having a strong desire to provide patient care in an effort to complete their task.

Identifying usability security failures are a unique endeavor in this study. While information integrity and the unavailability of information to users in the healthcare environment are prominently displayed in the captured usability failures, the root cause of the failures does not resonate to healthcare workers, primarily because the healthcare organization culture is well-versed at mitigating usability failures. Mitigating usability failures, coupled with the healthcare organization primarily applying technical security controls required focusing on the actions of the healthcare workers along with analyzing what was not said while discussing and understanding their usability failures. The actions of the healthcare workers under study explains how information security is applied within the organization, as well as how IS security performance is impacted during a usability failure. The dialogue captured within the information security threat theme displays how the full cycle of the information security threat materializes and is jeopardized when information integrity errors and the HIS is rendered unavailable to its users.

5.3.4 *Organizational Security Performance Impact Theme*

The second theme that emerged from pattern coding is the organizational security performance impact theme. The organizational security performance impact themes house the pattern codes of *misaligned development processes*, *misaligned support processes*, and the role *organizational culture plays*. The pattern codes gleaned from the interview process elicit the role each have on the organizational security performance impact as presented by the respondents in this study. The organizational support theme is understood from the combination of healthcare task characteristic and security technology characteristic constructs to determine the overall effects the failures have on an organization. *Misaligned development processes*, *misaligned support processes*, and *organization culture* were the patterns that formed to provide the imprint of the organizational security performance impact theme. The amalgamation of healthcare task and HIS security technology failure data was analyzed to determine the support needs of healthcare workers while interacting with their usability-related information systems security failure. To understand the HIS security performance impact, which can be traced to organizational support, additional interview questions were added asking the respondents to describe their specific usability-related failure case along with how the user was impacted by the failure. With the combination of all cases being used in the analysis of both the task characteristic and technology characteristic usability failures, a combination of answers from the information security threat theme and the usability assessment theme were used to realize the ramifications the failures had on the healthcare workers, thus forming the organizational security performance impact theme.

The organizational security performance impact theme data formed the pattern codes where the participants described the exterior interaction from use of the

HIS. The pattern codes that were formed were *misaligned development processes, misaligned support processes, and organization culture*. The participants regularly interacted with co-workers, and support staff as they attempted to manage their failure encounter. The dialogue of how participants responded to the usability failure they encountered in two instances were:

> TSKC1R1, an IT specialist said: "After triage didn't assign a provider in the application, I submitted a helpdesk ticket to see if it was a new feature that is being displayed in the application, or if it was a bug that caused the failure. It was indeed a bug."

A second respondent from TECHC2R2, an IT specialist that discussed a technology failure stated:

> "Sometimes I talk to the user and tell them that I found an error in the error trap, and they may not recall or notice a problem. That indicates that the data may not have been filed in VISTA correctly."

> TSKC2R2, an IT specialist stated: When the lab technician reported the problem, she said it was urgent, since it was related to IV medication, I knew it was important. It was not the type of medication that you can get from the pharmacy, so I knew to respond quickly.

The manner in how users of the HIS interact inside and outside the organization reflect how the *organization culture* pattern code emerged as a member of the organizational security performance impact theme. Healthcare workers and support staff members often interacted with subject matter experts at other medical centers before helpdesk tickets are submitted. That interaction process creates an opportunity of resolving usability failures in an expeditious manner. The dialogue by the respondents reflect how usability failures are analyzed at the beginning stages of a usability failure which leads to understanding the role of organizational culture play in resolving usability failures.

The following dialogue below from two respondents reflects the mindset of healthcare workers and support staff as they analyze and troubleshoot the usability failure. The *organization culture* is displayed by the respondents as they interact with the usability failure, and they are also providing a glimpse at both *misaligned development processes* and *misaligned support processes*. The experience healthcare workers provides often result in allowing support staff members to better understand the usability failures as well as how the usability failures impact the healthcare workers.

> TSKC1R1 response while interacting with an application associated with the emergency room follows: "I ran through the problem in our test account, and noticed what was happening, so I was able to duplicate the problem in the test account. The only troubleshooting we can do is add a patient, and go through the process. There is not much troubleshooting that can be done with a web-based system, so all I could do was refer the ticket to tier 2 support."

> TSKC6R1, a utilization manager that was interacting with a reporting application said: "I know it's a new program, and when it rolled out, the impact of this problem didn't exist, so the functionality of this problem may not have been realized. Let's work on this to get fixed. My on-going reaction is that it has gone on for many years, and it still hasn't been fixed."

The dialogue from task case 1, and task case 6 represents four challenges that has been predominately discussed throughout the research study (a) the manner in how applications and systems are developed and introduced into the organization reduces the ability of support staff to support applications and systems, (b) healthcare workers and support staff believes organization managers are not providing the support required to allow the employees to accomplish their task efficiently, (c) organizational managers have not recognized the impact of usability failures have on healthcare workers, and (d) organizational security performance is impacted on multiple levels when usability failures occur.

The impact of usability failures are captured from two respondents, where TECHC3R1, a registered nurse stated:

> "I was upset. I thought I had done something wrong because I was new. I reviewed my information, because I had written instruction and I put all the information like I was supposed to, so when I didn't have the score type, I knew I had done it right. I tried putting in the score type, and it wouldn't take it, but it should not have accepted the application. I tried putting it in again, so I was frustrated and confused, so I contacted the national team. I wanted to have someone look at it to see if I was doing something wrong."

The second respondent from TECHC3R2, a clinical application coordinator stated:

> "Initially, I got curious about how frequent this thing was happening, and whether or not if it was a fluke, so I ran a Fileman routine on the order file to determine if any other orders existed and whether there were additional inpatient med orders that had a display group of outpatient and a few other turned up. I determined that this was not a onetime problem, and that a system failure was going on, and it was happening more than once."

The dialogue from the participants covered in the above quotes highlight the thoughts of individuals based on the experience level within the organization, which ultimately encapsulates the organizational culture in respect to usability failures. Participants drew on their experience to manage a usability failure, but there are security implications around each failure, however information security failures are not easily detected and are addressed appropriately based on the nature of a usability failures because (a) the organization primary focus is on technical security failures and (b) patient care may not have been identified as being placed in jeopardy. The implications to this researcher's assertion is that the organization does not understand the risk usability failures present on the organization or the risk is negligible based on other information assets that may be placed at risk. The dialogue from TSKC9R, who is a pharmacist, discusses a clear usability failure that has caused the integrity of information to be placed at risk:

> "There is a field called Frequency in minutes. A field within the standard schedule enter-edit option. So this field determines for inpatient medication. It calculates when the next dose is due. The maximum number of that field is 129,600 minutes which is 90 days. We have medications right now in the system that is dispensed every six months. So it obviously does not account for that. That is the longest that I can account for, but I can imagine there are medications that are longer than that—yearly."

The respondent had more thoughts about the healthcare task failure:

> "The system does not allow us to account for doses that are standard doses for medication. It is set up to fail. It is no way for us to correct because the nurse is going to be prompted to give this medication three months early. There is no way for us to consistently notify the nurse that it needs to be given three months later."

The second usability failure captured is from a security technology-related usability failure. The nature of the failure is the invalid data display which is essentially an information integrity failure albeit presented differently when TECHC2R1, a clinical application coordinator states:

> "When pharmacist dispenses a medication to a patient, the provider or pharmacist does not want to prescribe a medication that the patient is allergic to. That's the purpose of the assessment. Either you have reaction assessment or you don't have an assessment. You cannot have both. This particular ticket had both."

After questioning the respondent about the usability failure encounter, TECHC1R1, a program analyst stated:

> "I was not sure if the problem was related to the task or the process I was trying to complete. The problem seemed to be tied to a programming error, because of how the data was returned. This was a unique problem related to one patient record. If that error was happening a lot that would make me think it was a process problem."

The data from the respondents illuminate the complex relationship between task, technology, and the user. An analysis is required to determine the cause and resolution of the problem, therefore the dialogue that exists from a reported usability failure is key to accurately adjudicating a failure. What must be brought to the fore in the data described by the respondents is these cases have not been slated for an intervention by the development staff. The healthcare workers perspective is to protect the health of their patients, which includes personal identifiable information, however the information security aspects of their usability-related information systems security case failures are not known, understood, or discussed by the participants.

According to the participants in this study, the fallout of the organizational mandates and how software is implemented into the organization have created organizational challenges with respect to both the support and development processes. With the advent of web-based applications, and organization data being re-located to data centers around the country, the organization now has a host of support challenges. The support challenges are centered on the loss of corporate knowledge, support staff reorganization, disparate support notification and communication tools, and access to software and hardware, which all ultimately result in poor response time to address problems, leaving a high amount of problems unresolved. The dialogue below from the respondents reflects the development of the organizational security performance impact theme from the misaligned support processes pattern code.

> TECHC3R1 thoughts were: “I am a registered nurse, in which have been employed with the VA since 2000. I work with spinal cord veterans. It would

> be nice to have a troubleshooting guide for all users to have access to that communicates a list of problems that the application is experiencing. That way, when problems are not fixed it a timely manner; we would at least know the cause of the problems to help us make decisions."
>
> TECHC2R2 stated: "I must say I have been a Clinical Applications Coordinator since 1999. I usually research a problem before I log a ticket. I know who to call, and I know where to look. In this particular case, there was no explanation as to why the problem happened, and that's why we logged the ticket. We never got a resolution, and unfortunate the problem never happened again, but I see from the transcript you sent me, the problem is still open."
>
> TSKC1R2 stated: "I am an IT specialist that have been employed with the VA for 30 years. Testing should have been better, and the problem would have been discovered. The development team should have been held accountable for the problem. The contractor was able to walk away from the problem without fixing it, before the 30 day point."
>
> TSKC2R2 stated: "I am an IT specialist that have been working with BCMA since 1987. I thought this problem had been fixed, because the development team released an emergency patch to clean up the variable that was not being renewed. It surprised me that you contacted me about this problem, and I was shocked that they only fixed half the problem. The nurses are using a workaround to clear IV drips."

There are three points of clarity that the respondents have revealed in their comments (a) the organization has highly skilled and experienced work force (*organization culture*) that has the potential to provide insight to reducing usability-related security failures, (b) there is a temporal element that is linked to usability failures that has been exhibited, particularly in how this healthcare organization addresses usability failures, and (c) the methods used to implement and develop software within the organization is not totally in alignment with the task the healthcare users are attempting to complete.

While respondents discussed their interaction with their support staff, the interactions produced profound results from the experiences communicating with staff members within the organization. Two respondents linked to both healthcare task characteristic failures along with security technology characteristic failures articulated the user perspective in relation to the organizational security performance impact theme when the following was shared:

> TSKC1R2, an IT specialist stated: "There are project managers, and developers that do not know the VA process. All they know is the PMAS process, if they didn't want to listen to the point of view of seasoned support staff; they basically missed an opportunity to use corporate knowledge."

> TECHC4R2, a clinical application coordinator stated: "The field has no expectations. When nothing happens, no one is pounding on the door. I have a problem that users don't report problems to me, because they feel nothing will be done about it."

The participants in this research study applied their experience to manage the usability failure they encountered by using resources to analyze the failure to determine the steps required to reduce the productivity loss due to the failure while also mitigating the failure. The analysis of the dialogue from the participants highlighted both support and development challenges healthcare workers are confronted with. For example, the development challenges are centered on the *misaligned development processes* employed within the organization. The *misaligned development processes* chooses from a pool of developers based on the competency level of the developer, and the project requirements. The fallout of the "developer project selection process," resides on how familiar the developer assigned to the project is with the application being developed. The *misaligned support processes* have been exacerbated by the restructuring of support teams within the organization that created new support policies that restricted support personnel access to medical center HIS.

Additionally, removing medical centers HIS and staging them at regional data centers that are now managed by contract personnel, has created a communication chasm that has increased the time usability-related information systems security failures are managed. The pattern codes of *misaligned development processes, misaligned support processes, and organizational culture*, were articulated by healthcare workers and members that supported usability failures to form the organizational security performance impact theme.

5.3.5 *Usability Assessment Theme*

The final theme garnered from analyzing interview data is usability assessment. The usability assessment theme houses the pattern codes of *task alignment assessment*, *technology alignment assessment, user attributes, and user behavior*. The pattern codes gleaned from the interview process elicit the role each have on the usability assessment theme as presented by the respondents in this study. The usability assessment theme consist of the overall user experience before, during, and after the failure encounter occurs. The emotions of the failure were confirmed when the participants articulated their experience while describing the usability failure. Finger pointing, frustrations, empathy, assigning blame assisted in developing the *user behavior* pattern code. The remaining pattern codes that were formed were *task alignment assessment, technology alignment assessment*, *user attributes*. When users in this study encountered a usability failure, their natural instincts were to assess whether or not their task was aligned with the technology in order to determine the root cause of the problem and the appropriate response to the usability failure based on their circumstances.

Based on the *user attributes*, which consist of experience and skill level, the user made choices on how to manage the usability failure. The user attributes often dictated the user behavior. Additionally, the usability assessment theme and pattern codes afford researchers an opportunity to evaluate the actions of users that encounter usability failures in a healthcare setting. The discussion with the respondents reflects the captured pattern codes when the respondents' state:

TECHC6R1, a registered nurse said: "They have had ample time to fix some of these problems, and yet they have continued to dog that system…it is very frustrating when you've done the review; you need to put it into the system to document it. Now you can't document the record you have obtained from the review, because the system locks up."

> TSKC7R2, an IT specialist comments were: "I looked at the problem after it was reported by the clinician in the test account. I tried to recreate the problem, but was unable to do so. I was not that familiar with the problem at the level that the error was occurring, so I had to escalate the ticket to the national team."

Once the user was able to complete their assessment whether there was a "task," failure or there was a "technology" failure with the application or system, the *user behavior* shifted into determining the source of the problem (*task/technology alignment assessments)* along with how to mitigate the failure. When the participants expected the cause of the problem was not related to their actions, a shift in behavior was detected. Five healthcare workers provided their thoughts and emotions towards their usability failure with the following dialogue:

> TECHC1R1, a program analyst stated: "None of this would be a problem if billers and coders would do what they are supposed to do."

> TECHC3R1, a registered nurse comment was: "I was upset. I thought I had done something wrong because I was new. I reviewed my information,

> because I had written instruction and I put all the information like I was supposed to, so when I didn't have the score type, I knew I had done it right."

> TSKC3R1, a registered nurse said: "I was slightly irritated, because it was a setback as I was on a tight schedule to get something done. Since I had a backup plan, I used the spreadsheet to complete the task."

> TSKC1R2, who is a seasoned professional stated: "I was pissed. The reason I was upset, was the way the software is developed today is based on PMAS and a timeline, and contracts that were not adequately made. The application contractor's contract ended, so they had not provided the amount of forethought that would adequately support the release of the software."

> TSKC4R2, an IT specialist said: "The initial troubleshooting consisted of asking HR staff to look into the old system to see how the data was displayed. It was displayed correctly, so I looked at the data dictionary at that specific field. The data dictionary showed that the numbers can be between 0 and 9.9999, so the root cause of the problem is percentages above 10 cannot be displayed. The development staff needs to change that data element to accommodate us employees, and it should be easy to do. I have no idea why it has taken so long to fix."

Evaluating the feedback from usability-related information system security failures discussed by respondents has led to three possible outcomes reported by users. The outcomes were: (a) An intervention was required by local or national support team members, (b) the healthcare worker utilized a workaround, or (c) the task was unable to be completed. Additionally, an intervention by local or national support team member indicates that the user was unable to come up with a solution for the healthcare task failure. Further, by contacting a support staff, the member suggested that there was a time element that factored into the intervention process. In the cases investigated, the time limit recorded to assist the user to complete the healthcare task failure cases ranged from 2 hours to 36 hours. The temporal element within the support process, ultimately attributed to emotional responses caused by inefficient, ineffective, and unsatisfactory interactions with the user interface, primarily because the healthcare workers understood task accomplishment would be delayed.

The outcome of a usability failure whether related to a healthcare task or a security technology failure, resulted in the healthcare worker utilizing alternative methods such as a workaround to complete the task. Workarounds and alternative methods were prevalent in this study. A typical workaround followed three paths. First, the healthcare worker would use the current software application in a different manner to produce the result expected from the original task; secondly, the user would look to use a different application or system to produce the expected outcome; and, thirdly, the healthcare worker would revert to a manual process by using paper products to complete the task. While discussing workarounds, it was confirmed that workarounds were limited to routine tasks. Furthermore, the use of workarounds and alternative methods presents a separate layer of challenges, such as the time required to complete the newly used task, the communication required throughout the organization to ensure all healthcare workers exposed of healthcare task failures use the same process, and to minimize information risk implied by the use of a new process.

When healthcare workers did not have alternative methods in which to choose from, their task was unable to be completed. While the sound of the healthcare worker’s inability to complete the task was reverberating throughout the organization, the effect of a healthcare worker’s inability to complete a task was not always immediately known. However, there was a high probability based on the data collected that non-routine tasks were unable to be completed due to access and skillset (*user attributes*) required to support the application and systems, as well as the limited troubleshooting capability of the web-based applications and systems the organization has integrated into its architecture. The pattern codes presented in the usability assessment theme are *task alignment assessment*, *technology alignment assessment*, *user attributes*, and *user behavior* of healthcare workers. The conversations with the respondents demonstrated usability-related information systems security failure created an internal process where the user assessed whether or not they executed the task correctly, if the task failure was not attributed to a user error, a process of troubleshooting the problem ensued. The more difficult the task accomplishment became, the more emotional the user became as they described their interaction with the usability failure. Hence, the development of the usability assessment theme, which encompasses the user attributes and interaction with a usability failure throughout the usability failure process.

5.3.6 *Impact Analysis on Task Accomplishment*

Healthcare tasks were compartmentalized into routine and non-routine tasks. A routine healthcare task is characterized by a task that users are adept at completing, and typically has a repetitive or intuitive nature to them, which allows for the creation of workarounds when roadblocks are encountered from task failures. Non-routine tasks required the use of multiple applications or systems (interdependence) to execute a task to completion. The difference between the two task types meant an additional strategy and user interaction existed as a non-routine task often depended on the operation of additional resources in order to function properly. Non-routine task were the tasked that created both intervention from national support teams and development staff personnel.

The interventions were primarily of a temporal nature that had a certain level of complexity based on communication challenges with support staff in the organization. The communication and support challenges centered on the structure of the organization, how usability failures were reported, and who had access to the support tools to add the essential troubleshooting and resolution information. During the interview process several respondents stated that they did not have access to the usability failure reporting tool, therefore the level of interaction was resigned to communicating with the support staff using email messages. In the cases investigated, the time limit recorded to assist the user to complete the healthcare task failure cases ranged from 2 hours to 36 hours. Among the 16 usability failure cases investigated, 86% of the cases have not been resolved. The open usability-related information systems security failures cases suggest that an information system security risk currently exist, and can be directly linked to the identified usability failures. The dialogue of the last entry placed on October, 2012, of a reported usability failure TSKC2 studied had the following entry: "This ticket is still a valid issue, do not close." Based on the communications and support challenges, the organization support practices are at best inefficient, and at worse have contributed to misaligned support processes.

The entry above is used to prevent a reported usability-information system security failure case to be closed without the failure being addressed by the development staff. In this study the entry suggest that the organization is vulnerable to information risk, and key organizational staff members are not aware of the information security threat.

The question posed from identifying and understanding usability-related information system security failures in relation to support challenges is what does the information mean? The challenges that healthcare workers were encountering within the organization was linked to how software and hardware are developed and integrated into the HIS. The healthcare organization under study development process radically changed in 2009 the way IT projects are delivered and managed. IT projects within this healthcare organization are required to deliver customer-facing functionality in six months or less. Customer-facing functionality essentially means to deliver software or hardware to healthcare workers within a specified time frame. The system used to provide the deliverables is the Project Management Accountability System (PMAS). PMAS is a disciplined IT development approach that uses data collection and monitoring tools along with business rules to produce IT functionality. In addition to using PMAS as part of the development process, ProPath is also used and is the companion tool to PMAS. ProPath is a process asset library that contains information of all VA processes that are linked to development projects. ProPath is a one-stop shop of formal approved processes, artifacts, and templates to assist project teams in facilitating their daily work. Respondents that are IT specialist, provided insight into how the development and implementation of software and hardware has impacted their productivity and performance within the organization with the following comment:

> TECHC1R2, and IT specialist stated: "The VA has gotten away from using the knowledge and programming expertise of its people that have used and developed software from the ground up, to now using a development system (PMAS/ProPath) that ignores the greatest gift the VA has."

A second statement expressed by an IT specialist from TSKC1R2 that was investigated was:

> "There are project managers, and developers that do not know the VA process. All they know is the PMAS process, if they didn't want to listen to the point of view of seasoned support staff provided to assist them; they basically missed an opportunity to use corporate knowledge."

The security implications discovered interviewing respondents that encountered healthcare task characteristic and security technology characteristic usability-related information system security failures are grounded in user behavior, credibility, economic, legal, productivity, and trust. Security comes into question with user behavior when the healthcare worker seeks workarounds to mitigate usability failures. Credibility, productivity, and trust issues materialized when respondents spoke of development and support challenges from usability-related information system security failures having a resolution rate of 14%. Credibility and trust follows two paths from the healthcare worker's perspective. Healthcare worker's perception is that they are losing credibility and trust from the Veterans they are charged to serve, while also feeling the manner in which software is developed and implemented in the organization has created credibility and trust issues among users of the HIS. Economic and legal issues manifested through information integrity failures where healthcare organization was unable to bill for services rendered, while the potential legal issues were concerned with inaccurate reporting of patient information.

The contradiction in how healthcare workers described their information security practices were discovered from analyzing usability-related information system security failures. The usability-related information system security failures were not considered an issue because technical security controls were not compromised; therefore a reaction to mitigate the failure by security professionals within the organization did not materialize. The non-action by security professionals suggest information security risk exist within the organization. The organization has strong security program that was prominently displayed in the manner how the respondents described the processes used to secure confidential and sensitive information. There was however, noticeable potential information security risk stemming from the information integrity and unavailability of applications and systems from both healthcare task characteristic and security technology characteristic usability failures. The information security risk has gone unrealized because (a) healthcare workers are unaware of the risk from usability-related information systems security failures, and (b) the development staff has not addressed the risk in resolving the reported usability failures. This researcher postulates that by the organization’s primary focus being geared towards technical security controls, therefore users of the HIS are unaware of the pitfalls of using workarounds and alternative methods to accomplish a healthcare task. Applying formal and informal security controls through security policies, education and training, along with information security awareness has the potential to reduce information risk as it relates to usability failures. Additionally, the organization’s culture must be evaluated to establish the exact measures required to bring awareness to the ramifications of usability failures, and how to most effectively reduce work arounds that will ultimately reduce information risk within the organization.

5.4 Hypotheses Testing

Hypotheses are statements in quantitative research, traditionally used in experiments, in which the investigator makes a prediction or a conjecture about the outcome of a relationship among attributes or characteristics (Creswell, 2012). Contrary to Creswell’s view of how hypotheses are used, and for which research methodology hypotheses are executed, Lee (1991) has provided a blueprint in which hypotheses can be used in qualitative research. Qualitative research can be executed with the same amount of analytical vigor as a quantitative study, which is done using the positivist paradigm following the rules of natural science. Following the rules of natural science the hypotheses under study will be satisfied by meeting four checks: (a) falsifiability, which is detected by contradictory observation; (b) logical consistency, which must be logically deducible from the same premise; (c) relative explanatory power, wherein one must be able to explain or predict the subject matter, and (d) survivability, in that the theory must be able to survive attempts to disconfirm (Lee, 1991).

Given the application of hypothetico-deductive logic (Lee, 1991), the three hypotheses tested can be observed by using a three-step process. The process is prescribed by Lee as observing the major premise which is a general theory, the minor premise which is a set of facts that describe the conditions, and the third step is the conclusion that is predicts or hypothesizes. The major premise is TTF theory, which holds that, for IT to have a positive impact on individual performance, the technology must be utilized and it must be a good fit with the task it supports. The following are the results from hypotheses testing.

5.4.1 *Hypothesis 1: Healthcare task characteristics will be associated with Task-Technology Fit.*

Healthcare tasks were parsed into routine and non-routine tasks. A routine healthcare task is characterized as a task that healthcare workers are comfortable and familiar with the steps required to execute the task to completion without the need of instructions or assistance. Routine healthcare task in this study suggest that there is a high probability that workarounds or alternative methods will be applied to complete a task when healthcare workers encounter usability failures. Non-routine tasks require the use of multiple applications, systems (interdependence) or additional checklists or instructions to execute a task to completion. The difference between the two task types lies in the strategies and resources that must be utilized to achieve task accomplishments. Of the nine healthcare tasks that were investigated, six were routine task, while three were non-routine. The two major types of healthcare task failures were linked to unexpected behavior of the software, and information integrity errors that prevented the healthcare worker from efficiently interacting with the information. All nine cases involved a failure in the handling or use of information. The list of healthcare task characteristic failures cases including the category and code selected can be viewed in table 3 (see page 60).

The arrow leading into Task-Technology Fit box (see page 33) from the Healthcare Task Characteristic box shows hypothesis 1. A high degree of support requires that the codes created for the task failure category and the application failure category codes determine the degree of TTF. There were 9 cases and 13 participants that provided data to analyze the hypothesis. There were four interview questions developed to test hypothesis 1. The predominant code count consisted of *organization culture* (13), *user behavior* (8), *user attributes* (7), and *misaligned support processes* (5). The less dominant codes were *misaligned development processes* (4). The minor premise and conclusion for hypothesis 1 is below.

When the healthcare worker encountered a healthcare task failure, the healthcare worker went through a mental checklist to determine whether the task failure was due to negligence or the failure was a result of the application or system failure. The manner in which the healthcare task failures were managed as well as the manner in how the healthcare worker responded to the error was directly connected to his or her role in the organization. The amount of experience the healthcare worker had within the organization, along with the amount of time spent working with the software or system comprised of user attributes that essentially had a direct correlation to the healthcare worker's behavior. Healthcare workers with more than five years of experience in the organization displayed a high level of emotion when discussing the healthcare task failure. Healthcare workers with greater than five years of experience were in a *technology alignment assessment* mode, as opposed to the healthcare workers with less experience who were in a *task alignment assessment* mode. The healthcare workers in *technology alignment assessment* mode were technically savvy; however, the healthcare worker displayed frustration, concern, and anger while discussing the healthcare task failure. Less experienced members displayed a sense of relief when the errors and failures were not caused by their actions.

Of the nine usability-related information systems security failure cases investigated, six cases were routine healthcare task cases, while three were non-routine healthcare task cases. The healthcare workers that encountered failures in the routine cases, four were able to use workarounds to complete their task, while two healthcare workers were unable to complete the task. Of the three non-routine healthcare task cases, two of the healthcare workers were able to complete their task when national support and development staff intervened, while the one remaining healthcare task was unable to be completed by the healthcare worker. The interactions and intervention of the healthcare task cases by support staff members and development teams indicated that the healthcare worker experienced major delays in accomplishing their task. Additionally, all nine usability-related information systems security failure healthcare task cases remains open waiting on a permanent resolution.

The results of hypothesis 1 strongly suggest that an association exist among healthcare task characteristic factors with TTF. This was conveyed first from the phase one data collection process, where nine cases were presented with task failure and information integrity usability-related information security failures. The combination *organization culture, misaligned support processes, user attributes, and user behavior* pattern codes affords this research to capture and demonstrate the total user experience while encountering a usability failure within the healthcare setting albeit varied based on individual ability and experience. The identification of the source of task failures essentially shows the correspondence of TTF; therefore, the hypothesis has been supported.

5.4.2 Hypothesis 2: *Security technology characteristics will be associated with Task-Technology Fit.*

In order to understand the context in which the participants of the study responded, there was a translation of terms required to satisfy testing of hypothesis two. A security technology characteristics construct is expressed by the use of the HIS. The HIS consists of hardware, software, and data. To ground an HIS into the context of security protection, the terms were further linked to potential threats to a HIS according to Dhillon (2007): (a) data modification, (b) destructions, (c) disclosure, (d) interception, (e) interruption, and (f) fabrication. The list of security technology characteristic failures cases including the category and code can be viewed in table 4 (see page 62).

The arrow leading from the Security Technology Characteristic into Task-Technology Fit box (see page 33) displays hypothesis 2. A high degree of support requires that the codes created for the systems production and the systems reliability categories will determine the degree of TTF. There were 6 cases and 11 participants that provided data by which to analyze the hypothesis. Four interview questions were developed to test hypothesis two. The predominant code count consists of *information integrity* failure (6), *organization culture* (6), *inadequate security policies* (10), *technology alignment assessment* (11), and *user security actions* (10). The less dominate codes were *misaligned development* *processes* (3), and misaligned *support processes* (3). The minor premise and conclusion for hypothesis 2 is below.

The threat to security was linked to the inability of healthcare workers to update data, data inconsistencies, data storage, and data transmission complications. To further discern the source of the failures, the participants described their task process that provided a means for understanding the source of the failure. The security technology failure was the malfunctioning of computerized HIS where the task of receiving data from a database or database repository failed to provide the healthcare worker with the expected results of the request. The questions posed to the participants by this research study sought to check the status and performance of their HIS, the accuracy and currency of data, and the security measures taken to protect data and information. One hundred percent of the respondents stated that the systems were available for use; however, two respondents added that the system was sometimes slow. The systems designated as slow performers were web-based applications that connected outside of their respective medical centers. The question related to the protection of data and information was answered by 99% of the respondents describing the steps they used to protect information. Each respondent described how he or she would transmit sensitive patient information to support staff members using encrypted email. Further descriptions of protecting sensitive information resulted in the healthcare workers describing a process of marking out sensitive data that were not required to troubleshoot a problem. The marking out of sensitive data eliminated the need for transmitting data via encrypted email.

The respondents conveyed that only information that was required to troubleshoot the problem was released to support staff personnel.

There was one outlier response to protection of sensitive information. One respondent described his frustration of working with private support contractors that do not have the ability to receive sensitive information to provide the necessary support. The respondent stated that there are private contractor support staff personnel who have not received background checks; therefore, they do not have the credentials or ability to access sensitive information within the organization. The result of this problem has limited the ability of organization employees to openly communicate with the private support contractors about security technology failures.

The primary causes of security technology failures were databases and data repositories providing duplicate, inconsistent, and inaccurate data. One of the respondents stated that 7 out of 10 attempts accessing her database would yield the information she asked for, while a second respondent stated that an individual record may be accurate, but, when she "attempts to run an aggregate report or a collection of records, the process fails." There was also a case failure that reported data inaccuracies due to the discovery of an algorithm that was miscalculating a data element that actually created the transmission and use of the wrong data.

Hypothesis 2 had strong results in the area of *inadequate security policies*, *technology alignment assessment*, and *user security actions*. The healthcare workers described how well they followed organizational security policies in the manner in which each healthcare worker engaged in good user security practices. However, the technical security failures in terms of the manner in which healthcare workers were not receiving the data as requested are essentially an information integrity issue which weakens security within the organization. Therefore, the conclusion found a reduction in security technology characteristics that created an association with TTF, hence resulting in a supported hypothesis.

5.4.3 *Hypotheses 3: Task-Technology Fit is associated with HIS Security Performance Impact*.

The HIS security performance impact construct is understood from the combination of healthcare task characteristic and security technology characteristic constructs to determine the impact on performance. The amalgamation of healthcare task and HIS security technology failure data was analyzed to determine the impact. To understand the HIS security impact, additional interview questions were added asking the respondents to describe their specific usability-related failure case and impact. With the combination of all cases being used in the analysis of both the task characteristic and technology characteristic usability failures, the major themes that were generated from pattern coding are used to measure hypothesis 3.

The arrow leading from Task-Technology Fit box (see page 33) to HIS Security Performance Impact box displays hypothesis 3. A high degree of support requires that the pattern codes created for the information security threat, organizational security performance impact, and the usability assessment themes determine the degree of HIS Security Performance Impact. A total of 22 respondents answered the questions involving the 15 usability cases investigated. Nine cases were healthcare task characteristic failures, while six were HIS security technology characteristic failures. Additionally, the total number of pattern codes from the three major themes was combined to accurately present the number of responses recorded. The information security threat theme had 26 responses, the organizational security performance impact theme had 36, and usability assessments had 33. The results of the data analysis process are reflected below. The theme code count exceeded the number of respondents due to some of the responses overlapping theme groups.

Of the 22 respondents who described the impact of their usability failure, two stated the failure did not negatively impact them from completing their task, nor was the impact of any concern. One respondent commented that, given the experienced and flexible staff, which was amenable to adjusting to the usability failure, the staff adjusted by seeking a temporary solution within minutes of the failure. A second respondent suggested that, although the failure was an issue, having an alternative plan to complete the task allowed the failure to not pose a problem or require the need to focus on the failure. However, ninety percent of the respondents described negative HIS security performance impact.

Ninety percent of the respondents described the HIS security performance impact affecting them in terms of user behavior, credibility, economic, legal, productivity, and trust. The aforementioned terms are the fallout from the information security threat, organizational security performance impact, and usability assessment themes respectively. Several healthcare workers described their usability failure encounter by stating they were angry, frustrated, and concerned when discovering their failure, which also included assigning blame for the cause of the failures. Another segment of the respondents discussed how usability failures have the potential of creating economic and legal issues if medical records are audited when medical error cases are investigated. One of the respondents described that inaccurate data from databases can affect the accreditation of clinical offices that are responsible to providing spinal care treatment and recovery services to veterans. Inaccurate data also had negative economic consequences when a program error mislabeled data, preventing medical organizations from billing insurance companies for the services provided by medical centers. Trust, credibility and productivity were discussed when one respondent stated that a new system mandated by Congress to eliminate fraud and create transparency had increased her department's workload by 400%. Additionally, productivity issues were evident in 86% of the cases primarily due to the cases left unresolved. In essence, the healthcare workers continue to seek permanent solutions to their reported usability failure; however, workarounds and task failure mitigation is the standard approach to manage said failures.

The results of hypothesis 3 suggest that Task-Technology Fit correlates with HIS Security Performance Impact. Based on the results, the hypothesis was supported. This conclusion was provided by analyzing the pattern codes, major themes, and the terms that emulsified while gaining a true picture of the impact from both task characteristic and technology characteristic usability-related information systems security failures. The six attributes of *user behavior*, *credibility*, *economic*, *legal*, *productivity,* and *trust* are sustainable when seeking to identify, understand, and reduce the nature and type of usability-related information security failures within this organization.

5.5 Summary

This chapter consisted of completing the phase two data collection and data analysis process. The process consisted of categorizing usability failures into a task and technology characteristic case groupings. Once the case groupings were established, pools of participants were interviewed to discuss their specific usability failure. The data collected from the interviews were analyzed using 12 interview questions. Information garnered from the interview process led to a need to evaluate the development process to reduce information risk from usability-related information system security failures. Additionally, the impact of task and technology failures had a pronounced impact on the area of user behavior and productivity, and on the organizational front, trust, credibility, legal, and economic impacts were expressed as factors that negatively impacted HIS security performance.

Chapter 6

Discussion

6.1 Introduction

The research focuses on understanding usability-related information systems security failures in a healthcare organization and how such failures impact IS security performance. This research study examined the nature and types of usability failures as a method to reduce usability-related information security failures within a healthcare organization. In order to execute this feat, the usability failures had to first be identified. Jacobson et al. (1999) described the nine types of usability failures that were covered in chapter 2, while Skov and Stage (2005) described usability failures through the use of a concept tool that categorizes usability failures as critical, serious, or cosmetic. Usability problems and failures are also identified through usability evaluation methods; however, usability evaluation methods cannot be compared reliably because of a lack of a standard criterion to measure and quantify usability, as well as not having a standard, stable process to follow (Hartson et al., 2001). Identifying a usability problem or failure simply is not enough; in fact, it is insufficient. According to Wixon (2003), usability practitioners must be able to explain them, understand what they involve, and how can they be fixed.

6.2 Findings

The argument presented in the first chapter states to reduce usability security failures, organizations must align security technology with tasks performed by healthcare workers and ensure such alignment does not hamper security performance in a healthcare organization. Moreover, this research postulates that the actions of the healthcare workers by using workarounds to mitigate usability-related information systems security failures has rendered the organization's information assets vulnerable to information security risk. The research problem has led to two research questions: What are the nature and types of usability-related information systems security failures in a HIS? How does usability-related information systems security failures impact task accomplishment in a healthcare setting?

The first key finding was in the discovery, identification, and reporting of usability failures by the healthcare workers. A high number of usability failures were identified through the analysis of data and information by the healthcare worker after the task had completed. In essence, the user interface did not alert the healthcare worker that the application or system did not effectively, satisfactorily, or efficiently process the request. It was in fact the actions of the users that were central to beginning the understanding and remediation of healthcare task failures.

The second key finding is related to how a healthcare task failure affects the actions of the healthcare worker. Among healthcare task failures, routine healthcare task failures created the highest opportunity for healthcare workers to use workarounds or alternative methods to complete a healthcare task after a failure was encountered. In this study, workaround and alternative methods to complete a healthcare task opens the organization up to information risk. Non-routine healthcare task failures, and technology failures often required intervention by support staff members or application developers, therefore, healthcare workers were less apt to subvert security controls, while providing application developers greater opportunities to mitigate information risk in the development process.

The third key finding was the identification and understanding the nature of usability-related information systems security failures. Usability-related information systems security failures are information integrity errors and the unavailability of application and systems to healthcare workers. During the analysis of task-related and technology-related usability failures, the root cause of usability-related information systems security failures were discovered by combining the definition of task-related and technology-related usability failures along with the information security failures. The combination of healthcare task failures, technology failures, usability failures, and security failures transformed the aforementioned failures into usability-related information systems security failures.

The fourth key finding was through the identification of the nature and types of usability-related information system security failures created a method to identify misaligned healthcare task with the technology currently being developed and implemented in a healthcare setting. Additionally, the method used to capture misaligned healthcare task with the technology also has led to identifying and understanding the impact a healthcare task failure and security technology failure negatively impacts security performance with the HIS. The impact security performance has on the HIS is realized through user behavior, credibility, economics, litigation, productivity, and trust.

The fifth key finding consisted of discovering how to reduce usability-related information systems security failures in the healthcare organization. There is a direct correlation between healthcare task failures and the technology used in this healthcare setting as it relates to HIS security performance. By adapting a method within the development process that targets the information integrity errors along with the causes of unavailable systems provides flexibility to reduce usability failures from misaligned healthcare task and technology failures while increasing security performance in the organization.

6.3 Discussion of Findings

This section discusses case study phase one data collection and data analysis along with case study phase two data collection and data analysis process.

6.3.1 *Case Study Phase One Discussion*

Evaluating the usability of applications and systems in the healthcare context proved fruitful by isolating healthcare tasks along with the technology used, provided a channel to evaluate the effectiveness, efficient, and satisfaction of the task (ISO 9241-11, 1998). When healthcare workers were unable to effectively, efficiently, and satisfactorily complete their task; a usability failure existed and was reported by healthcare workers.

Based on the nine types of usability failures described by Jacobson et al. (1999), six types—(a) the user articulates a goal and cannot succeed in attaining it, (b) the user explicitly gives up, (c) the user articulates a goal and has to try a different method to find a solution, (d) the user produces a result different from the task given, (e) the user expresses surprise, (f) the user expresses some negative affect or says something is a problem—were presented in this study, therefore aligning with usability research. Additionally, to further classify the gravity of usability failures, in this study all 15 cases of usability failures were classified as critical or serious following the failure taxonomy used by (Skov & Stage, 2005).

The discovery of usability failures were identified by using TTF theory as a guide. The usability failures were placed in two categories based on whether the usability failures were task-related or technology-related. Task failures were further classified as non-technical information security failures while technology failures were classified as technical information security failures. From the usability failure categories, it was discovered that the root cause of the failure were due to information integrity failures and the unavailability of applications and systems. The information integrity and unavailability of application and systems were identified and understood to be the nature of usability-related information systems security failures. Information integrity failures are directly associated with DQ and IQ errors that further established a relationship for the identified usability failures. The unavailability of an application or system equates to the unavailability of information to the healthcare worker in this study. Both information integrity and the unavailability of information is an information security requirement; therefore the integrity of information along with unavailability of said information is an information security failure.

This research discovered that the healthcare worker's ability to complete a task was related to the quality of information returned while interacting with the HIS. The testing of the TTF theory resulted in (a) the original task can be completed by the healthcare worker without full dependency of the technology, and (b) individual performance is not a factor in measuring TTF within this study. Historical data, manual processes, access to multiple non-primary software application and systems have been used to assist healthcare workers in completing a task when confronted with a task failure. Also, in this study, the individual performance level was negated primarily by this study focusing on usability-related information systems security failures that required an intervention. This approach essentially eliminated measuring individual performance which is often attributed and measured in similar studies that use TTF theory. The use of TTF theory provides a single focus by creating a pathway to identify a non-technical usability failure and follow its path throughout the failure cycle to determine the cause and impact. An interesting aspect of task-related usability-related information system security failures within a healthcare organization requires additional investigation due to the mitigating circumstances of such failures in a healthcare organization. The mitigating circumstances are the workarounds that are available to healthcare workers.

Healthcare workarounds are prevalent within this study, particularly when healthcare workers encounter a task-related usability failure. In healthcare literature, workarounds have been researched from various perspectives using the tools clinicians and healthcare workers use; however, according to Halbesleben et al. (2008), there is a lack of theoretically grounded and empirically tested understanding of the causes of workarounds and their impact from an HIS. This researcher likewise suggests that workarounds, particularly in this study, are used to get around a problem rather than displaying defiance or opposition. Additionally, hospitals view workarounds as an evasion of standardized routines that the hospitals insist save patient lives and safeguard hospital financial resources (Halbesleben et al., 2008), while healthcare employees believe workarounds increase their performance and patient safety (Beaudoin & Edgar, 2003). Workarounds are part of the culture of healthcare organizations primarily to thwart the unavailability of technology. However, that does not preclude the creation of answers to resolve workarounds as suggested by (Halbesleben et al. 2008; Yang, Ng, Kankanhalli, & Yip, 2012).

This research has established that usability failures, task failures, and technology failures can be addressed by analyzing the dialogue of healthcare workers when usability failures are reported. This approach is significant in the area of usability, as usability research primarily evaluates usability empirically during the testing or implementation stages of the usability development process (Akers et al., 2012). The research approach in this study has empirically evaluated usability failures by focusing on task and technology to determine the true user experience while applications and systems are currently used in the organization. Additionally, by analyzing the information provided by users of an HIS after usability failures are reported, further allows the capturing of additional usability failures that are not detected from the interaction with the user interface.

6.3.2 *Case Study Phase Two Discussion*

The behavior of healthcare workers was manifested by their response to the usability failures they encountered. The behavior was voiced in frustration, anger, lack of production, trust, credibility, and empathy due to the failures, suggests that this research should follow the results of said behavior through the actions of the users. The usability failures have led to healthcare workers employing workarounds to complete their task. According to Post and Kagan (2006), employees in an organization are more likely to bypass security measures in order to complete a task. In a healthcare organization where task completion can be life or death, healthcare workers will seek alternative methods to complete a task. Healthcare workers are driven to complete their task; therefore, in this study, the line of examination is to determine the type of threat existing from healthcare workers using workarounds to complete their task, particularly given the level of frustration and anger that goes along with the failure.

The behavior of users in relation to protecting information and information systems assets are covered by (Fagnot, 2008; Stanton et al., 2006). Two streams of information security research that addresses user behavior are counterproductive computer usage (Stanton, 2002; Weatherbee, 2010) and insider threat (Post & Kagan, 2006; Siponen & Willison, 2009). Counterproductive computer usage consists of a computer user in an organization that exposes the information assets to risk or liability or a loss of productivity time by engaging in activities that are counter to established computer resource usage policies (Ifinedo, 2014; Mastrangelo, Everton, & Jolton, 2006). Insider threat refers to intentionally disruptive, unethical, or illegal behavior enacted by individuals who possess substantial internal access to the organization's information assets (Stanton et al., 2005). The challenge presented from these two streams of research along with the information from this study suggests that the users of the HIS are not involved in intentional or unintentional security policy violation; therefore, how does user behavior get addressed when the organizational information security policies are not knowingly violated, although a potential threat exists? The answer was not forthcoming from Crossler et al. (2013), although the researchers made an effort to move behavioral information security research forward by separating insider deviant behavior from insider misbehavior; however, neither example nor definition applies to the healthcare worker.

A conceivable solution is to address user behavior through security training and awareness. Healthcare workers are unaware of the effects circumventing healthcare task failures through workarounds have on organizational security. Also, organizational managers have not yet understood the magnitude usability failures have on the organization, primarily because user security is managed through the technical view; therefore organizational managers are more concerned with security failures that are derived and related to technical failures. By addressing user behavior through security training and awareness has the potential of improving organizational security culture—thus reducing healthcare worker workarounds.

While analyzing the impact of usability-related information systems security failures, there were findings discovered from the interview process that required addressing. The research uncovered that usability-related information systems security failures highlighting the impact of misaligned task and technology have on an organization. The main areas impacted in the organization were economic, legal, trust, and credibility. The recognition of the impact was expressed from feedback healthcare workers experienced while working with the organization customers, as well as from the results of organizational policy changes including the motivation and implementation of new software applications and systems. The credibility, economic, legal, and trust fallout materializes through the organizational security performance impact theme. Based on such "impact attributes" discussed, the overarching domain in which the attributes should be addressed is through software development.

The fallout of usability-related information security failures provided the foundation for understanding the security implications from the failures. Healthcare workers that encountered usability failures whether task-related or technology-related had an emotional reaction to the failure. The emotional reaction contributed to workarounds in this study, along with the reluctance to report usability-related information systems security failures. The security implications of the user reactions are violation of the organization security policies. This researcher postulates the actions of the healthcare workers to use workarounds mitigating usability-related information systems security failures has rendered the organization's information assets vulnerable to information security risk.

The organization security implications are derived from how the organization’s inability to identify, understand, and address usability-related information systems security failures. The healthcare organization under study primarily used technical security controls to protect its information assets. Technical security controls are visible throughout the organization in the organization security program to include the development process. The development process security-related artifacts uses access controls as the primary focus to protect information assets. Researchers (Baskerville, 1993; Straub & Welke, 1998; Dhillon & Backhouse, 2001) have gone on record stating IS security can be more effectively managed if the emphasis goes beyond the technical means of protecting information resources. With the healthcare organization development process focus being on the technical view, the user viewpoint and role in the organization suffers.

Siponen (2002) suggested that organizations that employ the technical view ensure users can understand and follow their security mission easily, however at worst the user will not understand the relevance of security actions which will result in the users actions to be enforced or transition in the right direction. Moreover, the organization had a clear variance practices in the development process between newly developed software and software that required patching through maintenance. Software that required maintenance was the usability-related information security failures under study. Evaluating the communication history from development staff, reflect that there was not on-going communication established that provided opportunities to address usability-related information security failures in the development process.

The question posed while addressing the research questions was how does user behavior get addressed when the organizational security policies are not knowingly violated, although a potential information threat exist from the fallout of usability-related information systems security failures? To begin to address the root cause of usability-related information system security failures is to evaluate the organization’s development process. The development staff must first understand the impact of information integrity failures and the unavailability of applications and systems have on information security along with the users of the HIS. Additionally, both organization leadership and the development staff must recognize that usability failures are directly associated with information security failures and ultimately threatens the security of information resources.

Based on the organization under study primarily using a technical view to execute information security in the organization to include the methods used in the development process to address and reduce usability-related information systems security failures can be done in the development process. The organization currently uses a rigid IT development process of PMAS and ProPath that seeks to meet the needs of the customers by producing IT products through communications and timelines. The development process uses a process management approach that all project management and development team members follow. Incorporating the meta-notation framework proposed by Siponen et al. (2006) that provides the opportunity to incorporate security requirements in the design phase aligns with the current development method and processes used in the organization. A proposed process to reduce usability-related information systems security failures consist of applying the security controls against the identified usability-related information system security failure. This can be done during the troubleshooting phase of the usability-related information systems security failure; the failure will be associated with a specific application or system. The root cause of the usability-related information systems security failure can be modeled in the development process through PMAS and ProPath process while repairing the reported usability failure. The organization's help desk repository stores a history of cradle-to-grave communications on all usability failures. The information from the help desk repository is the catalyst to reduce usability-related information systems security failures by analyzing the information specific to task-related and technology-related failures to ensure alignment between the task and technology. Tracing the source of usability failures through the help desk repository improves application and system usage, while also improving information security within the organization.

6.4 Summary

This chapter addressed and discussed the finding of the two research questions along with the results of the hypotheses tested. The findings were compartmentalized by case study phase one, and case study phase two of the data collection and data analysis process. The findings for case study phase one process found that the nature and types of usability-related information systems security failure were caused by information integrity along with the unavailability of applications and systems. Phase one case study also determined that usability failures were also discovered outside of the user interface. Phase two case study found that the organization under study primarily uses technical security controls within the organization, therefore usability-related information failures were confirmed not to have been addressed by (a) development staff not addressing information integrity and application and system availability failures, (b) the development staff not identifying and understanding the nature and types of usability-related information system security, to include the threat the failures have on information assets, (c) the development process varies between newly released software and software that requires a fix, and (d) a lack of communication between users of the software and development staff reduces the effectiveness of the software released into the field. To address usability-related information systems security failures, a non-technical approach should be applied throughout the organization. A non-technical approach has the potential to address the healthcare organization culture of using workarounds when task and technology is found to be misaligned, thus creating usability-related information systems security failures.

Chapter 7

Conclusion

7.1 Introduction

In this chapter, a summary of the research findings are presented and the hypotheses tested, along with the goals of the study. Additionally, the limitations, implications of the study for research and industry, along with future research opportunities are covered. Future research recommendations have the opportunity to forge a stronger link between the usability, information security, and healthcare communities by better aligning healthcare task with the technology used while reducing information risk when usability failures occur.

7.2 Findings Summary

This research sought to identify and understand the nature and types of usability-related information systems security failures within a healthcare context. There were five key findings that were unveiled. The first finding was in the discovery, identification, and reporting of usability failures by the healthcare workers. The second finding was related to how a healthcare task failure affects the actions of the healthcare worker. The third finding was the identification and understanding the nature of usability-related information systems security failures. The fourth finding was creating a method to identify misaligned healthcare task with the technology currently being developed and implemented in a healthcare setting from identified usability failures. The fifth finding consisted of discovering how to reduce usability-related information systems security failures in the healthcare organization. By adapting a method within the development process that targets the information integrity errors along with the causes of unavailable systems provides flexibility to reduce usability failures from misaligned healthcare task and technology failures while increasing security performance in the organization.

The discovery of the five findings required a translation of usability, healthcare, and information security terms in order to create a usability failure taxonomy to appropriately examine the failures. The taxonomy allowed the discovery that the task-related and technology-related usability failures were misaligned and ultimately caused information integrity and the unavailability of applications and systems. The failures the healthcare workers were encountering led to creating workarounds in order to complete their task. In the evaluation of the usability-related information systems security failures, it was clear that non-technical information security controls would be most effective in an effort to reduce the failures. The organization uses a technical view to implement their organization security program which carries over to how software is developed and maintained in the organization. Leveraging the information and dialogue from reported usability-related information systems security failures and applying the information to the organization’s development process have the potential of reducing information security risk in the organization.

7.3 Limitations

This research study had four limitations. The first limitation is that this research study was conducted within a large government healthcare organization that has an integrated HIS that interconnects with 128 medical centers around the United States. The organization uses a combination of proprietary and nonproprietary software to include disparate, heterogeneous, and autonomous systems. The architecture used, along with the organization composition, may impact generalizability. A second limitation was the usability case study selection process. Systematic sampling was used to select the cases along with the candidates for the study. The cases selected required a candidate to volunteer to participate, which ultimately reduced the case and candidate pool. The third limitation was the temporal aspects surrounding usability-related information system security failures that were analyzed. The average case analyzed was two years old from the original date the failure was reported. Although there was an abundance of information available to discuss the cases with the candidates, several candidates were unable to recall all the details of usability-related information system security failure at the time it happened. The final limitation was the inability to expand the candidate pool and case selection pool to include development staff members to participate. The development staff members are composed of contract employees who were unable to participate due to contract obligations. The development staff members provided an opportunity to discuss potential security intervention controls related to the specific type of usability-related information systems security failure identified. Having development staff to participate in a similar study is a future research opportunity, primarily because contract staff members are the staff members who most often resolve the reported usability failures through the development process.

7.4 Implications

This section presents the implication that this research study has for research and industry.

7.4.1 *Implications for Research*

Through a unique lens, this research developed a method to identify and understand the nature and types of usability-related information systems security failures within an HIS. The discovery of the source of usability failures provides an opportunity to reduce usability-related information systems security failures. A modest amount of research has evaluated the effects a usability failure has on information systems security, but none analyzes the alignment of healthcare task and technology failures while seeking methods to reduce the failures.

The nature of usability security is to use technical security controls primarily through the user interface to protect information resources. Focusing only on technical security controls assures potential information security risk, when researchers argue non-technical security controls are required to protect an organization’s IS. This research has identified the root causes of usability-related information security failures, while also providing a proven method through secure system development that can reduce usability failures along with improving information security failures in the organization. Researchers have also argued for a need to address security controls through the software development process; however, very little evidence indicates that organizations have successfully adopted that approach.

Lastly, TTF theory has a direct and transparent connection to both usability and the IS Success model (Delone, 2003; Delone & McLean, 1992). The variables of efficiency, effectiveness, and satisfaction have the requisite elements to form a relationship for academic research in the domains of IS security, usability, and healthcare. The relationship can be used to create a diagnostic tool to address breakdowns in processes that affect information security, usability, and healthcare work processes.

7.4.2 *Implications for Industry*

The implications of this research for industry serve the usability, security, and healthcare communities respectively. Within the usability community, practitioners are often charged with explaining usability problems to include understanding what the problem involves, and how the problem can be fixed. This also holds true for the security community. This research provides a proven process that explains who, what, when, how, and why a usability-related information systems security occurred in the organization and the ramifications of said failure. Within the healthcare community, this research provides a novel way of identifying the misalignment of a healthcare task with the technology used to mitigate information risk particularly when users of the HIS begin to use workarounds when usability failures occur.

7.4.3 *Future Research*

This research used grounded theory techniques based on anecdotal terms used by the healthcare organizations to report usability failures, along with terms that defined the CIA triad and TTF theory. This method allowed the identification of the nature and types of usability-related information systems security failures that occur in a large healthcare organization. The identification of the aforementioned failures has led to future research opportunities.

One research opportunity is to extend this study by analyzing the usability related information system security failures after the development staff adds their intervention to resolve the failure. Evaluating the intervention provided by the development staff will allow this current research study to be extended by accurately diagnosing and recalibrating usability failure interventions to reduce usability-related information system security failures in the healthcare setting. Integrating such a resolution provides an opportunity to involve all parties to create solutions to usability failures, improve healthcare work processes, and apply security controls in the areas where vulnerabilities are discovered. Moreover, this approach provides an opportunity to bridge the desired link identified in literature between the healthcare, information security, and usability research communities respectively.

A second research opportunity is to combine the TTF theory with IS Success (Delone, 2003; Delone & McLean, 1992) to evaluate an organization's security program. Applying the independent construct of IQ from the IS Success model with the TTF theory allows a focus on the individual user, the task, and technology to determine the information risk that exists within an organization. An alternative research opportunity is to use the current research model (fit focus) in this study, or apply the Technology-to-Performance Chain (TPC) research model (Goodhue & Thompson, 1995, p. 216) in figure 9 comprised of the TTF theory to generalize the current study by applying quantitative methods to analyze usability-related information security failures in non-healthcare settings. By applying the individual characteristic construct (TPC model) to analyze usability-related information systems security failures focuses on usability failures that did not require an intervention by development staff. Therefore casting a wider net to capture, identify, and understand the nature and types of usability failures along with the impact created within an organization.

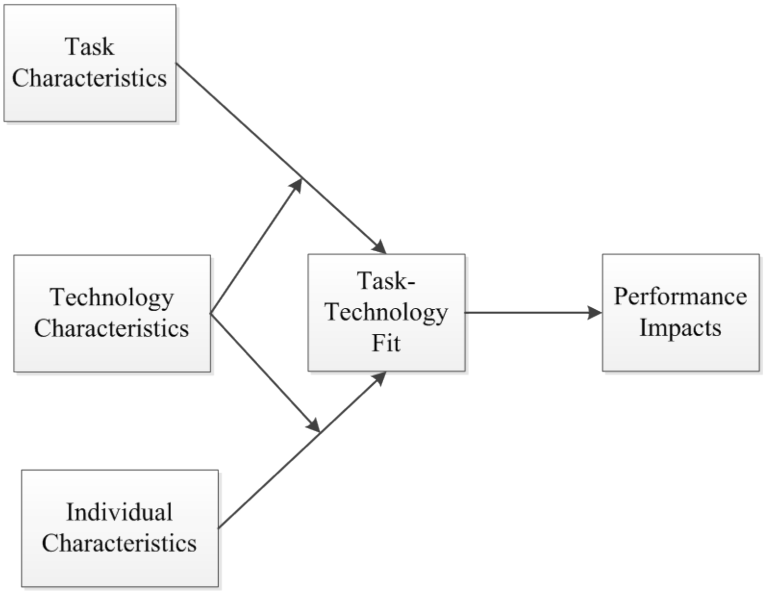


Figure 9. Technology-to-Performance Chain Model

7.5 Summary

This research study examined identified usability-related information systems security failures within a healthcare organization. The identified failures were then categorized based on task-related and technology-related usability failures. The taxonomy of usability failures provided the foundation to determine how to mitigate the actions of users based on the root cause of the problem. The aim of this research was to identify and enhance the understanding of usability-related security failures and how the failures impact IS security performance in a healthcare organization. Through a qualitative positivist case study, the goals of this research study were obtained.

Appendix A

Task-technology Fit Dimensions and Final 8 Factors

Table 7

Results of Factor Analysis : 16 Original Task-Technology Fit Dimensions and 8 Final Task-Technology Fit Factors

8 Final TTF Factors	16 Original TTF Dimensions (After poor questions dropped)	Cronbach's Alpha
Quality	Currency of the data Right data is maintained Right level of detail	0.84
Locatability	Locatability Meaning of data is easy to find out	0.75
Authorization	Authorization for access to data	0.6
Compatibility	Data compatibility	0.7
Ease of Use/Training	Ease of Use Training	0.74
Production Timeliness	Production Timeliness	0.69
Systems Reliability	Systems Reliability	0.71
Relationship with Users	IS understanding of business IS interest and dedication Responsiveness Delivering agreed-upon solutions Technical and business planning assistance	0.88

Appendix B

Phase One Data Collection Search Terms

Table 8

Phase 1 Data Collection Keyword Search Terms

Search Phase	Key Word Search Terms			
Anecdotal Search Phase One	Access Denied	Connections	Denied	Disconnect
	Failures	Interfaces	Interactions	Kajee
	Login	Permissions	Unable to Access	Usability
	User errors	User Preferences	Verify	Vista Link
Axial Coding Search Phase Two	Access Violations	Bypass	Context	Continuous Connections
	Display	Dropped Connection	Locked Record	Security
	User Complaints			
TTF (Task Characteristic) Search Phase Three	Authorized Access	Bad Data	Changed Data	Data
	Data Compatibility	Data Quality	Ease of Use	Hard to Use
	Locate Data	Misplaced Data	Missing Data	Quality
	System Compatibility	System Conflict	System Crash	System Down
	System Failure	Training		
TTF (Technology Characteristic) Search Phase Three	Delays	Flexible	IS Relationships	No Response
	Operations	Production	Production Lag	Production Slow
	Production Timeliness	Scheduled Operations	System Reliability	Unavailable
	Unreliable			

Appendix C

Usability Failure Semi-structured Interview Questions

Table 9

Interview Questions with Mapping to Research Measures

Research Questions	Factors/Focus	Interview Questions
Research Question Two	IS Security/Usability	Describe your thoughts and reaction once the failure occurred while using the system?
Research Question Two	IS Security/Usability	Did the task or process design factor into the application or system failure?
Research Question Two	IS Security/Usability	What steps or alternative methods did you take to complete your task?
Hypothesis One	Healthcare Task Characteristics	Were you able to complete the task? If not, how did the failure affect your ability to accomplish the task?
Hypothesis Two	Security Technology Characteristics	Were you able to complete the task? If not, how did the failure affect your ability to accomplish the task?
Hypothesis Three	HIS Security Performance Impact	Were you able to complete the task? If not, how did the failure affect your ability to accomplish the task?
Hypothesis One	Healthcare Task Characteristics	How do the alternative steps align with the original task design?
Hypothesis Two	Security Technology Characteristics	Is the application or system readily available for use? (If not, please explain.)
Hypothesis Two	Security Technology Characteristics	Does the application or system provide you accurate and current information? (If not, please explain.)
Hypothesis Two	Security Technology Characteristics	Describe the security steps that are associated with the application/system used to complete the task.

Research Questions	Factors/Focus	Interview Questions
Hypothesis Three	HIS Security Performance Impact	What recommendations do you have that could resolve the failure you encountered?
Hypothesis Three	HIS Security Performance Impact	How did the failure impact task accomplishment?
Hypothesis Three	TTF Theory	Describe your experience level with the application or system.

Appendix D

Task Characteristic Usability Failure Sub Code List

Access denied
Access violation error
Application error
Application failed
Application not responding
Application responding slowly
Application timeout
Application training request
Applications allows user to circumvent task
Confusing information display
Error generating report
Inaccurate information display
Inconsistent information display
Incorrect data display
Incorrect data returned
Information is not displaying as expected
Information missing from display
Information missing from report
Information not received
New Feature Request

Personal identified information display
Receiving confusing information
Remote connection unavailable
Report display data errors
Report generates application errors
Report generating incorrect information
Report generation failure
Sensitive information displaying
Software forced logoff
Software modification request
Solicited information not returned
System timeout issue
Unable to access system
Unable to add information
Unable to complete task
Unable to create report
Unable to display image
Unable to enter information
Unable to execute task
Unable to generate report

Unable to import information
Unable to interpret information
Unable to locate information
Unable to log into the system
Unable to print information
Unable to remove information
Unable to retrieve information
Unable to retrieve information
Unable to terminate user connection
Unable to update record
Unable to verify information
Unsolicited information display
Unsolicited information transmitted
Unsolicited removal of information
User access violation
User training issue
User unable to complete task
Wrong data update
Wrong information released
Wrong information returned

Appendix E

Technology Characteristic Usability Failure Sub Code List

Access Violation

Application connection failure

Application Failure

Application timeout

Application transmitted wrong data

Bad data display

Confusing data display

Corrupt report returned

Data display request

Data entry limitation

Data inconsistencies

Data mismatch

Data not received

Data not updating

Data transmission problem

Data unavailable

Data validation error

Database full error

System failure

Distorted image display

Duplicate data display

Inaccurate data during import

Incorrect data stored in database

Incorrect data used in application

Invalid data display

Missing data

Network connectivity problem

Record lock during access

Record locked

Slow system response

Software Bug

Software error

Software modification request

System authentication failure

System create duplicate transmissions

System not responding

System not transmitting

System responding slowly

System unavailable

Unable to access system

Unable to display data

Unable to display image

Unable to generate report

Unable to receive data

Unable to store data

Unable to transfer data

Unable to transmit data

Unable to update database

Unable to upload data

Unsolicited data display

Unsolicited data merge

Appendix F

Theme Emergence Interview Comments from Respondents

Table 10

Theme Emergence Table

Pattern Codes	Participant's Words	Theme Emergence
User Security Actions	"I see the potential of placing information in the wrong record"; "We cannot always trust our data"; "The host file is sent via secure FTP connection"	Information Security Threat
User Security Actions	"I am aware of privacy and security implications when transmitting patient information"; "Security measures are in place" "If patient information is written down on paper, once the use is completed, the paper is shredded."	Information Security Threat
Support System Breakdowns	"There is not much troubleshooting that can be done"; "some of these problem occurs because it is a web-based program"	Organizational Security Performance Impact
Organizational Culture Change	"I have a problem that users don't report problems to me, because they feel nothing will be done about it."	Organizational Security Performance Impact
User Behavior	"None of this would be a problem if billers and coders would do what they are supposed to do"	Usability Assessment
Task Assessment	"I ran through the problem in our test account"; "The initial troubleshoot I done, I asked HR to look at the old system, and was it displayed correctly"	Usability Assessment
Task Assessment	"There was nothing wrong with the ordering process, it was not a user error"; "I thought I had done something wrong because I was new"	Usability Assessment
Technology Assessment	"I had to look at the code, and figure out how to get this fixed"; "There is something wrong here, because if things were working right, I would not get this information"	Usability Assessment

Appendix G

Case Study Interview Record

Table 11

Interview Record for Case Study

Date	Respondent Key	Start Time	End Time	Total Time	Special Notes
11/20/2013	TSKC1R1	3:30	4:36	66	
11/26/2013	TSKC1R2	12:30	2:04	94	Interactive Interview
11/14/2013	TSKC2R1	10:30	11:29	59	
11/15/2013	TSKC2R2	9:30	10:31	61	
12/11/2013	TSKC3R1	1:00	1:53	53	
11/27/2013	TSKC3R2	1:00	2:30	90	Respondent discussed tskc3, techc3, and techc5
11/21/2013	TSKC4R2	2:00	3:15	75	Respondent discussed tskc4, and techc5
11/15/2013	TSKC5R1	1:30	2:44	74	
12/11/2013	TSKC6R1	4:00	5:09	69	
11/29/2013	TSKC7R2	10:00	10:43	43	
11/21/2013	TSKC8R1	11:00	11:47	47	
11/21/2013	TSKC8R2	2:00	3:15	75	
11/13/2013	TSKC9R1	11:30	12:24	54	
11/20/2013	TECHC1R1	9:30	10:32	62	
11/25/2013	TECHC1R2	10:00	11:18	88	
11/27/2013	TECHC2R1	12:00	12:58	58	
11/21/2013	TECHC2R2	12:30	1:19	49	
12/05/2013	TECHC3R1	2:00	2:52	52	
11/27/2013	TECHC3R2	1:00	2:30	90	Interactive Interview
11/15/2013	TECHC4R1	3:00	4:05	65	
12/05/2013	TECHC42R2	4:00	5:45	110	
12/13/2013	TECHC5R1	11:00	12:00	60	
11/27/2013	TECHC5R2	2:00	3:15	75	

Date	Respondent Key	Start Time	End Time	Total Time	Special Notes
11/14/2013	TECHC6R1	2:00	2:57	57	
	Total Interview Minutes			1,626	
	Total Number of Interviews			24	

Note. An interactive interview consisted of an reenactment of the reported usability failure

References

Akers, D., Jeffries, R., Simpson, M., & Winograd, T. (2012). Backtracking events as indicators of usability problems in creation-oriented applications. *ACM Transactions on Computer-Human Interaction (tochi), 19*(2), 16-40.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28,* 476-490.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Al-Ghatani, S. S., & King, M. (1999). Attitudes, satisfaction and usage: Factors contributing to each in the acceptance of information technology. *Behaviour & Information Technology, 18,* 277-297.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42,* 56-65.

Alter, S., & Sherer, S. (2004). A general, but readily adaptable model of information system risk. *Communications of the AIS, 14*(1), 1-28.

Ammenwerth, E., Iller., C., & Mahler, C. (2006). IT-adoption and the interaction of task, technology and individuals: a fit framework and a case study. *Biomedcentral Medical Informatics Decision Making, 6*(3). doi:10.1186/1472-6947.

Anderson, J. (1972). *Computer security technology planning study*. Deputy for Command and Management Systems, United States Air Force, Fort Washington, PA.

Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

August, T., & Tunca, T. I. (2006). Network security and user incentives. *Management Science, 52*(11), 1703-1720.

Austin, C. J., & Boxerman, S. B. (2003). *Information systems for healthcare management* (6th ed.). Association of university programs in health administration.

Avison, D. E., & Fitzgerald, G. (1995). *Information systems development: Methods, techniques, and tools*. London: McGraw-Hill.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems, 5,* 2-9.

Ballou, D., Wang, Pazer, H., & Kumar, G. (1998). Modeling informational manufacturing systems to determine information product quality. *Management Science, 44*(4), 462-484.

Bardram, J. E. (2005). Applications of context-aware computing in hospital work: examples and design principles. In *Proceedings of the 2004 ACM Symposium on Applied Computing* (pp. 1574-1579). New York: ACM.

Barkhuus, L., & Dey, A. K. (2003). Is context-aware computing taking control away from the user? Three levels of interactivity examined. In *Proceedings of UbiComp 2003* (pp. 149-156).

Baskerville, R. (1988). *Designing information systems security.* Chichester: J. Wiley.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375-414.

Beaudoin, L.E., & Edgar, L. (2003). Hassles: Their importance to nurses' quality of work life. *Nursing Economics*, 21(3), 106-113.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to Information Technology: A copy Model of User Adaptation. *MIS Quarterly, 29*(3), 493-524.

Benbasat, I., Dexter, A. S., & Todd, P. (1986). An experimental program investigating color-enhanced and graphical information presentation: An integration of the findings. *Communications of the ACM, 29*(11), 1094-1105.

Bennett, S. P., & Kailay, M. P. (1992). An application of qualitative risk analysis to computer security for the commercial sector. In *Computer Security Applications Conference* (pp. 64-73).

Bevan, N. (2005). International standards for HCI. In C. Ghaoui (ed.) *Encyclopedia of Human Computer Interaction*. Idea Group Publishing.

Bevan, N., Kirakowski, J., & Maissel, J. (1991). What is usability? In *Proceedings of the 4th International Conference on HCI:* Vol. 1. Stuttgart, Germany: Amsterdam: Elsevier.

Bhattacherjee, A., & Hikmet, N. (2007). Physicians' resistance toward healthcare information technologies: A dual-factor model. In *Proceedings of the 40th Hawaii International Conference on System Sciences* (pp. 1-10).

Blandford, A., Thimbleby, H., & Bryan-Kinn, N. (2003). Understanding Interaction Traps. In *Proceedings of HCI 2003* (Vol. 2, pp. 57-60).

Blythe, S. E. (2008). Croatia's computer laws: Promotion of growth in e-commerce via greater cyber security. *European Journal of Law and Economics*, *26*, 75-103.

Bonoma, T. V. (1985). Case-research in marketing: Problems and opportunities and a process. *Journal of Marketing Research, XXII*, 199-208.

Borek, A., Parlikad, A. K., Woodall, P., & Tomasella, M. (2014). A risk-based model for quantifying the impact of information quality. *Computers in Industry, 65*, 354-366.

Boswell, A. (1995). Specification and validation of a security policy model. *IEEE Transaction on Software Engineering, 21*(2), 63-68.

Bourimi, M., Barth, T., Kesdogan., Abou-Tair., D., Hermann., F., & Thiel, S. (2012). Using distributed user interfaces in collaborative, secure, and privacy-preserving software environments. *International Journal of Human Computer Interaction*, *28*, 748-754.

Braz, C., & Robert, J. M. (2006). Security and usability: The case of the user authentication methods. In *Proceedings of the 18th International Conference of the Association Francophone interaction Homme-Machine* New York: ACM.

Brostoff, A. (2004). *Improving password system effectiveness* (Doctoral dissertation, University of London). *Dissertation Abstracts*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Mis Quarterly, 34*(3), 523-548.

Card, S. K., Moran, T. P., & Newell, A. (1983). *The psychology of human-computer interaction*. Erlbaum.

Charmaz, K., (2001). Grounded theory. In R.M. Emerson (ed.), *Contemporary field research: Perspectives and formulations* (2nd ed.) (pp. 335-352). Prospect Heights, Il: Waveland Press

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: SAGE Publications.

Cockton, G. (2008). Revisiting usability's three key principles. In *CHI 2008 Proceedings alt.chi* (pp. 2473-2484). Florence, Italy.

Cranor, L., & Garfinkel, S. (2005). *Security and usability*: *Designing secure systems that people can use*. Sebastopol, CA: O'Reilly Media, Inc.

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.). Boston: Pearson

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Delone, W. H. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of Management Information Systems,19*(4), 9-30.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60-95.

Denning, D. (1987). An intrusion-detection model. *IEEE Trans. Softw. Eng*. 13(1), 222-226.

Denning, P. J. (1992). Passwords. *American Scientist, 80*, 117-120.

Dennison, R. D. (2005). Creating an organizational culture for medication safety. *Nursing Clinics of North America, 40*(1), 1-23.

Devaraj, S., & Kohli, R. (2000). Information technology payoff in the health-care industry: A longitudinal study. *Journal of Management Information Systems, 16*(4), 41-67.

Dey, A. K., & Newberger, A. (2009). Support for context-aware intelligibility and control. In *CHI 2009 - Programming Tools and Architecture* (pp. 859-868). Boston.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20*, 165-172.

Dhillon, G. (2007). *Principles of information systems security: Texts and cases*. New York: John Wiley and Sons.

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, *16*(1), 65-74.

Dhillon, G. & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research. *Information Systems Journal, 11*, 127-153.

Dhillon, G., Tejay, G., & Hong, W. (2007). Identifying governance dimensions to evaluation information systems security in organizations. Paper presented to the *Proceedings of the 40th Annual Hawaii International Conference on System Sciences.* IEEE, 157b.

Dickson, G. W., DeSantics, G., & McBride, D. J. (1986). Understanding the effectiveness of computer graphics for decision support: A cumulative experimental approach. *Communications of the ACM, 29*(1), 40-47.

Dunkerley, K., & Tejay, G. (2009). Developing an information systems security success model for eGovernment context. In *America's Conference on Information Systems (AMCIS)* (pp. 1-8). San Francisco.

Eckman, B. A., Bennett, C. A., Kaufman, J. H., & Tenner, J. W. (2007). Varieties of interoperability in the transformation of the health-care information infrastructure. *IBM Systems Journal, 46*(1), 19-41.

Ellis, T., & Levy, Y. (2006). A systems approach to conduct an effective literature review in support of information systems researchers. *Informing Science Journal, 9*, 181-212.

Eminagaoglu, M., Ucar, E., & Eren, S. (2009). The positive outcomes of information security awareness training in companies: A case study. *Information Security Tech Report*, *14*(1), 223-229.

Fernandez, A., Insfran, E., & Abrahao, S. (2011). Usability evaluation methods for web: A systematic mapping study. *Information and Software Technology, 53*, 789-817.

Flechais, I., Mascolo, C., & Sase, M. A. (2007). Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics, 1*(1), 12-26.

Frincke, D. (2000). Balancing cooperation and risk in intrusion detection. *ACM Transactions on Information and System Security (tissec), 3*(1), 1-29.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*, 16-30.

Glaser, B. G. (1978). *Theoretical sensitivity*. Mill Valley, CA: The Sociology Press.

Goodhue, D. L. (1988). IS attitudes: Toward theoretical and definition clarity. *Database*, *19*(3-4), 6-15.

Goodhue, D. L. (1995). Understanding user evaluation of information systems. *Management Science, 41*(12), 1827-1844.

Goodhue, D. L. (1998). Development and measurement validity of a task-technology fit instrument for user evaluations of information systems. *Decision Science*, *29*(1), 105-138.

Goodhue, D., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, *19*(2), 213-235.

Gould, J. D., & Lewis, C. (1985). Designing for usability: key principles and what designers think. *Communications of the ACM, 28*(3), 300-311.

Guarro, S. B. (1987). Principles and procedure of the LRAM approach to information systems risk analysis and management. *Computers & Security, 6*, 493-504.

Halbesleben, J. R. B., Wakefield, D. S., & Wakefield, B. J. (2008). Work-arounds in health care settings: Literature review and research agenda. *Health Care Management, 33*(1), 2-12.

Hammond, R. (1988). Improving productivity through risk management. In R. F. Umbaugh (ed). *Handbook of MIS Management* (pp. 655-665). Boston: Auerbach.

Harkee, V. Alessi, D. & Collan, M. (2003). IT and institutional constraints: Effects of legal and administrative constraints use IT in production of health care services. In R. H. Sprague Jr. (ed.). *Proceedings of the Thirty-Sixth Annual Hawaii International Conference on System Sciences* (pp.1-6). Los Alamitos. CA.

Hartson, H.R., Andre T., & Williges, R. C. (2001). Criteria for evaluating usability evaluation methods. *International Journal of Human Computer Interaction, 13*(4), 373-410.

Hendry, M. (1997). *Smart card security and applications*. Norwood, MA: Artech House.

Hilbert, D. M., & Redmiles, D. F. (2000). Extracting usability information from user interface events. *ACM Computer Surveys, 32*(4), 384-421.

Huang, J., Ding, Y., Hu, Z., 2008. Knowledge based model for holistic information security risk analysis. In *International Symposium on Computer Science and Computational Technology* (pp. 88-91). IEEE. Shanghai.

Hubbard, W. (2002). *Methods and techniques of implementing a security awareness program*. SANS Institute [White paper].

Iivari, J., & Hirchheim, R. (1996). Analyzing information systems development: a comparison and analysis of eight IS development approaches. *Information Systems,* 21 (7), 551–575.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer & Security, 31*, 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management, 51*, 69-79.

Institute of Medicine. (1999). *To err is human: Building a safer health system*. Washington, D.C. National Academy Press.

ISF. (2003). *The standard of good practice for information security*. Information Security Forum.

ISO 9241-11. (1998) Ergonomic requirements for office work with visual display terminals (VDTs) Part 11: *Guidance on usability*.

Jacobson, I., Booch, G., & Rumbaugh, R. (1999). *The unified software development process*. Addison Wesley, Reading.

John, B. E., Prevas, K., Salvucci, D. D., & Koedinger, K. (2004). Predictive human performance modeling made easy. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 455–462.

Johnson, C. M., Johnson, T. R., & Zhang, J. (2005). A user-centered framework for redesigning health care interfaces. *Journal of Biomedical Informatics, 38,* 75-87.

Johnson, M. E., & Willey, N. D. (2011). Usability failures and healthcare data hemorrhages. *Security & Privacy, IEEE, 9*(2), 35-42.

Johnson, M. E., & Pfleeger, S. L. (2011). Addressing Information Risk in Turbulent Times. *IEEE Security & Privacy*, *9*(1), 0049-57.

Juristo, N., Moreno, A. M., & Sanchez-Segura, M. I. (2007). Analysing the importance of usability on software design. *The Journal of Systems and Software, 80*, 1506-1516.

Ka-Ping, Y. (2002). User interaction design for secure systems. In *Information and Communications Security* (Vol. 2513, pp. 278-290).

Klein, H., & Hirschheim, R. (1987). Social change and the future of information systems development. In *Critical Issues in Information Systems Research* (pp. 275-308). Chichester, England: Wiley.

Knapp, K. J., & Marshall, T. E. (2006). Information security: management's effect on culture and policy. *Information Management & & Computer Security, 14*(1), 24-36.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*, 289-296.

Lategan, N., & Solms, R., (2006). Towards enterprise information risk management a body analogy. *Computer Fraud & Security* (12), 15–19.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization Science, 2*, 342-365.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research, 14*(3), 221-243.

Levina, N. (2005). Collaborating on multiparty information systems development projects: A collective reflection-in-action view. *Information Systems Research*, *16*(2), 109-130.

Liebenau, J., & Backhouse, J. (1990). *Understanding information: An introduction*. London: Macmillan.

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

Luftman, J., & Brier, T. (1999). Achieving and Sustaining Business-IT Alignment. *California management review*, *42*(1).

Marcus, A. (2002). Dare we define user-interface design? *Interactions*, *9*(5), 19-26.

Markus, M. L. (1983). Power, politics, and MIS implementation. In *Communications of the ACM* (Vol. 26, pp. 430-444).

Mastrangelo, P., Everton, W., & Jolton, J. (2006). Personal use of work computers: Distraction versus destruction. *CyberPsychology & Behavior, 9*(6), 730−741.

Maycut, P., & Morehouse, R. (1994). *Beginning qualitative research: A philosophic and practical guide*. London Falmer Press.

Mclean, J. (1990). The specification of modelling of computer security. *IEEE Computer, 23*(1), 9-16.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook* (2nd ed.). Thousand Oaks, CA: Sage.

Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Quality data analysis* (3rd ed.) [A Methods Sourcebook]. Thousand Oaks, CA: SAGE.

Newton, J. D., & Snyder, C. A. (1987). Risk analysis for computerized information systems. In *Proceedings, Southern Management Association* (pp. 306-308).

Niekerk, L., Labuschagne, L., 2006. The PECULIUM model: information security risk management for the south African SMME. In *Proceedings of the ISSA from Insight to Foresight Conference,* 5–7th July 2006, Sandton, South Africa.

Nielsen, J. (1993). *Usability engineering*. Academic Press.

Nielsen, J. & Molich, R. (1990). Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 249–256.

Orgun, B., & Vu, J. (2006). HL7 ontology and mobile agents for interoperability in heterogeneous medical information systems. *Computers in Biology and Medicine, 36*, 817-836.

Pare, G. (2004). Investigating Information Systems with positivist case study research. *Communications of the Association for Information Systems, 13,* 233-264.

Payne, B. D., & Edwards, W. K. (2008). A brief introduction to usable security. *Internet Computing, 12*(3), 13-21.

Peterson., R. (2004). Crafting information technology governance. *Information Systems Management, 21*(4), 7-22.

Post, G. V., & Diltz, J. D. (1986). A stochastic dominance approach to risk analysis of computer systems. *MIS Quarterly, 10*(4), 363-375.

Post, G. V., & Kagan, A. (2006). Information security tradeoffs: The user perspective. *Information Security and Risk Management, 15*(5), 22-29.

Price, R., & Shanks, G. (2005). A semiotic information quality framework: development and comparative analysis. *Journal of Information Technology, 20*(2), 88-102.

Rainer, R.K., Snyder, C.A., & Carr, H.H. (1991). Risk analysis for information technology. *Journal of Management Information Systems, 8*(1), 129-147.

Rasmussen., J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science, 27*(2), 183-213.

Rivest, R. L. (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Rubin, J., Chisnell, D., & Spool, J. (2008). *Handbook of usability testing: How to plan, design, and conduct effective tests (*2nd ed.). New York: John Wiley & Sons Inc.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics, 9*, 107-118.

Saldana, J. (2012). *The Coding Manual for Qualitative Researchers* (2nd ed.). Thousands Oak, CA: SAGE. (Original work published 2009)

Salkind, N. J. (2006). *Exploring research* (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Sambamurthy, V., & Zmud, R. W. (2000). Research commentary: The organizing logic for an enterprise's IT activities in the digital era—A prognosis of practice and a call for research. *Information systems research*, *11*(2), 105-114.

Sandhu, R. S. (1993). Lattice-based access controls. *IEEE Computer, 26*(11), 9-19.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computing, 29*(2), 38-47.

Sandhu, R. S., & Samarati, P. (1996). Authentication, access control, and audit. *ACM Computing Surveys, 28*(1).

Sarker S., & Lee, A. S. (2003). Using case study to test the role of three key social enablers in ERP implementation. *Information & Management, 40*, 813-829.

Schecter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *IEEE Symposium on Security and Privacy* (pp. 51-65). Berkeley, CA.

Schneier, B. (1996). *Applied cryptography* (2nd ed.). NY: Wiley.

Selig, G. J. (2008). *Implementing IT governance: A practical guide to global best practices in IT management.* Norwich, UK: Van Haren.

Sheng, S., Broderick, L., Koranda, C. A., & Hyland, J. J. (2006). Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software [Abstract]. *Soups 2006 Poster,* 1-2.

Shimeall, T. J., & McDermott, J. J. (1999). Software security in an Internet world: an executive summary. *Software, IEEE, 16*(4), 58-61.

Shneiderman, B. (1987). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Reading, MA: Addison-Wesley.

Shneiderman, B., Jacobs, S., Cohen, M., Plaisant, C., &. (2009). *Designing the user interface: Strategies for effective human-computer interaction* (5th ed.). Menlo Park, CA: Addison Wesley.

Siponen, M.T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal, 14*(4), 15-23.

Siponen, M. (2002). Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. *Information Management & Computer Security*, *10*(5), 210-224

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97-100.

Siponen, M., & Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information systems, 7*(7).

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270.

Skov, M. B., & Stage, J. (2005, November). Supporting problem identification in usability evaluations. In *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future* (pp. 1-9). Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

Spears, J., 2006. A holistic risk analysis method for identifying information security risks: Security management, integrity, and internal control in information systems. *International Federation for Information Processing* (Vol. 193, pp. 185-202).

Stanton, J. M. (2002). Company profile of the frequent internet user. *Communications of the ACM*, *45*(1), 55-59.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *Mis Quarterly,* 441-469.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. London: Sage.

Suh, B., and Han, I. (2003). The IS risk analysis based on a business model. *Information & Management* (41:2), pp. 149-158

Sun, L., Srivastava, R.P., & Mock, T.J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems, 22*(4), 109-142.

Tejay, G., Dhillon, G., & Chin, A.G. (2005). Data quality dimensions for information systems security: A theoretical exposition. In P. Dowland, S. Furnell, B. Thuraisingham, & X. S. Wang (Eds.), *Security Management, Integrity, and Internal Control in Information Systems* (pp. 21-39). New York: Springer.

Toussaint, P. Bakker. A., & Groenewegen, L. (1992). Integration of information systems: Assessing its quality. *Computer Methods and Programs in Biomedicine, 64*(I) 9-35.

Van Grembergen, W., & DeHaes, S. (2007). *Implementing information technology governance: Models, practices and cases*. IGI Publishing.

Vega, D.E., Schieferdecker, I., & Din, G. (2010). Design of a test framework for automated interoperability testing of healthcare information systems. *In*

Proceedings of Second International Conference on eHealth, Telemedicine, and Social Medicine. 134-140.

Vigna, G. & Kemmeerer, R.A. (1999). NetSTAT: A network-based intrusion detection system. *Journal of Computing Security*, 7, 1, 37-71.

Vilbergsdottir, S. G., Hvannberg, E. T., & Law, E. L. C. (2014). Assessing the reliability, validity and acceptance of a classification scheme of usability problems (CUP). *Journal of Systems and Software*, *87*, 18-37.

Von Solms, B. (2005). Information security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99-104.

Von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376

Von Solms, R., & von Solms, S. H. (2006). Information security governance: A model based on the direct–control cycle. *Computers & Security*, *25*(6), 408-412.

Voss, B.D. (2001). *The ultimate defense of depth: Security awareness in your company*. SANS Institute [White paper].

Wang, R. Y., Storey, V. C., & Firth, C. P. (1995). A framework for analysis of data quality research. *Knowledge and Data Engineering, IEEE Transactions on*, *7*(4), 623-640.

Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, *12*(4), 5-34.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101-105.

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, *20*, 35-44.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Wharton, C., Bradford, J., Jeffries, R., & Franzke, M. (1992). Applying cognitive walkthroughs to more complex user interfaces: Experiences, issues, and recommendations. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 381–388.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*, 43-57.

Whitman, M.E., & Mattord, H.J. (2012). Principles of information security. (4th ed). Boston: Cengage.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium* (pp. 169-183).

Winograd, T., & Flores, F. (1986). *Understanding computers and cognition: A new foundation for design*. Norwood, NY: Ablex.

Wixon, D. (2003). Evaluating usability methods: why the current literature fails the practitioner. *Interactions*, *10*(4), 28-34.

Woodall, P., Borek, A., & Parlikad, A. K. (2013). Data quality assessment: The hybrid approach. *Information & Management*, *50*(7), 369-382.

Woody, C. (2006). *Applying OCTAVE: Practitioners report.* Carnegie Mellon University.

Worthley, J.A. (2000). *Managing information in healthcare: Concepts and cases*. Chicago, IL. Health Administration Press.

Yang, Z., Ng., Kankanhalli, A., & Yip, J. W. L. (2012). Workarounds in the use of IS in healthcare: A case study of an electronic medication administration system. *International Journal Human-Computer Studies, 70*, 43-65.

Yee, K. P. (2004). Aligning security and usability. *Security & Privacy, IEEE, 2*(5), 48-55.

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed., Vol. 5). Los Angeles, CA: SAGE.

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & Security, 26*, 256-265.

Zhang, P., Benbasat, I.,Carey, J.,Davis, F.,Galletta, D., & Strong, D. (2002). Human Computer Interaction Research in the MIS Discipline. *Communications of the AIS*, 9(20), 334-355.

Zigurs, I., & Buckland, B. K. (1998). A theory of task/technology fit and group support systems effectiveness. *MIS Quarterly, 22*(3), 313-334.

Zviran, M., & Haga, W. J. (1993). A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal, 36*(3), 227-237.