2020

Cyber Security in Mental Health: An Assessment of Current Practice and Behavioral Intent

Richard Hamilton Stotts

CYBER SECURITY IN MENTAL HEALTH:

AN ASSESSMENT OF CURRENT PRACTICE AND BEHAVIORAL INTENT

A DISSERTATION

Presented to the Faculty of the Graduate School of

St. Mary's University in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

in

Marriage and Family Therapy

by

Richard H. Stotts

San Antonio, Texas

April 26, 2020

CYBER SECURITY IN MENTAL HEALTH:

AN ASSESSMENT OF CURRENT PRACTICES AND BEHAVIORAL INTENT

APPROVED:

_____
Dan Ratliff, Ph.D.
Dissertation Advisor

_____
Jason Northrup, Ph.D.

_____
Moonyeen O'Phelan, Ph.D.

APPROVED:

_____
Leona Pallansch, Ph.D.
Dean, College of Arts, Humanities and Social Sciences

_____
Date

Abstract

Mental health practitioners rely on digital systems to interact with and in some instances treat patients (Hydari, Telang, & Marella, 2015; Recupero, & Rainey, 2005). Yet, while widespread use of digital devices provides significant practical advantages, that same use exacerbates the possibility of a cyber breach (Guterman, 1999). This research describes mental health practitioners' current cyber security practices and the factors influencing their behavioral intentions to implement cyber security within clinical mental health settings. Factors assessed included knowledge, self-efficacy, norms, threat awareness and penalties. Mental health practitioners (n = 210) from across the United States formed the sample population, received a Qualtrics on-line survey link through their affiliated professional organizations, and responded with the completed survey. Data was analyzed using structural equation modeling and SmartPLS. Results indicated although practitioners profess knowledge of legal and ethical requirements, actual behaviors do not reflect those assertions. Practitioners claimed knowledge of federal law (76.7%); knowledge of state law (70.5%); and knowledge of ethical guidelines (90.5%), yet only 32.4% of practitioners have conducted a risk assessment within the last year and more than 50% do not know how to conduct an assessment. Additionally, more than 20% of our colleagues believe professional liability insurance alone will prevent financial losses from a breach. Finally, 66% of our colleagues believe the cyber security threat is exaggerated. These findings suggest practitioner understanding of the requirements for addressing privacy and confidentiality risks in the use of digital systems fall short of desired standards.

Acknowledgements

In conducting this research, I have been blessed to have the mentoring and guidance of my committee, Dr. Dan Ratliff, Dr. Jason Northrup, and Dr. Moonyeen O'Phalen. Their encouragement and wisdom provided me with the essential guidance required to complete the project. Dr. Carolyn Tubbs provided significant counsel and gave generously of her time in discussing both process and approaches in working through conceptual areas. Most significantly, I am grateful to my wife, Julia Stotts, whose gentle inspiration continued to guide me from study inception to its conclusion.

Table of Contents

List of Tables

List of Figures

Chapter 1 – Introduction

As in the general population, the use of digital capabilities in clinical practice continues to expand among mental health providers. However, although many clinicians employ digital systems, there is yet little practitioner understanding of the threats and security imperatives that would enable alignment of cyber security decisions with legal mandates and professional codes. In addition, limited research exists on the use of cyber security in private mental health settings. However, Claar (2011) states that research that does exist states that many clinicians do not understand the vulnerabilities inherent in the use of digital systems. As a result, mental health practitioners working in clinical settings exercise few cyber security protections and have limited awareness of the risks they are accepting on behalf of their clients, themselves, and potentially their colleagues. Furthermore, while federal guidelines and professional standards describe ethical and legal requirements to minimize cyber security risk, methods for implementation remain broad with limited details on specific actions required to defend client and clinician data (Kobus, 2015).

In that regard, this study provided descriptive insights into the cyber security knowledge, legal and ethical understanding, and decision processes of mental health practitioners. Establishing those insights provides the therapeutic community with a refined understanding of practitioner compliance with cyber security guidance within clinical settings. Furthermore, survey results examined through various theoretical lenses continue to develop understanding of the factors that influence a therapist's behavioral intent within clinical settings. Notably, theories which emphasize the effects of norms (social learning theory, open systems theory, control theory, social control theory, theory of planned behavior), self-efficacy (expansive learning theory, general deterrence theory, theory of planned behavior), and threat awareness (open

systems theory, risk homeostasis, TRIRISK model) were proven to have significance in determining a clinician's behavioral intent. Finally, analysis of data enabled partial closure of significant gaps in existing cyber security and risk assessment literature, enabled development of initial clinical practice security recommendations for consideration, and may assist therapists in implementing cyber security capabilities aligned to practice priorities, resources, and legal and professional mandates.

This study consists of a thorough literature review of motivational and risk perspectives directed toward establishing an understanding of cyber security awareness for practitioners when using digital systems. Furthermore, the primary researcher created a measurement instrument adapted from previously validated research (Herath & Rao, 2009; Rhee, Kim, & Ryu, 2009; S. Boss, Kirsch, Angermeier, Shingler and R. Boss, 2009; Ajzen, 2002) and modified or developed questions to focus specifically on therapist influence factors aligned to behavioral intent. Analysis of responses from mental health clinicians compared to federal guidelines and professional standards produced insights into both clinician recognition of ethical and legal responsibilities and use of cyber security within a representative population.

Statement of the Problem

Although mental health practitioners increasingly rely on digital systems for medical records, scheduling, collaboration with colleagues, and other business functions, clinicians remain largely unaware of the sophistication of the cyber threat. Ranging from state actors through criminals and novice hackers, the tools and techniques employed by those seeking to breach digital systems increases more rapidly than protective measures. Additionally, many clinicians and associates within a practice anticipate that digital systems are basically secure yet interconnections of devices, wireless connectivity and service providers to include the cloud and

or third-party colleagues introduce substantial vulnerabilities (Tschider, 2017). This misunderstanding of technology creates significant vulnerabilities in any clinical systems configuration. Furthermore, misunderstandings surrounding legal and ethical requirements compounds the risk clinicians accept. As a result, mental health professionals accept far more risk than anticipated and provide hackers with varied avenues to attack vulnerable systems.

With those ideas in mind, many questions surface in respect to why clinicians approach cyber security with only a risk tolerance or perhaps risk acceptance perspective. Four risk mitigation approaches are available to anyone using digital systems: risk acceptance, risk avoidance, risk mitigation, and transferring risk (Howard & Jawahar, 2002). All these measures are in fact important considerations for effective cyber security and solely relying on any one approach increases the likelihood of damage for the clinician, clients, and colleagues if a breach occurs. Consequently, exploration of a clinician's behavioral intent becomes an important area in evaluating the rationale for the choices clinician's make when deciding how to approach cyber security.

Assessing behavioral intent involves understanding the factors that influence a clinician's decisions to implement cyber security within their practice. Factors assessed in this research include knowledge, self-efficacy, norms, threat awareness and penalties and were selected based on previous theoretical studies. Identifying the areas which provide the most compelling reasons for clinician behaviors may lead to approaches to correct gaps in training and educational programs, establishing awareness of risk strategies, and developing enhanced methods to implement the broad legal and ethical requirements that exist today.

Finally, another essential aspect of the cyber security challenge involves penalties for inaction. As cyber threats continue to increase in numbers of attacks and sophistication, the

financial penalties associated with failure to comply with mandated requirements are also increasing. Fines ranging in excess of $100 per record and potentially much more for repeat violations are now viewed as reasonable judgements against noncompliant organizations. Furthermore, the Office of Civil Rights (OCR) that oversees HIPAA regulations for the federal government has imposed penalties of $1.5 million to $5.5 million for firms that displayed significant negligence (Conaty-Buck, 2018). Finally, legal defense fees may also contribute to the costs associated with a cyber breach. In one instance, a small medical laboratory stated it "was forced to wind down operations and stop diagnosing cancer" because of the "crushing burdens imposed upon it by the FTC's investigation and ensuing action" (Selznick & LaMacchia, 2017, p. 248). Results generated in this study provide perspective into the behavioral intent of clinicians as they interpret the risk-reward aspects of cyber security – the costs of taking cyber security action compared with the costs of a sensitive information breach.

Research Question

The questions posed in this research concern the current practices of clinicians and the factors which serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice. Specifically, the research question was, what factors (e.g., knowledge, self-efficacy, threat awareness, norms, and penalties) serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice? Survey questions were developed to test the relationship between the clinician's perspectives on each of the five factors and their intent to employ methods to protect sensitive information and digital systems. Hypotheses centered on the impact of all five factors on the clinician's postulated behaviors or actions. Each hypothesis was structured to relate to not only specific behavior intent (e.g., impact of Knowledge on

Knowledge Behavioral Intent) but also aggregated factors to provide insight into the combined effects of all factors (e.g., Knowledge, Self-efficacy, etc.) against combined behavioral intent.

Rationale for the Study

This study has both practical and descriptive relevance. In a practical sense, mental health therapists must adhere to legal and ethical mandates in protecting client and clinician data and digital systems from compromise. However, the literature suggests that legal and ethical mandates alone have not proven to compel significant motivation toward effective action in areas of cyber security. While significant literature exists on risk and motivational influence in decision making, Bruch and Feinberg (2017) make the case that a lack of focused work to integrate those insights leaves significant space for research directed toward the application of process models that affect real world scenarios. Consequently, adding to the current body of knowledge on mental health standards of practice, motivational influencing factors, and behavioral intent analysis for cyber security decision-making will enhance the profession's ability to gain insights that may advance protections of sensitive information and systems.

Current Practices

Literature investigated, and the on-line survey also provided insight into the current use of digital systems as a standard of practice. Additionally, the literature and the survey also established insight into the cyber security capabilities incorporated in practices and the factors which influence therapist risk decisions as a function of behavioral intent. Specific factors incorporated in this research include knowledge of laws and ethical guidelines, self-efficacy in implementing protective measures, understanding of threat intent and capabilities, the norms for adhering to typical security practices within the mental health community, and the recognition of the impact penalties may have for non-compliance. Selected motivation, influence, risk, and

family theories were used to assess the influencing factors for cyber risk mitigation when aligned to behavioral intent in decision making. Results show that while therapists report they are knowledgeable of the laws and ethical guidelines which mandate specific actions for client confidentiality and privacy, few precautions are taken to address the potential for compromise. Instead, a significant majority of therapists take a risk acceptance attitude in implementing cyber security within their practices. Furthermore, even when conscious decisions to implement cyber security precautions are made, therapists may be largely unaware of security possibilities, sub-optimize their available alternatives, and consequently, do little to mitigate the client's and clinician's cyber security risks (van Schaik, Jeske, Onibokun, Coventry, Jansen, & Kusev, 2017).

Behavioral Intent Research

Significant behavioral intent research emerges from psychology, sociology, business and many other disciplines where explaining human motivation offers an ability to shape behavioral conditions. In fact, understanding the factors that affect decision making may provide guideposts for educational programs, organizational success, and legal and ethical policy formulation. The theory of planned behavior refined from the theory of reasoned action suggests that behavioral intent is associated with attitude, norms, and self-efficacy when aligned with the expectation of desired outcomes (Kidwell & Jewell, 2003). Additionally, these authors further suggest that perceived outcomes are affected by both internal and external factors. Consequently, although several other theoretical constructs (e.g., social control theory, general deterrence theory, etc.) were used in selecting factors for this research model, behavioral intent can be seen as the combined impact of knowledge, self-efficacy, norms, threat awareness, and the perceived likelihood of penalties in producing protective security action. Furthermore, knowledge as a basis for any of the factors considered may form a necessary precursor in every area studied.

Limitations of the study

While this research provides significant insights into the current practices and corollary behavioral intentions of mental health therapists surrounding the implementation of cyber security, it is not intended to be exhaustive and consequently may not reflect all levels of understanding nor all approaches to cyber security within the mental health community. Furthermore, the study does not claim to address all practice types nor large institutional organizations. More broadly, further research may be required to gain additional perspective into the nature and dynamics of cyber security in other mental health settings. Finally, this research does not attempt to assess in-depth knowledge of an individual clinician's cyber threat understanding nor the clinician's specific ability to implement cyber security technologies within a practice. Consequently, other factors may also contribute to a therapist's behavioral decisions.

Another limiting factor concerns the instrument itself. Surveys have been assessed as constituting a potentially problematic sampling design based on both voluntary bias and response bias. Also, a self-selected sample may produce unrepresentative results of the larger professional population as those most familiar with cyber security may feel more willing to complete survey questions. Consequently, surveys may misrepresent the intended research population. Similarly, respondents may answer survey questions to conform with or deviate from anticipated researcher preferences. Providing an anonymous link is used here to provide partial control for potential survey bias yet caution in interpreting findings is warranted. Furthermore, to address response bias, neutral phrasing was incorporated into survey questions.

With those limitations in mind, further quantitative and qualitative research may provide greater detail with which to create specifically designed implementation practices for standardizing cyber security within professional mental health settings. Although inferred vice

causal relationships may produce insights into future research areas, test results should be replicated before accepting variable relationship interpretations or overall model judgement.

Definitions of significant terms

Advanced Persistent Threat (APT): is an attacker (usually nation-state sponsored) who attempts to gain access to a network, remains undetected and removes (exfiltrates) data and/or creates conditions for later network exploitation. (Kissel, 2012)

Black Hat: a hacker who "violates computer security for little reason beyond maliciousness or personal gain. (Gregg, n.d.)

Cracker: a computer user who attempts to break into copyrighted software or network computer systems. (Gregg, n.d.)

Cyber security: technologies, processes and polices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. (Kissel, 2012)

Federal Trade Commission (FTC): Department of Commerce organization created to protect consumers from unfair business practices. FTC has the authority to create cyber security policy, enforce laws and inspect businesses for non-compliance with regulations. (U.S. FTC, 2010)

Grey Hat: a computer hacker or computer security expert who may violate laws or ethical standards but without specific malicious intent. (Gregg, n.d.)

Hacker: one who breaks in to computer systems via communication networks - includes those who debug or fix security problems, and the morally ambiguous. (Gregg, n.d.)

Hacktivist: user of computers to promote a political agenda. (Gregg, n.d.)

Health Information Technology for Economic and Clinical Health Act (HITECH): Title XIII of the American Recovery and Reinvestment Act covering responsibilities for digital protections in healthcare. (Hecker, et.al, 2014)

Health Insurance Portability and Accountability Act (HIPAA): Executive Order 13636 created a requirement to maintain security for the confidentiality, integrity, and availability of client health
care records for covered entities. (U.S. HIPAA, 2015)

PHI: personal health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data collected to identify an individual and determine appropriate care. (Kumar & Wambugu, 2015)

PII: personally identifiable information is information that can be used on its own or with other information to identify, contact, or locate a person. (Kissel, 2012)

Script Kiddie: an unskilled individual who uses scripts or programs developed by others to attack computer systems, networks and/or deface websites. (Gregg, n.d.)

Sweep: scanning computer/digital systems to determine potential weaknesses (Chowdhury & Ferdous, 2017)

System vulnerability: the intersection of three conditions - a susceptible system, an attacker with ability to identify weakness, and with capability/motivation to exploit the flaw. (Vulnerability Computing, 2016.)

System weakness: flaws which allow an attacker to exploit vulnerable systems. (Vulnerability Computing, 2016.)

White Hat: Internet slang for an ethical computer hacker/computer security expert. (Gregg, n.d.)

Chapter 2 - Literature Review

Current literature on cyber security in mental health tends to address telehealth challenges and potential issues vice the motivation of clinicians to implement security measures within their practice. The paragraphs which follow focus on the requirement for clinician knowledge, motivation, and behavioral intent. The section on Cyber Security Considerations provides a brief perspective on the ubiquitous nature of digital systems essential in today's clinical practices and the risk associated with the incomplete understanding of those systems. The following three sections provide more specific detail on the theories which underpin the theoretical model for this research. First, the section on Threat Perspective describes various hacker sub-types as well as the factors which may compel hackers to engage in this type of activity. Notably distinguishing the types of relevant threat to a practice is a significant factor in security preparation. Second, Family Systems Theories provide insights into the requirements for knowledge, threat awareness and enforcement understanding in establishing clinician motivation to establish behavioral intent. Third, and finally, the section on Behavioral Intent specifically addresses the theoretical constructs used in developing the model for this research. The section also details various theoretical approaches used to predict behavioral intent.

Cyber Security Considerations

While legal and ethical guidelines mandate the protection of client confidentiality and privacy for e-records and in the use of digital systems, many therapists remain uninformed of available protections. As a result, while digital capabilities have become essential tools in clinical practice and e-records are rapidly becoming the storehouse of choice for many practices, cyber security approaches to safeguard those systems remain shadowed in technical jargon and arcane processes. Consequently, therapists accept significant risk on behalf of clients, themselves, and

potentially associates by misunderstanding or in some cases opting out of available protections (Aksel, Trung, & Faxvaag, 2005).

Luxton, McCann, Bush, Mishkind, and Reger (2011) describe the ethical constraints associated with the use of smartphone technology in behavioral health. Their assessments of threats to smartphone security include both illegal access and loss of devices which compel active security measures to prevent data loss under those conditions. Furthermore, while HIPAA covers data in transit as described by Hecker and Edwards (2014), other guidelines also provide broad instructions on the ethical treatment of client data. Federal Trade Commission (United States, FTC, 2010) guidelines and the Health Information Technology for Economic and Clinical Health Act (Secretary H. O., HITECH Act, n. d.) along with many professional standards address data privacy and confidentiality for client information. However, implementation guidance, standards, and evens laws are non-specific, leaving practitioners to establish their own moral, ethical and legal safeguards for cyber security.

Yet current federal guidelines and professional standards do describe ethical and legal requirements to minimize cyber security risk (Kobus, 2015), albeit with broad descriptions of requirements vice specifics on implementation standards. The Health Insurance Portability and Accountability Act establishes both security and privacy guidelines for covered entities to include all those who "…work in healthcare facilities or private offices" (Edemekong & Haydel, 2019, p. 10). Requirements identify what obligations covered entities must enact to align privacy and security for protected health information (PHI) with HIPAA guidelines. PHI is defined as any health information which can disclose the client's identity (Kumar, M. & Wambugu, S.; 2017) and includes any data that may reveal health services, treatment, or payment information. Areas such as mandatory electronic and physical requirements are outlined

within the security rule such that practitioners are assigned responsibility for training personnel, encrypting and password protecting information, and conducting security risk audits. While this definition necessarily includes both PCI and PII, mechanisms to implement guidance are not specified.

The health Information Technology for Economic and Clinical Health Act (HIGHTECH Act) provides further insight into business associates as covered entities, notification responsibilities if breached, and penalties associated with failure to comply with federal mandates. Business associates are defined as an organization or person that works with a covered entity but not as a member of the covered entity's organization (45 CFR 160.103). The Act requires the same level of security protections for associates that apply to the health care practice. Additionally, the HIGHTECH Act established rules for notification procedures if a breach occurs. The requirement specifies notification of the individual whose information was compromised, notification of law enforcement, and notification of state and local media for a breach consisting of more than 500 records. Penalties associated with a breach were also increased under HIGHTECH and enforcement authorities clarified (Health Information Technology Provisions of American Recovery and Reinvestment Act of 2009, 2016). Notably, the third circuit court of appeals determined the Federal Trade Commission (FTC) has the authority to enforce cyber security practices to insure alignment with legal mandates (Pardau & Edwards, 2017). However, while the FTC continues to determine cyber security deficiencies based on both deception and unfairness, specific cyber security implementation standards remain to be defined. In that regard, the eleventh circuit court of appeals determined that specific harm must be identified before the unfairness codes may be used to compel penalties (Denny, 2016). Yet in the absence of legally mandated implementation standards, the FTC retains broad

authority to determine if cyber security practices are sufficient to insure client protections (Pardau & Edwards, 2017).

In addition to legal requirements albeit with vague, undetermined implementation standards, Jordan, Russell, Afousi, Chemel, Mcvicker, Robertson and Winek (2013) assert that, "Professional organizations do not provide adequate ethical guidelines for therapeutic practice" (p. 105). Further, Jordan, et al. (2013) state that across all professional mental health organizations, "…none provide officially recognized ethical standards for the use of social (digital) media in therapeutic practice" (p. 106). They also emphasize the need to discuss the potential risks of a data breach or other compromise with clients to ensure they understand the hazards involved with the use of digital media. Consequently, while guidance concerning confidentiality and privacy when using digital systems exists, methods and approaches to comply with those requirements remains at individual practitioner discretion.

Finally, Claar (2011) determined that users of digital systems disregard even basic cyber security. A finding suggesting that even if legal and ethical guidance on implementation standards were developed, clinicians may not have the ability or intent to adopt those standards. Consequently, while specifying at least minimum implementation practices would provide clarity into expected digital privacy and confidentiality actions, actual execution of cyber security may be dependent on additional factors as well.

Very limited research has been conducted on cyber security for smaller clinical practices and virtually no research has been conducted to consider the effects of a clinician's knowledge of cyber security requirements or the factors which influence a therapist's behavioral intent. Bruch and Feinberg (2017) determined that insufficient research has been conducted on risk and motivational models for real world conditions. Consequently, no exploratory studies have

attempted to address the knowledge therapists have of laws and guidelines for digital confidentiality, their use of systems and protections to enhance security, nor the therapist's behavioral influences in addressing the risks associated with digital systems in clinical practice. As a result, this research was designed to provide insight into the factors which serve to reflect a therapist's knowledge of requirements and those that influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice.

Threat Perspective

A key dynamic for practitioners in assessing the use of cyber security in mental health involves the therapist's understanding of the threat. In cyber terms, a threat consists of two equally emphasized areas. First, an adversary must have the capability to inflict harm on a system. Second, the adversary must have the motivation to carry out an attack. Many capabilities to compromise computer systems can be found on-line and many more can be purchased for varying amounts. As a result, since the tools to compromise systems are readily available, motivation for hackers is assigned a significant prominence in reviewing cyber security operations and establishing protective approaches (Vidalis & Jones, 2005).

Motivation spans many impulse layers based on the goals of the hacker: Advanced Persistent Threats (APTs – hackers working for nation states), criminals, crackers, hacktivists, or script kiddies (Leonard, 2013). However, a consistent set of traits describe many of the members of these groups. First, hackers of all varieties tend to be bright, technically adept, and gratified by solving challenges. Second, "crackers" are especially characterized as very skilled, over-qualified, arrogant, and view themselves as "Robin Hoods" of the digital age, taking from the rich and giving to the disadvantaged (Goode & Cruise, 2006). Additionally, while all hackers

commit criminal acts, each subculture retains a distinct code of ethics (Goode, et al., 2006) reminiscent of codes established in other groups such as prison populations or gangs.

Power is yet another hacker motivation. Smyslova and Voiskounsky (2009) describe a hacker's motivation as generating positive feelings of competence and power. Furthermore, as a hacker's skills increase, their ability to solve ever more complex challenges not only continues to build their reputation but serves as a positive reinforcement for feelings of worth and accomplishment. Fotinger and Ziegler (n.d,) advanced the idea that hackers may be plagued by deeply rooted feelings of inferiority. As a result, their skills and abilities to assess system weaknesses, identify vulnerabilities and exploit those vulnerabilities may yield a sense of power not available to the hacker in other aspects of their lives.

Hackers commonly group themselves by the intentions of the hacker – white hat, grey hat, or black hat (Nikitina, 2012). Furthermore, the same skills used for hacking by attackers are used by cyber forensics experts, vulnerability assessment professionals and other government and law enforcement experts to defeat cyber-attacks (Fotinger & Ziegler, n.d.). Also, younger hackers may begin hacking from a desire to experience a thrill, pursue a challenge or even use hacking as an escape. Notably, Swan, (n.d.) addressed the ideology of hackers as deriving from an ethical code but based on ambivalence to the law, disdain for legal consequences, and derision for the structures that created dysfunctional interpersonal dynamics in their social systems.

Systems Theory Perspectives

In regard to relational theories, Symbolic Interactionism (SI) suggests that individuals interact based on their ability to connect around a common set of symbols that have recognized meaning for the group. Leonard (2013) describes the hacker's world as forging recognizable groups based on dress, virtual locations - signatures, and specifically the "tools of the trade"

(e.g., laptops, etc.). Yet, mental health therapists also have a lexicon of practice jargon that stretches from theoretical to applied language, generally accepted rules for dress, and practice settings. Therefore, norms and accepted standards become predictors of member behavior once individuals adopt identity within the group. Similarly, learned successful behaviors provide the basis for future behaviors although modified by current situations. Consequently, while learned behaviors from the standpoint of the hacker revolve around various emotional and/or physical rewards, learned behaviors for many clinicians involve accepting the status quo since they have not yet been compromised. Additionally, our definition of a perceived environment is important even though there may be a real environment that we do not accept or understand (Boss, 1993). The virtual worlds created by and/or infiltrated by hackers provide them with a sense of control and power that they often do not possess in their physical environments. All these factors, to include a divergence in threat understanding among cyber security and clinical professionals, align significantly with the sub-optimal use of risk mitigation techniques in mental health.

To further complicate the cyber security problem, the symbols and labels used in mental health and cyber security or even with the use of digital systems (broader IT terminology), in general, are not congruent. In fact, the technical jargon in cyber security is based on a very specific set of principles which is part of the professional language of the discipline. Consequently, it is difficult to bridge the language gap created by technical descriptions of cyber practice with the far more humanist language of mental health. Second, it is also difficult to understand the complex technologies associated with unique technical architectures, protection systems and assessment capabilities. For example, Guterman and Kirk (1999) observe that the ever-changing technological advances in the internet continue to create an entirely new set of conditions for social interaction. They assert, from a postmodern perspective, that reality is

created through society and based on a common language within those interactions. Consequently, if therapists are continuously required to learn new conceptual approaches and descriptions for digital changes, they may be unable to adapt security practices to those changes in meaningful ways. Third, the ever-expanding use of digital systems enables a significant increase in professional dialogue for research, education and training, and in the wider delivery of clinical services through remote therapy. However, Guterman and Kirk (1999) go on to stress that knowledge derives from the synthesis of observations across an entire community of participants. This synthesis of experiences across the community of mental health practices appears to be absent today. Fourth, and finally, from a social justice perspective, the larger the number of contributors to a specific concept, the greater the likelihood that the concept will reflect the norms and values of the society as a whole. Consequently, while web services, email and other digital systems provide a much richer opportunity to create knowledge for our profession and the broader mental health community, those advances also create attack surfaces for possible compromise. Of no surprise, Guterman and Kirk (1999) predict that the use of digital systems will continue to grow throughout our society, yet the sophistication of the threat, the pace of technological change, and a lack of cyber security insights serve to exacerbate already complex decision dynamics for non-cyber security professionals.

In addition to increased dependence on digital systems, many clinicians assume the use of these systems is either without risk or only creates small risk to the practice since they have not experienced a breach themselves. This false sense of security may arise from a faulty premise – why would anyone want to attack my networks as I'm only a small business and not worth anyone's time? That thought process defines a specific kind of risk environment and expected set of interactions that do not match the intentions of would-be attackers (Hoffman & Podgurskey,

2007). In fact, the fewer security features and protections aligned with small businesses make them more vulnerable to virtually any hacker skill level (script kiddies – APTs). Therefore, while clinicians interpret their digital environment as relatively safe, the reality of risk exposure is exactly the opposite (Pfleeger & Caputo, 2012).

Camp (2006) found "individuals systematically fail to respond to detailed risk information in a manner that would be predicted by strict rationality" (p. 2). Her research on mental models for reducing risk further suggests that as individuals fail to assess their risks effectively, technological solutions will not provide sufficient vulnerability mitigation. Consequently, models for effective risk mitigation must evolve to produce change in a clinician's threat awareness, recognition of policy, process, and technological actions, and understanding of the mitigating strategies available for use. Those enhancements to understanding may stem from employing multiple mental models to achieve change in clinician behaviors.

Recupero and Rainey (2005) discuss both the risks and benefits of digital media in use by clinicians following a forensic model of analysis (e.g., vulnerability + threat = risk). Their initial assessment considers the benefits of e-therapy in clinical practice noting that outcomes were similar for depressed patients in either face-to-face or e-therapy sessions. Recupero and Rainey (2005) also state that other studies suggested the efficacy of e-therapy in anxiety, loneliness and eating disorders. However, their research also identified numerous areas for concern in the use of digital media. Problems for clinical evaluation and consequently effective treatment can be influenced by patient anonymity, assuring patient identity, and incorrect contact data. Ethical concerns include technical problems that produce feelings in the client of apparent clinician disinterest. Other ethical issues involve ensuring an acceptable level in the standard of patient care – very difficult with the minimal guidelines currently established – and technical concerns

in automatic intercept and archiving of information by Internet Service Providers (ISPs). The authors also caution that legal implications for e-therapy may be influenced by laws that regulate inter-state telemedicine. Finally, the authors confirm, "That even when therapist and patient both employ sophisticated technology measures to increase the security of their communications, there is no ultimate guarantee of privacy or data security" (Recupero & Rainey, 2005, p. 408).

Similarly, family theories that consider hierarchies, power and control as central elements also intersect with cyber security. For example, systems theory views nature as a layering of systems, subsystems, and suprasystems that closely parallel the digital world and its network design constructs (Boss, et al., 2009). Additionally, systems theory also introduces the concept of "cybernetics' that incorporates the idea of communication and manipulation of information in controlling behaviors (Boss et al., 2009). Digital media were constructed to facilitate communication and manipulate data to enhance human connectivity and allow rapid access to information.

Abawajy (2012) highlights human factors as a major contributor to risk mitigation in his description of cyber security as the, "…comprehension that users have about the importance of information security best practices" (p. 237). His research emphasized the legal requirements for Payment Card Industry (PCI) Data Security Standards for anyone accepting credit card payments and the training requirements associated with that guidance. In fact, Abawajy (2012) found that multiple delivery methods for cyber training enhanced communication and retention of cyber security best practices and provided essential reinforcement of learning for risk mitigation.

Finally, social justice theory incorporates the concept of a social contract as one basis for moral and ethical interaction in society (Capehart & Milovanovic, 2007). Within that concept,

the implied or in some instances the explicit contract between client and clinician includes the mandate to “do no harm”. That requirement includes the clinician’s responsibility to defend against the potential compromise of client information from a lack of cyber security awareness or poor implementation of cyber policy, process, and technology. Hydari, Telang, and Marella (2015) advance the thought that higher levels of patient data security and confidentiality are enabled by the use of electronic health records but also conclude that Patient Safety Events (PSEs), including data breaches or other Information Technology (IT) lapses, “affect hundreds of thousands of patients in the U.S. and cost billions of dollars” (p. 31). However, they also identified that in Pennsylvania Hospitals, those that had adopted e-record protocols experienced a 27% decline in PSEs over the measurement period with additional improvements in reducing medication errors. As a result, the move to more sustained use of digital systems is likely to increase with a commensurate responsibility for clinicians to attain greater understanding of cyber security to fulfill the digital privacy and confidentiality contract with their clients.

Digital Practice in Mental Health Theoretical Support

Fernandez-Aleman, Senor, Lozoya, and Toval (2013) describe security and privacy concerns in using digital systems which also suggest a need for clinician action in securing client Personal Health Information (PHI), Personally Identifying Information (PII) and Personal Credit Information (PCI). They suggest that the use of e-records exposes client data to a wide number of administrative, financial, and other staff who should not have access to that information. Furthermore, their study showed that multiple layers of cyber security action provide the highest degree of risk mitigation for clients and practitioners. Sweeney (2002) suggests a specific anonymity technique (k-Anonymity) which incorporates physical characteristics and other identifying information as a substitution approach in identifying clients. Her methodology

enables increased client privacy protection through the use of unique personal characteristics combined with identifiers (e.g., a client's zip code, etc.) to establish client identification without the use of or reference to names when using digital systems. Similarly, Barrows and Clayton (1996) assess cyber security options in maintaining access while mitigating the risks of a digital compromise. Their model recommends a recognition of how digital systems will be used to meet operational needs, what threats are likely to be encountered and how to secure systems in light of those factors.

Finally, the social contract with clients and the broad guidelines established by federal, state, local, and tribal governing bodies as well as the lack of specific standards promulgated by professional organizations creates a confusing and uncertain terrain for clinicians to navigate (Kobus, 2015). However, risk mitigation approaches and accepting responsibility for maintaining client privacy and confidentiality are not options. In fact, they are essential elements in maintaining client trust.

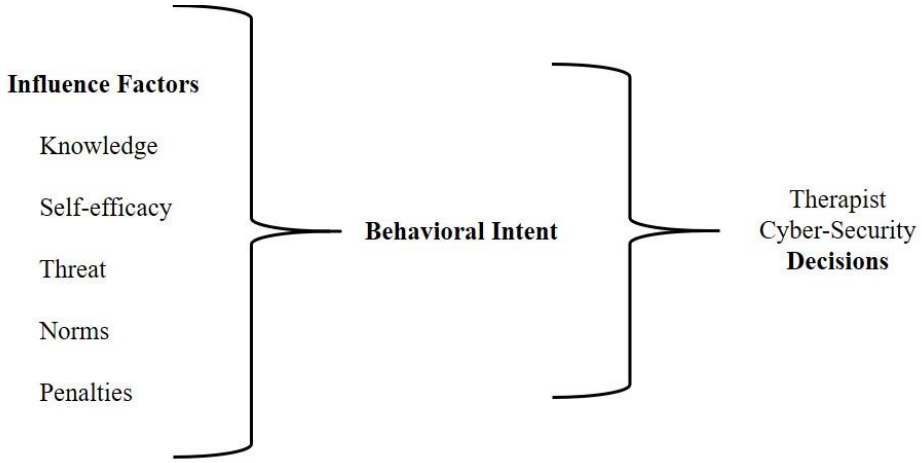
Behavioral Intent Theories on Motivation and Risk

Motivation and risk models have been developed for a wide range of human behavior, yet none have been specifically adapted to study the factors which may influence a therapist's cyber security behavioral intentions. Consequently, significant factors were extracted from open systems theory, expansive learning theory, general deterrence theory, control theory, social control theory, social learning theory, the theory of planned behavior, and the risk homeostasis, and TRIRISK models. These factors represented the practitioner's knowledge of laws and ethical guidelines, self-efficacy in implementing protective measures, understanding of threat intent and capabilities, the norms for adhering to typical security practices within the mental health community, and the recognition of the impact penalties may have for non-compliance. The

selected factors (Figure 1) emerged as a potential predictive design to describe the areas influencing a therapist's understanding of cyber security requirements (knowledge) and behavioral intent in enacting cyber security within a practice.

Figure 1

Influence Factors and Behavioral Intent Model



Although mental health clinical practices are, by definition, organizations designed to facilitate the delivery of treatment for clients with mental health and/or relational concerns, each practice is organized to provide specific services to clients and is therefore optimized around delivery of those services. However, general structures which enable service delivery, remain relatively constant across clinical practices (e.g., client health records, invoicing, informed consent documents, etc.). Yet, practices are also tailored to match the unique preferences of the practice owner or the environmental, legal, or ethical mandates of the practice location, clientele, or business model. As a result, organizational psychology in general, and open systems theory specifically, provide some perspectives surrounding the influences which may contribute to understanding the motivation of practitioners in adopting or dismissing intentions to address cyber security options within private practice. Notably, in open systems theory, three influencing, normative motivational areas are needed for organizations to function effectively:

awareness of "environmental pressures generated by the direct, observable requirements of a given situation, shared values and expectations, and rule enforcement (Katz & Kahn, 1978)." Therefore, the environmental pressures created by the use of digital systems in clinical practice aligned with an ever-increasing threat would be predicted to elicit a practitioner's decision to implement cyber security within the practice. Similarly, Herath and Rao (2009) determined that perceptions of the likelihood of a breach, social-organizational norms and the availability of resources are significant factors in decisions to adopt cyber security within an organization. However, while practitioners are exposed to news and other media reporting on cyber breaches at an increasing rate, most practices have neither been hacked nor even know of a hack firsthand. Consequently, the "direct, observable" aspect of the requirement may not be met (van Schaik, et al., 2016)

Second, although mental health therapists share ethical intentions concerning confidentiality and privacy, the unique ingredients for adopting cyber security may remain motivations at an individual, not shared, level and be more effected by risk tolerance than shared values. Awareness, then, may not be sufficient to compel action. In a study of German nationals' motivational processes, Scholl, M., Fuhrmann, and Scholl, L. (2018) suggested that educational programs would benefit students by including digital security as part of core programs to help individuals begin to develop a sense of responsibility and intentionality for cyber security. In keeping with Vygotsky's "zone of proximal development" (individual problem-solving versus learning from others), Engeström and Sannino (2009) provided insights into expansive learning theory that suggest that during times of significant change (e.g., rapid technological advance), disciplines are not completely mastered. Learning the intricacies of cyber security as a subcomponent of overall Information Technology (IT) fits this theoretical interpretation. This

perspective further suggests that dedicated focus on cyber security may be required to provide learning in how to secure digital systems effectively. Nevertheless, Carver and Scheier (1982) demonstrated that exposing individuals to specific schema make the ability to access actionable areas more available when needed if an effective feedback loop was also available. The catalyst for such a feedback loop may be influenced by the accepted norms established within a profession. The resulting message implies that cyber security motivation could be addressed through learned focus on individual responsibility as contributing to a shared value and with a realization that cyber security must be an inseparable component of any ethically sound business model (Boss, et al., 2009).

Third, and finally, although Health Insurance Portability and Accountability Act (HIPPA), Health Information Technology for Economic and Clinical Health Act (HITECH), Federal Trade Commission (FTC), and other federal, state and local laws require protection for personal information (e.g., Personally Identifying Information (PII), Personal Credit Information (PCI), Personal Health Information (PHI)), how those protections are implemented remains at the discretion of a practitioner population unfamiliar with the methods of creating effective security protocols (Hecker & Edwards, 2014; United States, Department of Health and Human Services, The Office of the National Coordinator for Health Information Technology, 2015; Secretary, H. O. HITECH Act Enforcement Interim Final Rule, n.d.; United States, Federal Trade Commission, Bureau of Consumer Protection, 2010). Furthermore, enforcement of legal standards continues to be inconsistent and audits only effect a small percentage of organizations. Highlighting this disconnect, Boss, et al., (2009), stress the importance of monitoring activities for compliance if organizational motivation is to be encouraged. Through this lens, the three requirements to establish an effectively operating organizational structure appear to be violated

when considering factors which could influence a therapist's intentions to incorporate cyber security decision making into clinical practice.

Many theories of motivation draw on the work of Bandura (Ajzen, 2002), especially in his discussion of self-efficacy. While an individual's specific actions or behaviors may not reflect confidence in completing the steps within an overall project, the individual's lack of confidence that executing the specific steps will create the desired conditions certainly effects their willingness to engage in the activities (Dwivedi, Rana, Anand, Clement & Williams, 2017). With a focus on cyber security, perceived self-efficacy would suggest that clinicians may struggle with multiple aspects of project control. For example, as attackers have more technical sophistication than most clinicians, attempts to technically control the digital environment may appear futile (locus of control). Furthermore, the clinician may also perceive that despite significant effort, the end state of those efforts may still not produce cyber security. The theory of planned behavior describes self-efficacy, perceived behavioral control, and locus of control in just this way: the recognition that even best efforts may not create the desired result leads to a decision to reject an action (Ajzen, 2002; Armitage & Conner, 2001).

Lee, S. M., Lee, S., and Yoo (2003) describe motivation for internal cyber security by combining elements of general deterrence theory (GDT) and social control theory (SCT). Research in these areas indicates that organizational focus of attention creates motivational influences that produce individual responsibility for cyber security. Lee, et al., (2003) describe GDT as involving an emphasis on security *actions*, while four areas comprise SCT: Attachment (affection for others), Commitment (investment in societal values), Involvement (dedicated time), and Norms (acceptance of traditional values). These SCT areas focus on an individual's connection to others within the organization and loyalty to the organization itself. In that context,

a professional organization's involvement in establishing focused, enforceable requirements for licensed practitioners may advance cyber security actions throughout the profession. Indeed, creating a professional commitment focused on expected cyber security behavioral norms may be important in motivating practitioner action to secure information and systems.

While social control theory focuses on the significance of social connections to affect behavior, control theory emphasizes a difference between strong and weak bonds within a system – predictive of choices an individual may make based on self-interest. Carver and Scheier (1982) suggest control theory (CT) as a mechanism for understanding human decision-making processes. With broad applicability for cyber security decision making, CT emphasis on systems dynamics and feedback loops is especially noteworthy. In CT, "perception, comparison of the perception with a standard, behavioral output, and the effect of the behavior on the environment" (Carver & Scheier, 1982, p. 112) serve to provide structure for understanding influential motivations and judgement in the intention-decision process. In cyber security, a clinician's perception of the security of the practice's digital systems and the likelihood of a compromise may establish the conditions to create a negative feedback loop surrounding additional required protections for confidentiality and privacy. Similarly, comparing that perception to others within the mental health field, may move the clinician to a perspective of being within the standard of practice for the profession. However, as discussed under the theory of planned behavior (Madden, Ellen & Ajzen, 1992) and reinforced here in control theory, an *expectation* that a more effective outcome may not be the result of changed behavior and recognition that change in action may not produce reduced risk, both serve to reinforce a status quo motivational construct.

Also, West (2008) confirms this process in his discussion of "risk homeostasis". In his research, as people implement greater security, they engaged in riskier behaviors. Additionally,

individuals may believe they are at less risk than others, regardless of the security they have in place and although intellectually people understand the risk and implications of compromise - belief that others are more vulnerable militates against adopting greater security measures. Finally, safety and security are abstract with an uncertain amount of value while costs to establish effective cyber protections are concrete. Consequently, when people calculate the relative value of loss and gain, assured loss (cost to implement protection) is weighted more heavily (Chronopoulos, Panaousis, & Grossklags, 2018).

Ferrer, Klein, Avishai, Jones, Villegas, and Sheeran (2018) discuss the idea of risk perception in motivation. Employing a TRIRISK model comprised of deliberative (reasoned judgements), affective (feelings), and experiential (heuristic) perception, the authors examined risk decision processes based on self-protective assessments to mitigate a health threat. While not a direct comparison to systems risk decisions, the results provide an intriguing parallel within a risk-reward, cost-consequence context. Notably, fear becomes less meaningful as a motivational element as the threat increases. Consequently, although the risk of compromise for digital systems continues to escalate, from these research findings, the threat alone would not be expected to generate an intention to act to combat the challenge of a potential breach.

Chapter 3 - Methods and Procedures

This study was designed to identify factors that influence the intentions of mental health therapists to address cyber security in clinical practice. Specifically, the question researched was, Do the following factors serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice?: (a) knowledge of laws and ethical guidelines, (b) self-efficacy in implementing protective measures, (c) understanding of threat intent and capabilities, (d) the norms for adhering to typical security practices within the mental health community, (e) the recognition of the impact penalties may have for non-compliance. Information was collected using a modified questionnaire based on previously validated instruments.

Research Design

Notably, representative surveys have been constructed to provide broad insights into relevant areas of motivation (Herath & Rao, 2009; Rhee, Kim, & Ryu, 2009; S. Boss, Kirsch, Angermeier, Shingler & R. Boss, 2009) but none specifically designed to address cyber security practices within the mental health arena. Also, the National Institute of Standards and Technology (NIST) (Swanson, 2001) developed surveys which provide a broad, generalized multi-industry standard but again without direct focus on mental health. The survey developed for this study was also created with an understanding of generalized industry level studies but modified to reflect the probable uses of digital capabilities and systems within mental health clinical practice. The survey was designed to determine a clinician's knowledge of cyber security requirements, gain an understanding of their use of digital systems in practice, assess the factors influencing behaviors, and the clinician's intentions for protecting data, information, and information systems themselves. The research instrument was submitted to the St. Mary's

University Institutional Review Board and piloted to insure content validity and clarity of the survey questions. The validation group consisted of mental health therapists drawn from private practice: individual, small group, and larger institutions. Revisions to questions were reviewed by the author to determine the sufficiency of required modifications and face validity. Once developed, piloted and adjusted for language and understandability of terms, the survey was advertised through multiple state and professional mental health membership sites. The advertisement contained a link to the survey (Appendix A) enabling participants to complete the instrument while remaining anonymous. Results of the survey were intended to extend our knowledge of cyber security practices within the mental health community, the factors which influence cyber security actions, and the way those factors affect the therapists' intentions to address cyber security within clinical settings. Furthermore, the survey responses also established initial information on threat awareness and clinician motivation to address cyber security requirements established by legal mandates and professional codes of ethics.

Participants

In collecting data relevant to mental health practitioners' intended processes for addressing cyber security in clinical practice, it was important to clearly define the sample population. Therefore, since clinicians are either fully licensed members of the mental health community or associate/intern members, and since associate/intern members must be supervised, decisions for incorporating cyber security into clinical practice may appear to fall to those who are fully licensed. However, both associates and interns are licensed professionals (albeit at a provisional level) and are therefore ultimately responsible for client confidentiality, privacy, and the integrity of the electronic capabilities (data and systems) they use. As a result, a composite, convenience sample population for this study consisted of all licensed practitioners whether fully

or provisionally licensed. Furthermore, as MFTs, counselors, and counseling psychologists are largely representative of the broader mental health profession, the study may also be of use to other mental health providers, and in fact, to those within the cyber security community whose interests and responsibilities extend to the mental health field.

Participants were recruited through state professional organizations. Initially, state organizations were selected through identification of states with the highest numbers of mental health providers. States were also selected across regional areas to establish a representative cross section of marriage and family therapists, counselors, and psychologists throughout the United States. Based on the numbers of questions in the survey, states continued to be contacted until the number of completed surveys provided an ability to generalize research findings. Research participants who completed the survey were able to access an author developed Risk Assessment template following submission of their answers as incentive to complete the instrument.

Model Design

Sarstedt, Ringle, and Hair (2017) suggested two stages in evaluating the model design and the structural and predictive elements of the instrument in a SmartPLS structural equation model (SEM). Stage one addresses the theoretical underpinnings for the model itself while stage two concerns developing insight into the instrument's structural and predictive dynamics. Additionally, when both reflective and formative indicators comprise the model different, yet specific tests are required to test the model's strength and predictive abilities. For reflective elements within the composite model, indicator reliability, internal consistency, and discriminant validity were examined. For composite model formative factors, determining acceptable outer

weights, outer loadings when necessary (e.g., if outer weights were low), model bias, and collinearity were important. Finally, model fit was established using SRMR data.

Stage one examination of the theoretical basis for the new model was accomplished through comparison with existing models and instruments. Instrument factors were initially selected based on relevant theories of motivation to include: open systems theory (awareness of environmental pressures that are directly observed, shared values and expectations, rule enforcement) - expansive learning theory (with significant change, disciplines not completely mastered) – general deterrence theory (actions aligned with penalties) - social control theory (attachment, commitment, involvement, norms) – control theory (strong vs weak system bonds) – theory of planned behavior (expectation of results) – risk homeostasis (greater security produces riskier behavior, scale reduces risk of compromise) – TRIRISK model (reasoned judgement, feelings, experience). However, knowledge was also included as a factor since knowledge of requirements, capabilities, threats, others' actions (norms), and consequences for inaction (penalties) are requirements for effective motivation and behavior determination.

Instrument Design

To enable collection of data that allows for an assessment of motivational influences and clinician intentions, a practitioner-cyber security measurement instrument was developed. Instrument indicators were designed by aligning questionaire language with questions similar to those developed by Herath and Rao (2009), Rhee, Kim, and Ryu (2009), and S. Boss, et al., (2009). In addition, the author developed new behavioral intent questions patterned after the theory of planned behavior (TpB) design established by Ajzen (2002). The result is a modified, study specific, survey instrument. Questions were designed with either semantic (nominal) or scaled (ordinal) responses. Semantic responses were: Yes, No, I don't know, while scaled

responses employed a five point Likert scale. Additionally, the survey was piloted (Cronbach's alpha = .912) to identify any necessary structural modifications and further verify content validity, construct validity and reliability.

Definitional consistency was maintained throughout the instrument design and modification processes by comparison with existing surveys (Herath & Rao, 2009; Rhee, et al., 2009; S. Boss, et al., 2009; van Deursen & Van Dijk, 2010; Swanson, 2001) and construction methods (Ajzen, 2002). Variables were operationalized across survey sections representing the potential influencing factors and behavioral actions. Using similar sentence structure to the Herath and Rao (2009) design approach, behavioral intent (BHI) was derived from questions concerning the perceived likelihood of a compromise, severity of a compromise, a clinician's concerns of a compromise and the ability of the clinician to take effective cyber security action (BHI questions 15 – 17, 20 – 22, 29 – 32, 39 – 42, 49 – 52, and 58 – 61). Attitude questions were used to determine a therapist's perspective on security policy and effectiveness if actions were taken (questions 15, 16, 19, 22, 26, 38, 40, 42, 43, 48, 49, 50, 51, 55,56, 60, and 61). To measure awareness of requirements, knowledge of legal and ethical regulations (questions 12 – 14 and 18) and expected enforcement of policies (penalties; questions 53 – 57) were included. The effect of norms (questions 43 – 48) for influencing intentions was addressed through questions on both subjective and descriptive norms. Self-efficacy (questions 23 – 28) incorporated questions on a therapist's facility in recognizing and implementing cyber security options in the context of operational vulnerabilities. Threat awareness (questions 33 – 38) was covered by questions on both threat sophistication and threat intentionality

Materials

Materials consist of an approximately 60 item survey accessible through an anonymous Qualtrics link, advertising information, and an author developed cyber security risk assessment template. Item and structural analyses were performed using both SPSS and SmartPLS statistical programs.

Procedures

The survey consists of 60 multiple-choice, scaled, and semantic questions surrounding the factors that may influence a therapist's intentions to enact cyber security within their clinical practice in accordance with published guidance (e.g., law and ethical codes). After subtracting demographic questions, approximately 200 completed responses were desired to provide sufficient power to enable generalization of results. The instrument itself along with additional required research information specifics, were submitted to the St. Mary's University Institutional Review Board (IRB) for approval and authority to conduct the research. Following IRB approval, the survey was pilot tested to insure clarity of question intent and understandability of language and terms. Required adjustments were incorporated and the resulting modifications assessed by the author. No major revisions were required, and the survey was promulgated for data collection. The final survey instrument was loaded onto the Qualtrics website and the access link transmitted to state professional organizations for advertisement to their members. Therapists accessed the instrument anonymously through the advertised link. Responses were then extracted from Qualtrics for analysis and manipulation in the selected statistical programs (e.g., SPSS, SmartPLS).

Research Hypotheses

The purpose of this research was to describe mental health practitioners' current cyber security knowledge, practices, and the behavioral intentions influencing a therapist's implementation of cyber security within clinical mental health settings. Factors for the study were determined through a review of current systems, behavioral, and motivation theories then selected based on expected relevance to actual clinical practices. The research explored the factors of knowledge, self-efficacy, threat awareness, norms, and penalties. The specific research question was: What factors serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice? Consequently, the research design was constructed to provide insight into the significance and strength of each factor on a clinician's behavioral intent. Research hypotheses tested included:

H_1: Practitioners with greater knowledge of legal and ethical requirements to protect sensitive information and systems will adopt precautions

H_2: Practitioners with higher perceptions of self-efficacy will take greater direct precautions to protect sensitive information and digital systems

H_3: Therapists with greater insight into the severity of the potential threat will enact more digital security protections.

H_4: A therapist's commitment to protecting sensitive information/systems will be increased by their perception of compliance by other practitioners.

H_5: Practitioners who believe penalties will be associated with non-compliance of cyber security rules will take precautions to protect sensitive information.

The results of data analysis were expected to show that therapists believe they understand the requirements for confidentiality established by federal and state law (H_1). Additionally,

therapists with a greater sense of self-efficacy were expected to take more precautions to address cyber security risk (H_2). Similarly, therapists with minimal awareness of the potential severity posed by cyber threats (H_3), may believe they do not have the ability to create a meaningful difference in addressing risk. Additionally, those therapists that perceive their peers as fulfilling the guidance specified in law and ethical codes may be more likely to conduct appropriate measures to defend sensitive information and information systems from attack (H_4). Finally, those therapists that believe processes are in place to enforce the standards required by law and ethical codes may be motivated by the potential penalties associated with non-compliance (H_5).

Statistical Methods and Analysis

In stage two, the finalized composite research model was assessed for structural and predictive sufficiency. Several researchers (Kock, N. 2017; Becker, Klein, & Wetzels, 2012; Lowry & Gaskin, 2014; Hair, Sarstedt, Hopkins & Kuppleweiser, 2014) reported the strength of structural equation modeling (SEM) and partial least squares (PLS) in behavioral investigation and predictive analysis. Consequently, PLS – SEM was determined to be an effective method for analyzing the resulting survey data. In that regard, SmartPLS software enabled insights into both structural and path analysis to determine the significance of formative factor variables on the reflective behavioral intent variable. Standard default SmartPLS settings were used, with the exception of 5000 sub samples in bootstrapping, to create analytic insights and to ensure data elements reflected acceptable structural and predictive results.

Face validity was established through direct observation and comparison with existing models (Herath & Rao, 2009; Rhee, et a;., 2009: S. Boss, et al., 2009; Ajzen, 2002). Internal consistency was established using Cronbach's alpha and composite reliability. Composite reliability also confirmed construct validity (Hair, Sarstedt, Hopkins, & Kupplweiser, 2014).

Discriminant validity for reflective factors was assessed using the preferred Heterostat – Monostat method where a value less than .9 indictes acceptable discriminant validity (Henseler, Ringle, & Sarstedt, 2014). Content validity was determined through expert examination of factors and indicators and convergent validity was not assessed for the composite model (Lowry & Gaskin, 2014). However, convergent validity was recommended to be assessed using individual factor analysis for each formative factor pathway – Knowledge to Knowledge behavioral intent (BHI), Self-efficacy to Self-efficacy BHI, etc. where a 0.5 path score is considered acceptable (Carlson & Herdman, 2012; Wong, 2013; Sarstedt, Ringle & Hair, 2017, p. 28).

In formative models, indicators define different aspects of a factor, therefore typical measurements for structural integrity are not considered conceptually valid (Lowry & Gaskin, 2014). Similarly, outer loadings, except as needed to assess outer weights that fall below accepted values, and average variance extracted are also irrelevant for formative factor variables (Wong, 2013, p. 14). However, Wong (2013) also asserted that measuring inner model relationships, outer model weights, and collinearity were necessary assessments for models with at least one formative factor. Finally, Hussain, Fangwei, Siddiqi, Ali, and Shabbir (2018) proposed that for an outer model (e.g., the structural components of the model), reliability is measured by assessing results from the entire composite survey instrument as opposed to individual factor analysis.

As a result, both factor and path analyses were used to understand the structural effectiveness and predictive power (e.g., significance and strength) of independent latent variables on the dependent variable of behavioral intent (BHI). Structural assessment was conducted using a combination of the Lowry and Gaskin (2014), Wong (2013), Sarstedt, Ringle,

and Hair (2017), and Hussain, Fangwei, Siddiqi, Ali, and Shabbir (2018) methods. Path coefficients, t-scores, f^2, and R^2 were used to determine the predictive significance of relationships and the strength of factor impact (Wong, 2013).

Outer model weights were assessed with t-scores of 1.96 considered as acceptable (Lowry & Gaskin, 2014; Wong, 2013). However, for indicators with t-scores below 1.96, comparison with outer loadings above 0.4 was used to determine item significance (Sarstedt, Ringle, & Hair, 2017). Factor loadings and weights appear in Appendix B, tables B1 and B2 respectively. Following that review, indicators 18, 24, 29 (Knowledge); 33, 35, 36 (Threat); 45, 47 (Norms); and 53, 54, 55 (Penalties) were initially removed from the model. However, individual item removal and model testing did not reflect increased model strength. Therefore, all indicators were allowed to remain within the model (Sarstedt, et al., 2017).

Formative factor multicollinearity was evaluated through assessing variance inflation factors (VIF) where values below 10 are acceptable and below 3.3 defined as rigorous and model fit was evaluated using SRMR below 0.08 desired. Survey results were also compared with government established cyber security best practices (U.S. NIST, 2014) but evaluated through a lens of mental health clinical practice. Finally, demographic survey questions were used as control items to include age, gender, professional affiliation, educational level, and urban vs rural practice.

Chapter IV – Results

The purpose of this research was to describe mental health practitioners' current cyber security knowledge, practices and the behavioral intentions influencing a therapist's implementation of cyber security within clinical mental health settings. As a result, the research explored the factors which serve to reflect a therapist's understanding of legal and ethical mandates and behavioral intentions to protect sensitive information and systems in clinical practice. Knowledge of laws and ethical guidelines, self-efficacy in implementing protective measures, understanding of threat intent and capabilities, the norms for adhering to typical security practices within the mental health community, and the recognition of the impact penalties may have for non-compliance comprise the areas studied. The specific research question was: What factors serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice? Potential factors were identified through investigating earlier research on motivation and particularly research into cyber security motivational constructs then compared to theoretical models predictive of behavioral intent. Social learning theory, open systems theory, control theory, social control theory, and the theory of planned behavior emphasize the effects of norms in establishing behavioral intent while expansive learning theory, general deterrence theory, and the theory of planned behavior predict self-efficacy as an essential factor. Also, open systems theory, general deterrence theory, and the TRIRISK model stress the importance of knowledge, penalties, and threat awareness respectively. Factors and behavioral intent questions for inclusion in the study were then developed to align with representative practice dynamics (e.g., use of electronic medical records, computer-based communication systems, etc.). Hypotheses were examined through analysis of model results using structural equation modeling (e.g., SmartPLS) while

theoretical results were assessed through an evaluation of specific questions matched to their theoretical constructs. Finally, data collection was concluded after more than 300 participants accessed the survey resulting in 210 completed responses.

Results of the study indicated that although practitioners believe they have the requisite knowledge to address cyber security within their practice, inconsistencies in their understanding of implementation responsibilities create gaps in protecting client confidentiality and privacy. Similarly, clinicians also reported they are not confident in conducting required risk assessments, have little understanding or awareness of the threat, and fail to expect consequences for non-compliance behaviors. Furthermore, although clinicians anticipate professional organizations and colleagues expect compliance with laws and ethical mandates, clinicians also believe specified standards are not being followed. The contradictions visible in these study results suggest a significant level of confusion among clinicians as they attempt to adhere to legal and ethical guidance without the ability to implement security practices, the awareness of cyber security threat conditions, nor a recognition of the consequences for practitioner inaction. and motivation.

Sample Description

The study included Marriage and Family Therapists, Counselors, and Psychologists in clinical practice. Participants were contacted through their specific professional organizations and advertisement for the anonymous survey Qualtrics link was announced in accordance with the professional organization's guidelines (e.g., email, website, Facebook, etc.). Although more than 300 surveys were initiated, 210 (n=210) surveys were completed and submitted. Potential reasons for unfinished surveys include a respondent's perception of failing to answer questions correctly, length of the survey resulting in a longer time commitment than anticipated, and

interruptions which required immediate attention, then not returning to complete the survey. As partial surveys may not have reflected accurately on descriptive factor or behavioral intent responses based on the distribution of questions throughout the instrument, partial surveys were not included in the data assessment. Therefore, only the completed and submitted surveys were included in the final data analysis.

Demographic Data

Of the final completed surveys, 69% were completed by Marriage and Family Therapists, 27.8% were completed by Counselors, and 6.2% were completed by Psychologists (Table 1). Additionally, although 110 professional organizations were contacted across 40 states, only 30 organizations agreed to advertise the survey link while others cited professional guidelines as rationale for refusing the request. After several months and repeated contact with those organizations which provided support, a sufficient sample of clinicians was obtained. Of the survey respondents, 69.5% reported being female and 30% male with 1 person deciding to select "prefer not to answer." Also, the majority of participants (87.1 %) identified themselves as located in an urban practice while 12.9% defined their practice as being rural. Most participants selected southern (57.6%) and mid-western (19.5%) regions as their practice location and notably, the highest percentages of responding practitioners reported having 21 or more years in practice (31%) followed by less than five years of practice experience (24.3%) and 6 – 10 years of experience (24.3%) respectively (Table 1) for demographic statistics details).

Table 1

Descriptive Statistics

	Count	Percent		Count	Percent
Gender			*Geographic Region*		
Male	63	30.0	East	14	6.7
Female	146	69.5	South	121	57.6
Primary Location			Midwest	14	19.5
Urban	183	87.1	West	34	16.2
Rural	27	12.9	*Professional Alignment*		
Years in Practice			Psychologist	13	6.2
<5	51	24.3	Counselor	52	27.8
6-10	31	14.8	MFT	145	69.0
11-15	26	12.4	*Highest Level of Education*		
16-20	8	3.8	Masters	136	65.0
11-15	26	12.4	Doctorate	74	35.0
16-20	8	3.8	*License Category*		
21+	18	8.6	Fully Licensed	182	86.7
			Provisional	28	13.3

Note: n=210

Composite Model Results - Structural Analysis (Outer Model)

Lowry and Gaskin (2014) provide rationale to clarify the determination of formative versus reflective variables. Their discussion emphasizes the requirement for formative indicators to align as factors which produce or define a construct. As a result, they then state, “The concepts of construct validity and reliability, therefore, do not apply to formative constructs” (p. 15). However, construct validity and reliability are important for reflective constructs. As the selected research model contains formative and reflective factors, multiple tests were performed to ensure the structural integrity and predictive ability of the instrument. Formative indicators consisted of

questions associated with each factor (e.g., knowledge, self-efficacy, norms, threat, and penalties) while reflective indicators were associated with the factor designated as behavioral intent (BHI). Arrows pointing from indicators to factors establish formative relationships. Arrows pointing from the factor to indicators display reflective constructs.

Internal consistency

Survey questions were piloted using representative clinicians. The initial piloted survey consisted of 71 nominal and scaled questions. Resulting internal reliability (Cronbach's alpha = 0.912) and dialogue with pilot participants indicated excellent question clarity and content. However, additional feedback revealed the survey required an average of 20 – 25 minutes to complete. As a result, survey questions were reduced to enable instrument completion within 15 minutes by removing a motivational factor-behavioral intent section (e.g., resource availability) to be assigned for future research. The internal consistency of the final version of the scale was determined to be acceptable with Cronbach's alpha at 0.873. In addition, internal consistency of final scale items was assessed using SmartPLS composite reliability. Composite reliability (0.883, $p<0.000$) confirmed Cronbach's alpha measurements for internal consistency.

Construct Validity

While the composite model is not measured for convergent validity, convergent validity was assessed by examining individual constructs within the model (Sarstedt, et al., 2017). Each factor was aligned to its specific Behavioral Intent indicators (e.g., Knowledge, Norms, Penalties, Self-efficacy, Threat, aligned with their specific Behavioral Intent factors (Figures 4 - 13). Formative factor content validity was determined through comparison with previously developed instruments (Herath, et al, 2009; Rhee, et al, 2009; Boss, et al, 2009; Ajzen, 2002).

Indicator item question stems are listed in Table 2 with stems from previously developed instruments included for comparison.

Table 2

Content Validity of Formative Factors

Formative Factors, BHI Items	Herath & Rao (2013) Items	Rhee, et al. (2013) Items	Boss et al. (2013) Items
Knowledge			
Knowledge reduces compromise risk…	Policies are available…	I will learn more about information security …(BHI)	I am familiar with guidelines and policies …
I review cyber security practices… (BHI)	I follow security policies…(BHI)		I am required to know procedures…
Knowledge enables me to comply…(BHI)	Adopting security is important…(BHI)		
Self-efficacy			
I feel confident in my skills…	I would be able to follow policies…	I feel confident in protecting…	Employees can make a difference…
I can make a difference…	Adopting policies are important…	How often do you check security…(BHI)	I secure my system…(BHI)
I will take steps…(BHI)	If I wanted to, I could follow policies…(BHI)	I will enforce procedures…(BHI)	
Norms			
My organization thinks I should follow …	I am expected to help this organization…	Not addressed	Security takes too much time…
My colleagues think I should…	My colleagues think I should follow security…		There is an understanding I will comply…
I intend to comply with…(BHI)	I am certain I will follow security rules…(BHI)		It is expected I will take an active role…
Threat			
I believe information is susceptible…	Not addressed	Threats to information are controllable…	I believe information is vulnerable…
Threats are controllable…		There exists means to control threats…	How likely will a security violation cause…
I plan to understand…(BHI)			I keep aware of the latest threats…(BHI)
Penalties			
There are penalties for breaking rules…	Computer practices are monitored…	Not addressed	Managers evaluate security behaviors…
I will take action to reduce risk…(BHI)	Organization disciplines employees who break rules…		I pay attention to computer security…(BHI)
	I am likely to follow…(BHI)		

Discriminant validity was determined through SmartPLS using the Heteroststst-Monostat method with an observed value of 0.853. Similarly, assessing variance inflation factors (VIF) to determine collinearity is important when formative factors are involved. VIF results were determined to be less than 3.3 with one exception, question 30 at 3.6. Most factor results were below 2.0 (Table 3).

Table 3

Composite Collinearity VIF

Q #	Value	Q#	Value	Q#	Value	Q#	Value	Q#	Value
Q12	1.669	Q23	2.657	Q33	1.057	Q43	1.565	Q53	1.306
Q13	1.619	Q24	3.126	Q34	1.073	Q44	1.359	Q54	1.473
Q14	1.291	Q25	1.521	Q35	1.532	Q45	1.310	Q55	2.275
Q15	1.326	Q26	1.381	Q36	1.412	Q46	1.538	Q56	2.466
Q16	1.112	Q27	2.291	Q37	1.253	Q47	1.178	Q57	1.122
Q17	1.251	Q28	2.224	Q38	1.062	Q48	1.446	Q58	2.690
Q18	1.011	Q29	2.293	Q39	1.921	Q49	2.367	Q59	2.320
Q20	1.329	Q30	3.623	Q40	1.783	Q50	1.219	Q60	1.201
Q21	1.251	Q31	3.288	Q41	1.768	Q51	2.054	Q61	2.541
Q22	1.500	Q32	2.658	Q42	1.687	Q52	1.952		

Outer weights were measured with indicators 14, 18, 24, 29, 33, 35, 36, 45, 47, 53, 54, and 55 displaying weight results lower than 1.96. Upon comparison with outer loadings for those indicators, indicators 18, 33, 35, 36, 47 and 53 remained below desired levels. Consequently, those indicators were removed from the model and the model was re-run following every deletion. Nevertheless, removing the indicators did not change composite reliability nor improve other model values significantly. Therefore, all indicators were retained within the model (Hair,

et al., 2014). Finally, model fit was confirmed using standardized root mean square residuals (SRMR) with a result of 0.075.

Composite Model Results - Path Analysis (Inner Model)

All analyses were conducted through either SPSS (e.g., initial survey pilot results and demographic data) or SmartPLS (final survey analysis results). Path importance was determined using composite bootstrapping for statistical significance and strength of factor relationships was identified using f^2 where less than .1 represents small effect, 0.15 is associated with moderate effect and .3 or larger constitutes large impact (Chin, Marcolin & Newsted, 2003). Also, significance for path coefficients is considered sufficient when the coefficient is greater than 0.2 (Wong, 2013). Path coefficients for the composite models, confirm t-score interpretations.

For the inner predictive model, variable relationship strength was assessed with an R^2 of 0.822 indicating a substantial effect for the five formative factors on behavioral intent. Yet, individual differences were observed for each of the factors. Path coefficients and t-statistic values for Knowledge (0.02; 0.632) and Penalties (0.068; 1.209) did not reflect a significant impact on the aggregated BHI dependent variable. Results for Self-efficacy (0.319; 5.534), Threat (0.218; 4.738) and Norms (0.549; 11.094) did, however demonstrate significant impact on BHI. F^2 scores of 0.002, 1.082, 0.016, 0.322, and 0.211 for Knowledge, Norms, Penalties, Self-efficacy, and Threat respectively indicate a range of effect t sizes. Norms reveled significant effect, Self-efficacy and Threat showed medium effect size, and there were insignificant effects for Knowledge and Penalties.

Of note, Lowry and Gaskin (2014) suggest even small effect sizes may be significant. As displayed in composite model Figures 2 & 3. Knowledge and Penalties appear to have little effect on clinicians aggregated behavioral intent. In fact, Knowledge appears to have a slightly

negative effect on behavior suggesting Knowledge without the impact of other influencing factors is not sufficient to create behavioral intent more broadly. Similarly, questions 33, 36, and 53 displayed slightly negative effects on behaviors yet while questions 33 and 36 are included within the threat area, Threat still is associated with significant effect on Behavior. Penalties (including question 53) also contributes to the overall composite positive effect with the aggregated R^2 displaying strength of the integrated relationships model above 0.8 (actual value of 0.822; Figure 2).

Hypothesis Results

Hypothesis results displayed varying results for model factors aligned with composite behavioral intent. The alternate hypothesis of ***H*₁: Practitioners with greater knowledge of legal and ethical requirements to protect sensitive information and systems will adopt precautions** was not substantiated within the composite model. The path coefficient of – 0.021 (p = 0.874) demonstrated no significant relationship to combined behavioral intent characteristics. Furthermore, the Knowledge t-score of 0.632 confirmed acceptance of the null hypothesis.

However, the path t-score (5.534) and path coefficient (0.319) for Self-efficacy (p = 0.025) indicated rejecting the null hypothesis and accepting the alternative hypothesis of ***H*₂: Practitioners with higher perceptions of self-efficacy will take greater direct precautions to protect sensitive information and digital systems.** The effects of self-efficacy on a clinician's intentions and are important considerations in establishing motivation and subsequent action to protect sensitive digital systems and information.

Additionally, the path t-score (4.738) and path coefficient (0.218) for Threat validated rejection of the null hypothesis and accepting the alternative (p = 0.046). ***H*₃: Therapists with greater insight into the severity of the potential threat will enact more digital security**

protections. The clinician's understanding and awareness of Threat dynamics effected the composite view of clinician responses to cyber security intent.

Of note, the path t-score (11.094) and path coefficient (0.549) for Norms ($p = 0.004$) displayed the largest significance on behavioral intent. These results determine rejecting the null hypothesis while accepting ***H_4*: A therapist's commitment to protecting sensitive information/systems will be increased by their perception of compliance by other practitioners.** Although inconsistencies appeared in answers to Norms indicator questions, the overall effect of the Norms area created significant motivation to protect privacy and confidentiality for clients and clinicians.

Finally, results of the Penalty t-score (1.209) and path coefficient (0.068) revealed that the factor did not sufficiently impact behavioral intent to reject the null hypothesis ($p = 0.64$). Consequently, the null hypothesis in this case was accepted. While the alternate hypothesis of ***H_5*: Practitioners who believe penalties will be associated with non-compliance of cyber security rules will take precautions to protect sensitive information** was not accepted**.** Penalties alone appear to have insufficient strength to compel compliance.

Figure 2

Composite Factor Analysis and Behavioral Intent using Consistent PLS Algorithm

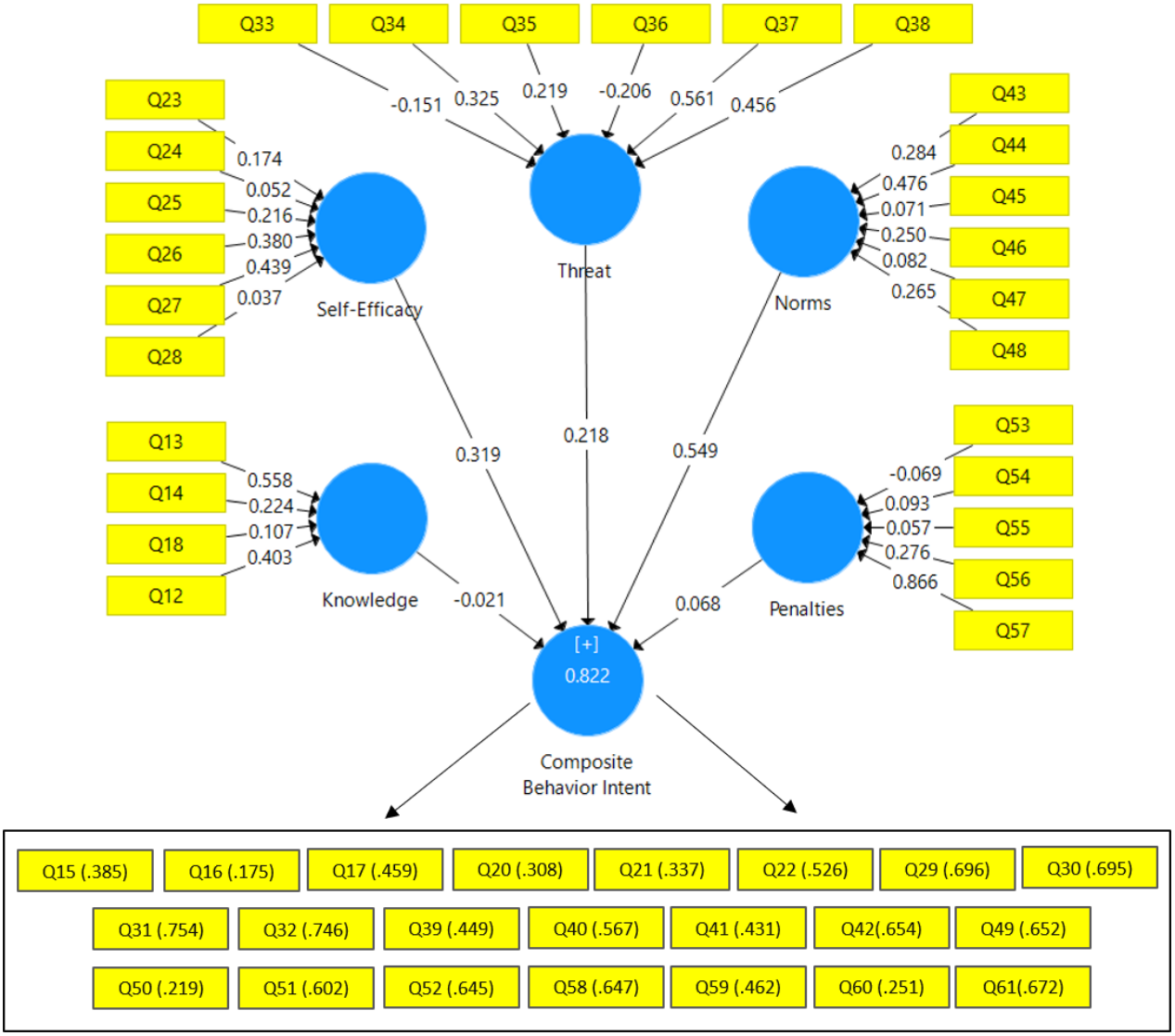
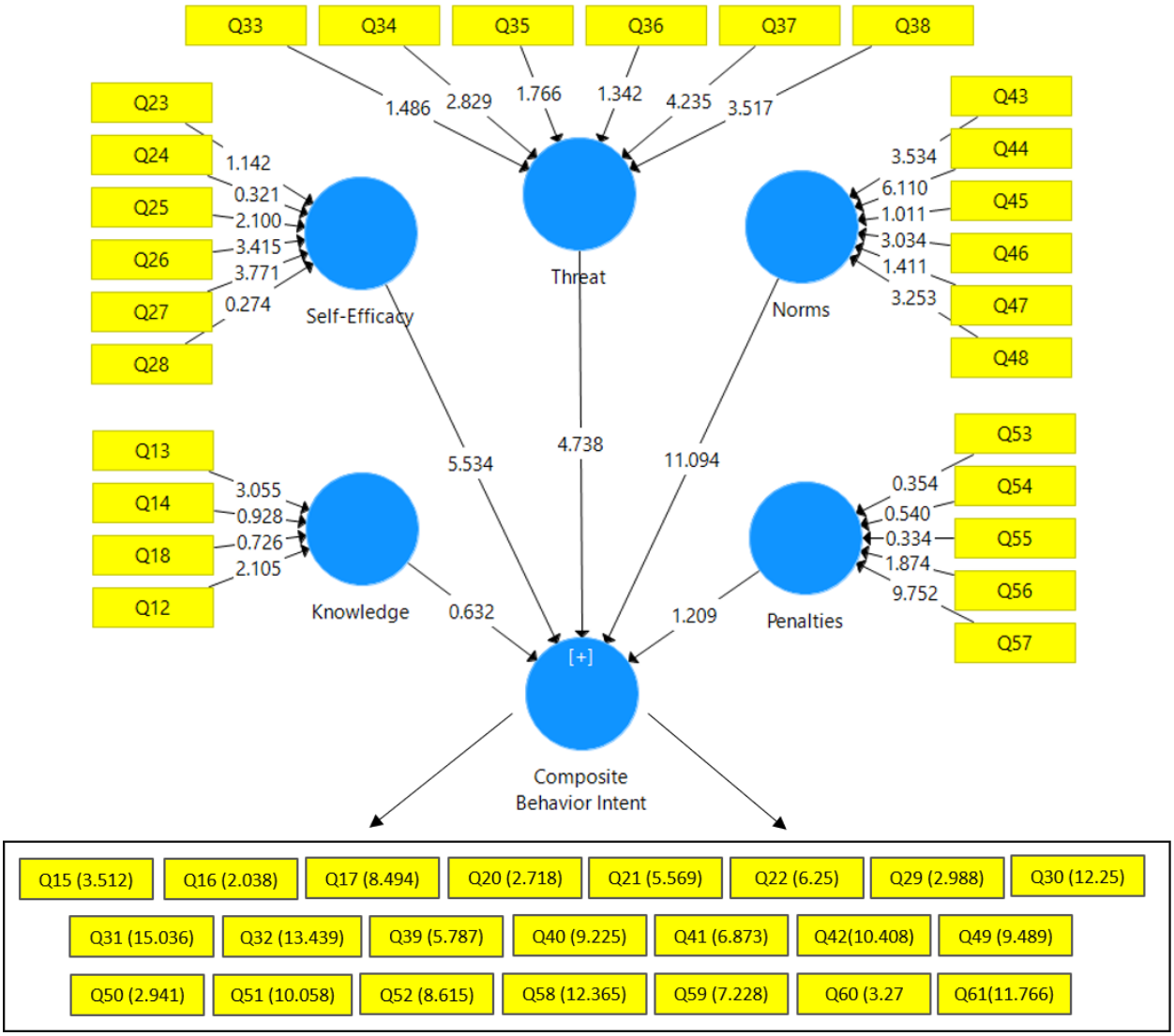


Figure 3

Composite Path Analysis and Behavioral Intent using Consistent Bootstrapping



Individual Factor Results

Although the composite model is not assessed for convergent validity in models with formative elements, each independent latent factor should be evaluated against its specific dependent variable (Garson, 2014; Starstedt, Ringle & Hair, 2016). Also important for formative factors, Andreev, Heart, Tsipi, Maoz, Hanan, Pliskin, and Nava (2009) stated, "The *contribution*

power of each of the explanatory constructs can be substantiated by calculating the weighted effect of the independent construct on the dependent one…" (p. 8). Therefore, inner model measurements were conducted for each specific factor against their respective behavioral intent variables but specifically for convergent validity and predictive performance. Supporting convergent validity results are reflected in Figures 4 – 13: Knowledge = 0.726; Self-efficacy = 0.707; Threat = 0.546; Norms = 0.885; and Penalties = 0.513 reflected acceptable convergence levels (e.g., path results above 0.5 required; Carlson & Herdman, 2010).

Also, results for relationship significance and effect strength for the individual factors: Knowledge, Self-efficacy, Threat, Norms, and Penalties, appear in the figures below. All path and t-score values demonstrated both significance and strength associations reflecting each factor – behavioral intent area supported the predictive value of the instrument. Specific values and interpretations appear below by factor area. Additionally, p values for all factor – behavioral intent constructs demonstrated 0.000 significance (with the exception of indicator 60 at 0.152). Outer weights and loadings for individual factor structural integrity appear in appendices D, E, F, G, and H.

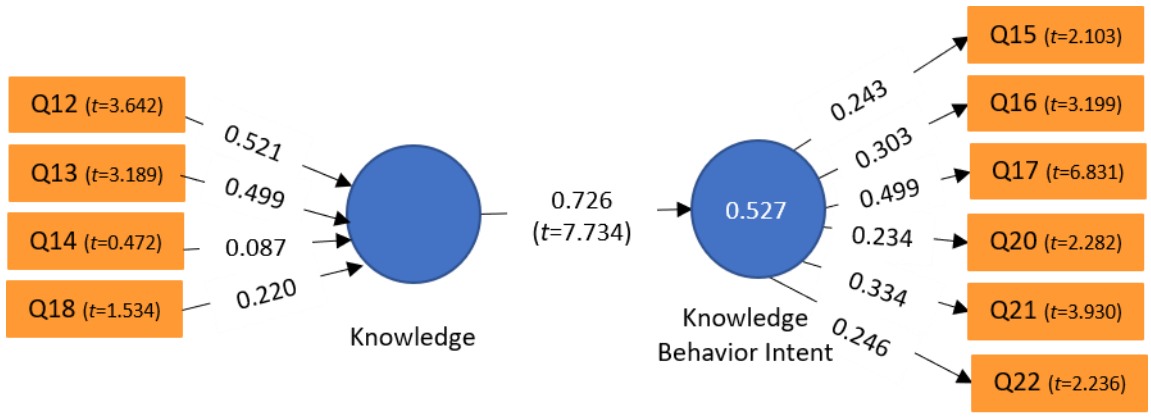
Knowledge

The path coefficient of 0.726 (Figure 4) indicates Knowledge has a significant effect on Knowledge Behavioral Intent ($p = 0.000$). While the R^2 of .527 (Chin, Marcolin, & Newstad, 2003) indicates almost 53% of the change in behavioral intent can be attributed to Knowledge factors. Additionally, an f^2 of 1.112 represented a large effect between factors. Additionally, the Knowledge – Knowledge Behavioral Intent assessment provided predictive assurance for effective IV- DV model design. Structurally, the impact of Knowledge on Knowledge Behavioral Intent was also significant in establishing convergent validity with the same path

coefficient of 0.726. The t-score of 7.734 substantiated path coefficient indications. Outer weights and loadings for Knowledge relationships (See Appendix C) demonstrated acceptable structural dynamics.

Figure 4

Knowledge Factor Analysis and Knowledge Behavioral Intent using Consistent PLS Algorithm and Consistent Bootstrapping

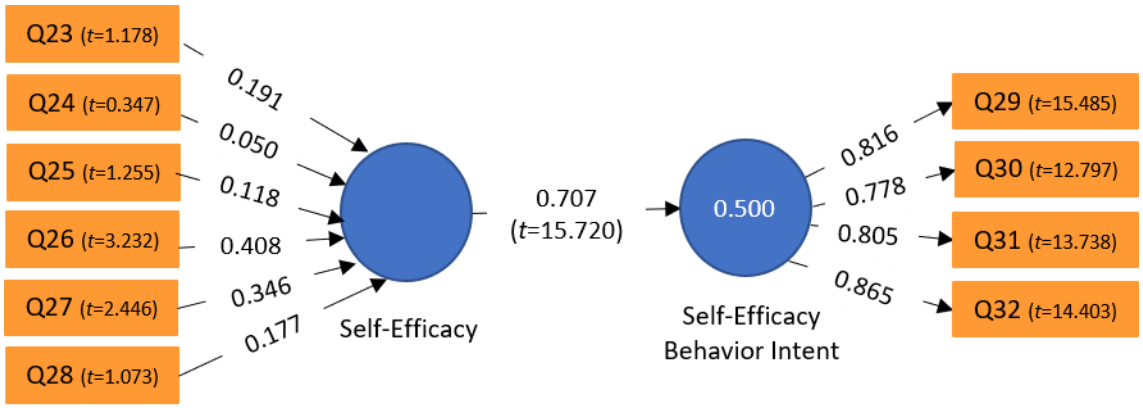


Self-efficacy

The Self-efficacy path coefficient of 0.707 and bootstrapped t-score of 15.720 (Figure 5) indicated Self-efficacy has a significant effect on Self-efficacy Behavioral Intent (p = 0.000) and establishes convergent validity for the construct. While the R^2 of .500 (Figure 5) indicated 50% of the change in behavioral intent can be attributed to Self-efficacy factors. Furthermore, an f^2 of 1.001 substantiated Self-efficacy's large effect on Behavioral Intent. Outer weights and loadings for Self-efficacy relationships (See Appendix D) demonstrated acceptable structural dynamics.

Figure 5

Self-efficacy Factor Analysis and Self-efficacy Behavioral Intent using Consistent PLS Algorithm and Consistent Bootstrapping

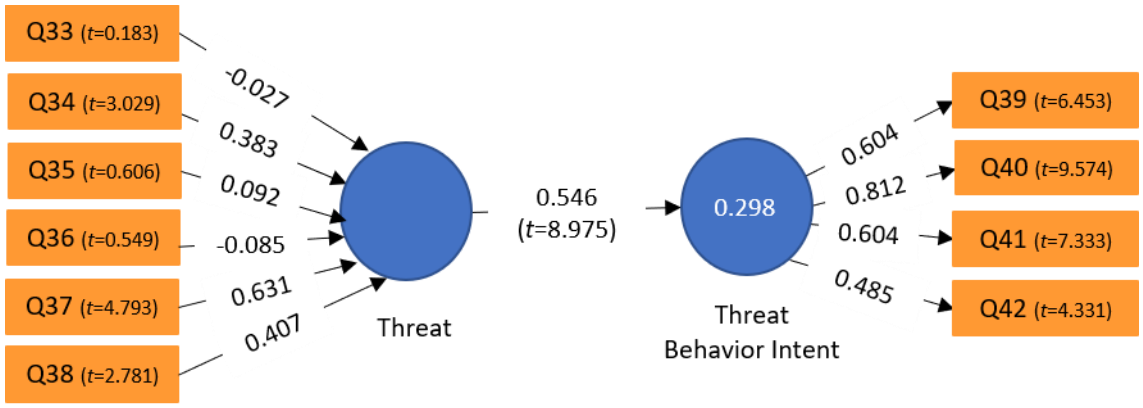


Threat

Threat results indicate a significant path coefficient of 0.546 and bootstrapped t-score of 8.975 (p = 0.000; Figure 6). Threat has a significant effect on Threat Behavioral Intent and convergence is not significant. While R^2 of .298 (Figure 6) indicates almost 30% of the change in behavioral intent can be attributed to Threat perception factors. However, Threat has only a small effect on Threat Behavioral Intent with an f^2 of 0.424. Finally, outer weights and loadings for Threat relationships (See Appendix E) demonstrated acceptable structural dynamics.

Figure 6

Threat Factor Analysis and Threat Behavioral Intent using Consistent PLS Algorithm and Consistent Bootstrapping

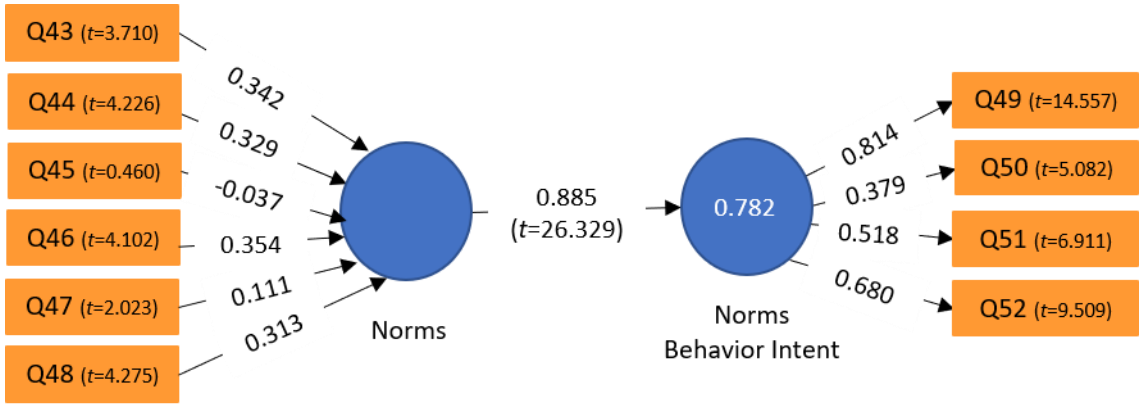


Norms

Norm results indicate a path coefficient of 0.885 and bootstrapped t-score of 26.329 (p = 0.000; Figure 7). Norms has the most significant effect on Normed Behavioral Intent among the factors studied. While an R^2 of .782 (Figure 7) indicates 78% of the change in behavioral intent can be attributed to normative factors. Effect size was also demonstrated with an f2 of 3.598. Furthermore, convergence concerns were not present as determined by the path coefficient. Finally, outer weights and loadings for Norm relationships (See Appendix F) demonstrated acceptable structural dynamics.

Figure 7

Norms Factor Analysis and Norms Behavioral Intent using Consistent PLS Algorithm

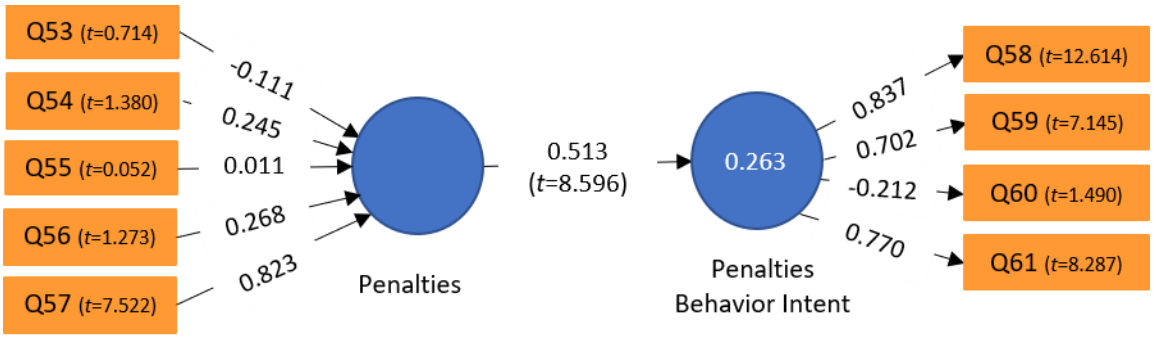


Penalties

Penalty results indicate a path coefficient of 0.513 and bootstrapped t-score of 8.596 (p = 0.000; Figure 8). The Penalties factor has a significant effect on Penalty Behavioral Intent. While the R^2 of .263 (Figure 8) indicates 26% of the change in behavioral intent can be attributed to the Penalties factors. Effect size confirmed a small effect on Penalty Behavioral Intent with an f2 of 0.357. Convergent validity was measured using the 0.513 path coefficient. Outer weights and loadings for Penalty relationships (See Appendix G) demonstrated acceptable structural dynamics.

Figure 8

Penalties Factor Analysis and Penalties Behavioral Intent using Consistent PLS Algorithm and Consistent Bootstrapping



Behavioral Intent Theoretical Support

The purpose of this research was to describe mental health practitioners' current cyber security practices and the behavioral intentions influencing a therapist's implementation of cyber security within clinical mental health settings. Behavioral intent involved establishing an understanding of the factors that influence a clinician's decisions when implementing cyber security within their clinical practice. Factors assessed in this research included knowledge, self-efficacy, norms, threat awareness and penalties and were selected based on previous theoretical studies. Research results provided insights into the understanding clinicians claim to have of required mandates and the factors influencing a clinician's behavioral intentions to conduct cyber security risk mitigation within their clinical practices. The impact of knowledge, self-efficacy, threat, norms, and penalties exert pressure on the behavioral intentions of practitioners to comply with legal and ethical requirements. Additionally, the results of this research support the model factors postulated to influence behavioral intent. Furthermore, the research model results reported here displayed general support for the theoretical precepts used to form earlier research model and theoretical constructs on behavior and motivation.

Open systems theory (OST) (Katz & Kahn, 1978) predicts that behavioral intentions are affected by an environmental awareness which was tested in the research model through assessment of clinician knowledge claims aligned with behavioral intent (actions to mitigate cyber security risk). While greater than 70% (Table 4, Questions 12 and 13) of clinicians stated they know federal and state legal requirements and more than 90% (Table 4, Question 14) practitioners reported they know ethical mandates (professional organization and peer expectations), answers to many behavioral questions displayed a significant misunderstanding in how to minimize privacy and confidentiality risk. For example, more than 78% (Table 4, Question 18) of practitioners stated that liability insurance alone will mitigate financial risk if sensitive information was lost. Yet, if practitioners do not also take other required actions mandated by ethics and law, insurers will most certainly claim mitigating factors themselves in refusing claims (not following the law relieves the insurance company of coverage responsibility). The resulting impact on clinicians may then range from loss of license to significant fines and other penalties. Furthermore, open systems theory proposes shared values and expectations as criteria impacting behavioral intent. While norms (alignment with professional organizations and/or colleagues) indeed showed the highest impact on behavioral intent within the study, and practitioners reported believing both professional organizations and our colleagues feel legal and ethical codes should be followed, only 41.9% (Table 4, Question 47) believe the established rules are being followed. Finally, OST also places emphasis on rule enforcement (measured through the significance of penalties in generating behavioral intent). When penalties were considered as a contributory factor within the composite model, penalties were shown to have no significant effect on behavioral intent (t-score 1.209; Figure 3).

Table 4

Open Systems Theory Support

Q12: Knowledge of federal Law				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	161	76.7	76.7	76.7
No	49	23.3	23.3	100.0
Total	210	100.0	100.0	
Q13: Knowledge of state Law				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	148	70.5	70.5	70.5
No	58	27.6	27.6	98.1
I don't know	4	1.9	1.9	100.0
Total	210	100.0	100.0	
Q14: Knowledge of ethical requirements				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	190	90.5	90.5	90.5
No	20	9.5	9.5	100.0
Total	210	100.0	100.0	
Q18: Liability insurance alone for risk mitigation				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	45	21.4	21.4	21.4
No	165	78.6	78.6	100.0
Total	210	100.0	100.0	
Q47: Others follow laws and ethics				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	45	21.4	21.4	21.4
No	165	78.6	78.6	100.0
I don't know	1	0.5	0.5	100.0
Total	210	100.0	100.0	

The TRIRISK model (Ferrer, Klein, Avishai, Jones, Villegas, & Sheeran, 2018) suggests reasoned judgement, feelings and experience impact behavioral intent. The knowledge of law and ethics and other model factors provides perspective around this area. Although clinicians report knowledge of legal and ethical requirements, mitigation measures for minimizing risk exposure are not often understood or applied effectively. In fact, when asked to identify all risk mitigation measures, approximately 1% (3 out of 210 respondents; Table 5) correctly selected all measures as important in minimizing risk (Accepting, Avoiding, Mitigating, and Transferring). Similarly, although not separately quantified, most mental health practices have not experienced a breach. Consequently, the experience of the consequences resulting from a compromise has not been felt.

Table 5

TRIRISK Model Support

Q19: All protective measures of sensitive digital information				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	3	1.4	1.4	1.4
No	207	98.6	98.6	100.0
Total	210	100.0	100.0	

Expansive learning theory (Engeström & Sannino, 2009) suggests that during times of significant change, disciplines may not be completely mastered. Results of the survey clearly demonstrated incomplete mastery of the requirements and implementation actions aligned with behavioral intent and risk mitigation. While more than 90% (Table 6, Question 15) of respondents indicated protecting digital information was inseparable from successful practice, clinicians also indicated attending to security takes time away from primary responsibilities (53.8%; Table 6, Question 60).

Table 6

Expansive Learning Theory Support

Q15: Protecting sensitive information				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	196	93.3	93.3	93.3
No	12	5.7	5.7	99.0
I don't know	2	1.0	1.0	100.0
Total	210	100.0	100.0	

Q60: Attention to security takes time				
	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	39	18.6	18.6	18.6
Somewhat agree	74	35.2	35.2	53.8
Neither agree nor disagree	43	20.5	20.5	74.3
Somewhat disagree	35	16.7	16.7	91.0
Strongly disagree	19	9.0	9.0	100.0
Total	210	100.0	100.0	

General deterrence theory (Lee, Lee, and Yoo, 2003) emphasizes actions in relation to penalties, yet the threat of enforcement consequence (e.g., fines, license impact) is significantly mitigated by the anticipation of risk. Only 34.3% (Table 7, Question 35) of practitioners believe a security violation would result in financial loss and only 24.8% (Table 7, Question 36) believe their practice may lose sensitive data if breached. In fact, 66.2% (Table 7, Question 38) of our colleagues believe the cyber security issue is exaggerated. Minimizing the likelihood of adverse action and the potential impact of a cyber security breach on a practice enables clinicians to avoid behaviors which would draw off resources (e.g., time, money, etc.) and if potentially undiscoverable (e.g., an undetected/unreported compromise), mitigating the initial risk of breach exposure - breaches have often remained unrecognized and consequently unreported for years.

Table 7

General Deterrence Theory Support

Q35: Violations result in losses				
	Frequency	Percent	Valid Percent	Cumulative Percent
Extremely likely	17	8.1	8.1	8.1
Somewhat likely	55	26.2	26.2	34.3
Neither likely nor unlikely	57	27.1	27.1	61.4
Somewhat unlikely	52	24.8	24.8	86.2
Strongly unlikely	29	13.8	13.8	100.0
Total	210	100.0	100.0	
Q36: Sensitive data loss in security violations?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Extremely likely	11	5.2	5.2	5.2
Somewhat likely	41	19.5	19.5	24.8
Neither likely nor unlikely	42	20.0	20.0	44.8
Somewhat unlikely	80	38.1	38.1	82.98
Strongly unlikely	36	17.1	17.1	100.0
Total	210	100.0	100.0	
Q38: Information security is exaggerated				
	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	2	1.0	1.0	1.0
Somewhat disagree	29	13.8	13.8	14.8
Neither agree nor disagree	40	19.0	19.0	33.8
Somewhat agree	63	30.0	30.0	63.8
Strongly agree	76	36.2	36.2	100.0
Total	210	100.0	100.0	

Social control theory (Lee, S. M., Lee, S., and Yoo, 2003) builds its' constructs on the effect of norms on behavioral intent. Again, in this research, results demonstrated the strength of norms on behavioral intent. Yet the inconsistencies addressed under open systems theory apply

to social control theory as well – while clinicians believe professional organizations and colleagues expect alignment with legal and ethical requirements (Table 8, Questions 45 and 46), they also believe others do not adhere to those requirements (Table 8, Question 47).

Table 8

Social Control Theory Support

Q45: Professional organization follows legal/ethical code				
	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	180	85.7	85.7	85.7
Somewhat agree	20	9.5	9.5	95.2
Neither agree nor disagree	8	3.8	3.8	99.0
Somewhat disagree	2	1.0	1.0	100.0
Total	210	100.0	100.0	
Q46: Colleagues follow laws and ethics				
	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	128	61.0	61.0	61.0
Somewhat agree	59	28.1	28.1	89.0
Neither agree nor disagree	18	8.6	8.6	97.6
Somewhat disagree	5	2.4	2.4	100.0
Total	210	100.0	100.0	
Q47: Others follow laws and ethics				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	88	41.9	41.9	41.9
No	121	57.6	57.6	99.5
I don’t know	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Control theory (Carver & Scheier, 1982) incorporates the idea of strong vs weak bonds within systems. The study included small practices through sole proprietorships yet even within small practices, practitioners are usually independent contractors vice employees of the practice. Consequently, while systems may be influenced by the norms established by the practice, and

practitioners claim that policies and procedures are enforced (94.8%; Table 9, Question 32), only 26.7% (Table 9, Question 21) of practices review security procedures and policies at least quarterly.

Table 9

Control Theory Support

Q21: Review of cyber security policies, processes, technologies				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	56	26.7	26.7	26.7
No	153	72.9	72.9	99.5
I don't know	1	0.5	0.5	100.0
Total	210	100.0	100.0	
Q32: Ensure policies are followed				
	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	157	74.8	74.8	74.8
Somewhat agree	42	20.0	20.0	94.8
Neither agree nor disagree	9	4.3	4.3	99.0
Somewhat disagree	1	0.5	0.5	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

The theory of planned behavior (Madden, Ellen & Ajzen, 1992) identifies an expectation of results as significant in determining behavioral intent. Recognition of the ability to effect results is partially a function of a practitioner's self-efficacy. This study showed that self-efficacy has a significant effect on behavioral intent and clinicians reported that even though they know the law requires actions to reduce the risk of data compromise, only 32.4% (Table 10, Question 17) have conducted a risk assessment within the last year and only 49.5% (Table 10, Question

25) report confidence in their ability to conduct the assessment. Finally, only 57.6% (Table 10, Question 34) of practitioners agreed that information security threats are controllable.

Table 10

Theory of Planned Behavior Support

Q17: Risk assessment				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	68	32.4	32.4	32.4
No	142	67.6	67.6	100.0
Total	210	100.0	100.0	
Q25: Confident about risk assessment				
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	104	49.5	49.5	49.5
No	106	50.5	50.5	100.0
Total	210	100.0	100.0	
Q34: Threats are controllable				
	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	19	9.0	9.0	9.0
Somewhat agree	102	48.6	48.6	57.6
Neither agree nor disagree	39	18.6	18.6	76.2
Somewhat disagree	44	21.0	21.0	97.1
Strongly disagree	6	2.9	2.9	100.0
Total	210	100.0	100.0	

Finally, risk homeostasis (West, 2008; Chronopoulos, Panaousis, & Grossklags, 2018) provides insights into behavioral intent through the concepts of risk tolerance and risk acceptance. The theory posits that greater belief in the security of the systems within a practice leads to greater complacency in establishing protections. As a function of belief in threat significance, the susceptibility of systems to compromise, and the potential impact of a breach practitioners will minimize behavioral intent in addressing potential compromise.

Misunderstanding the threat and the implications of cyber security lapses (24.8% believe a breach will result in the loss of data (Table 11, Question 36); 50.0% believe systems are susceptible to attack (Table 11, Question 33); 34.3% believe a compromise will result in financial loss (Table 11, Question 35) produces an ineffective approach to security policy, procedures, and action.

Although the theories employed in constructing the model for this research enabled significant context for factor development aligned to behavioral intent, there remains much additional motivational and behavioral perspective to be explored. While clinicians express a knowledge of law and ethics, their behavioral intents display emphasis based on three factor areas – norms, self-efficacy, and threat awareness (Figures 2 and 3). Yet based on the questions and responses explored above, inconsistencies appear in the assertions of knowledge and the implementation of security practices across Marriage and Family Therapists, Counselors, and Psychologists. These inconsistencies serve to attest to the complexity of predicting behavior based on specific theoretical models and compound the challenges of creating effective behavioral mitigation approaches.

Finally, several study limitations are noteworthy. First, surveys have been shown to be the least effective data gathering tool when populations feel their responses may reflect poorly on themselves or their profession. To mitigate associated risks in the data, the survey was anonymous and was promulgated across multiple different professional populations and areas of the country. However, even with those procedures in place, the predictive certainty of the study must be viewed as optimistic in terms of behavioral intent. Second, multiple attempts were made to connect with potential respondents from different populations resulting in 210 completed surveys. While that number provides insight into the knowledge and behavioral intent of

Table 11

Risk Homeostasis Support

Q33: Systems are susceptible to attack

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	34	16.2	16.2	16.2
Somewhat agree	71	33.8	33.8	50.0
Neither agree nor disagree	45	21.4	21.4	71.4
Somewhat disagree	42	20.0	20.0	91.4
Strongly disagree	18	8.6	8.6	100.0
Total	210	100.0	100.0	

Q35: Violations result in losses

	Frequency	Percent	Valid Percent	Cumulative Percent
Extremely likely	17	8.1	8.1	8.1
Somewhat likely	55	26.2	26.2	34.3
Neither likely nor unlikely	57	27.1	27.1	61.4
Somewhat unlikely	52	24.8	24.8	86.2
Strongly unlikely	29	13.8	13.8	100.0
Total	210	100.0	100.0	

Q36: Sensitive data loss in security violations

	Frequency	Percent	Valid Percent	Cumulative Percent
Extremely likely	11	5.2	5.2	5.2
Somewhat likely	41	19.5	19.5	24.8
Neither likely nor unlikely	42	20.0	20.0	44.8
Somewhat unlikely	80	38.1	38.1	82.9
Strongly unlikely	36	17.1	17.1	100.0
Total	210	100.0	100.0	

clinicians, results should only be viewed as representative of the larger professional community. Additionally, results should not be viewed as conclusive in regard to the broader professional community without confirmatory research. Third, while statistical data manipulation determined

correlations among data elements at required levels, inferring causative relationships would be premature.

Chapter V- Summary, Implications, & Recommendations

The questions posed in this research concern the current practices of clinicians and the factors which serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice? Consequently, the study was designed to identify the factors that affect the behavioral intent of clinicians in conducting cyber security within their practices as mandated by law and professional ethics guidance. The research was undertaken to provide insight into the factors which serve to influence a therapist's behavioral intentions to address the protection of sensitive information and systems in clinical practice. A researcher developed survey was created based on earlier general cyber security survey designs. Questions were developed to evaluate the effect of multiple motivational factors on behavioral intent based on several existing theoretical constructs. Factors were then assessed individually to determine formative and reflective relationships and in combination to determine the significance of the composite factors on behavioral intent.

Summary

The project consisted of a convenience sample of 210 Marriage and Family Therapists, counselors, and psychologists in private practice across various state and regional professional organizations. Survey links were advertised by the professional organization and anonymous results provided through Qualtrics. At the conclusion of the survey, respondents who submitted the finalized survey were provided an author created risk assessment template based on the National Institute of Standards and Technologies (NIST) generalized templates but tailored for mental health practitioner use.

Study results portray a pattern of incomplete knowledge for clinician's as they attempt to implement cyber security responsibilities within a practice. Although practitioners believe they

have the requisite knowledge to address cyber security, inconsistencies in understanding of implementation responsibilities to reduce confidentiality and privacy risk create gaps in protecting clients and practitioners. Clinicians also reported a lack of confidence in conducting required risk assessments, have little understanding or awareness of the threat, and fail to anticipate consequences for non-compliance behaviors. Furthermore, although clinicians anticipate professional organizations and colleagues expect compliance with laws and ethical mandates, clinicians also believe specified standards are not being followed. Finally, although clinicians reported awareness of penalties associated with a breach or audit, their behaviors did not reflect a true understanding of the severity of fines, or other consequences associated with failures to comply with established standards.

Several theories of motivation were used as the conceptual basis for question development and testing clinician behaviors. Notably the tenents of open systems theory, expansive learning theory, general deterrence theory, social control theory, control theory, the theory of planned behavior, risk homeostasis, and the TRIRISK model were supported through this research as applied to mental health clinicians in private practice although data analysis showed some inconsistencies in relation to theory application. Knowledge, self-efficacy, threat, norms, and penalties were identified as potential influencing factors in predicting the behavioral intentions of clinicians when adopting cyber security measures within their practice. While all indicators produced significant results against specific influencing factors aligned with specific factor behaviors, the effect of Norms on behavioral intent proved most significant. Of note, both Knowledge and Penalties revealed the least impact on their specific behaviors and were not significant when aligned against all behaviors. Specific questions (Appendix A) and associated frequency data (Appendix B) indicated disparities within clinician responses. Implications reflect

the potential that knowledge alone is insufficient to produce behavior changes while concerns over penalty enforcement may also be lacking. Conversely, when clinicians believe others engage in required security and privacy mandates, they may be more diligent in enacting their own protocols. Similarly, while self-efficacy is an important factor in initiating behaviors, threat awareness may only be significant as threat understanding increases. Finally, knowledge may create conditions which are necessary as a precursor for clinician action, but behavioral intent occurs only if aligned with other motivating factors.

Implications

Path coefficients, R^2, f^2, and t-scores demonstrated significant predictive results. However, this research also indicated a lack of actual knowledge as clinician behavioral intent often did not align with specific laws, guidelines, rules or best practices for protecting digital systems and information. Furthermore, a clinician's uncertain confidence in implementing cyber security within their practice may create additional barriers to completing required actions. For example, although risk assessments are required, many clinicians indicated they do not know how to perform the assessment (Appendix H, Question 25). Also, an incomplete understanding of threat dynamics may militate against effective action within a practice. Nevertheless, professional emphasis on privacy and confidentiality remains a constant for all mental health practitioners – psychologists, counselors, and marriage and family therapists. Of note, uncertainty surrounding the implementation of security standards and inconsistency in enforcement of mandated responsibilities also appeared to effect behaviors. For those who depend on specific standards to provide prescriptive direction vice general guidelines, implementation of required actions may be difficult. Likewise, if enforcement of required actions is inconsistent, practitioners may believe that weathering an inspection or a breach may be the preferred alternative.

Although knowledge of requirements appears to be a prerequisite in adoption of protective behaviors, the lack of ability to produce effective mitigation results coupled with a lack of threat awareness create gaps in the application of available risk mitigation measures. Additionally, consistency of professional messaging may contribute to lower levels of engagement behavior with regard to cyber security (e.g., when practitioners hear a minimizing message, they may also minimize the risk). Similarly, while experts provide insights into cyber law, ethics, threat, and mitigation opportunities, the material is often discussed in conjunction with other ethical responsibilities and consequently minimized in significance. Frequently, those providing instruction are not current in cyber security and treat it as a bolt-on to their ethics instruction, may not be current in the areas covered by the Health Insurance Portability and Accountability Act (HIPPA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Federal Trade Commission (FTC) regulations and ethical codes, or may misunderstand the extent of digital systems and information covered under the guidance.

Consequently, certification to provide ethics continuing education units (CEUs) may be insufficient to also provide cyber security awareness CEUs. Furthermore, our academic institutions could create a greater awareness of cyber security responsibilities by introducing courses on cyber security in clinical practice. Emphasis by the institutions that provide clinician training may establish a depth of awareness for clinicians into the responsibilities for confidentiality and privacy aligned to the use of digital systems in practice. Nevertheless, clinicians appear to take confidentiality and privacy responsibilities seriously and strive to provide environments that optimize security for their clients, their colleagues and themselves. Anecdotal evidence suggests that clinicians aligned as contractors to a private practice may believe confidentiality and privacy responsibilities accrue to the practice rather than remain

individual responsibilities. Other evidence suggests that practitioners may feel overwhelmed by therapeutic responsibilities themselves, time required to mitigate risk and align with legal and ethical requirements, and feel the resources expended will not create additional security. These misunderstandings of legal and ethical requirements may create a behavioral malaise which results in inaction when even minimal attempts to mitigate risk (e.g., conducting a risk assessment, establishing training for employees/clinicians, specifying security procedures in guidance documents, etc.) can produce valuable protections.

Recommendations

Awareness of cyber security responsibilities for mental health practitioners is key to establishing effective risk mitigation practices. In that regard, education and training are important strategies for advancing protections in addressing cyber security in mental health. That education could be advanced during master's degree and/or doctoral programs by introducing specific ethical blocks dealing with cyber security (e.g., how to conduct a risk assessment, etc.). Additionally, continuing education could be enhanced by requiring cyber security training aligned to development of threat awareness, understanding requirements for a practice vice unnecessary uses of technologies, and methods to accept, avoid, mitigate and transfer risk. These approaches could be assessed in comparison to privacy and confidentiality as specified through law and ethical guidelines to mitigate risk at all levels - client, clinician, and associated professionals. Additionally, professional organizations and/or licensing boards could become significantly more engaged in ensuring specific standards are developed and enforced. While federal agencies have the authority to perform audits of cyber security for covered entities, professional organizations and licensing boards could easily adopt approaches to ensure minimum requirements have been met. Requiring a risk assessment to be submitted along with

licensing documentation would be a start. Also, adopting cyber security compliance presentations at state and national conferences could advance awareness and help create insights into security trends and legal or ethical changes. Furthermore, journal articles providing topical insights may provide added exposure to current best practices and normed behaviors.

Finally, a thought process that suggests there is safety in numbers and the likelihood of a breach is remote, fails to acknowledge the legal and ethical responsibilities of our profession. Education, training, expectations of others, and the threat of sanctions may not serve to compel behavioral change. Rather, recognition of our responsibilities to our clients, colleagues and ourselves may remain the basis for effective cyber security. Motivation for change is enacted when individuals recognize patterns of behavior as ineffective in creating desired conditions. To establish an awareness of the need for change, professionals may need to examine their current approaches and balance effective action with the resources available. Yet commitment (Locke, 1996) to re-evaluating current action requires an ongoing effort to align behavior with values – not accepting all risk as a foregone conclusion.

Future studies

This research provided preliminary perspectives into the factors that influence a clinician's cyber security behaviors for privacy and confidentiality within clinical practice. However, additional research could be conducted to identify the effect of other factors on behavioral intent. Also, confirmatory research could be undertaken to verify findings produced in this study. Similarly, insights into normed behavior suggested the largest effect on clinician behaviors and yet a substantial number of clinicians reported not anticipating their colleagues were actually following legal and ethical mandates (Appendix H, Question 47). Therefore, future research could also be initiated to assess inconsistencies in the results observed here. Finally, qualitative

and mixed methods approaches may reveal additional insights into factors effecting behaviors. Specific populations could then be considered along with other approaches to influence behavior that align mandates with action (Locke, 1996; Herath and Rao, 2009). Follow-on research associated with this study will include a qualitative study to investigate additional clinician awareness factors contributing to behavioral intent. Further research associated with this study will address the potential expansion of model parameters to test behavioral contributing factors and the effectiveness of recommended changes in education, continuing education approaches, and professional organization involvement in rule enforcement.

References

45 CFR § 160.103 - Definitions. (n.d.). Retrieved January 26, 2020, from https://www.law.cornell.edu/cfr/text/45/160.103Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 236-247. doi:10.1080/0144929x.2012.708787

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior1. *Journal of Applied Social Psychology, 32*(4), 665-683. doi:10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I. (2002). Constructing a TpB Questionnaire: Conceptual and Methodological Considerations [PDF file]. Retrieved from https://pdfs.semanticscholar.org/0574/b20bd58130dd5a961f1a2db10fd1fcbae95d.pdf

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action Control,* 11-39. doi:10.1007/978-3-642-69746-3_2

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology, 40*(4), 471-499. doi:10.1348/014466601164939

Andreev, P., Heart, T., Maoz, H., & Pliskin, N. (2009). Validating formative partial least squares (PLS) models: Methodological review and empirical illustration. *ICIS 2009 Proceedings*. 193. https://aisel.aisnet.org/icis2009/193

Bandura, A. (1988). Organisational applications of social cognitive Theory. *Australian Journal of Management, 13*(2), 275-302. doi:10.1177/031289628801300210

Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association, 3*(2), 139-148. doi:10.1136/jamia.1996.96236282

Becker, J. M., Klein, K., & Wetzels, M. G. M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. *Long Range Planning, 45*(5-6), 359-394. doi:10.1016/j.lrp.2012.10.001

Boss, P. (1993). *Sourcebook of family theories and methods:* A contextual approach (pp. 332-368). New York: Plenum Press.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatories, control, and information security. *European Journal of Information Systems, 18*(2), 151-164. doi:10.1057/ejis.2009.8

Bruch, E., & Feinberg, F. (2017). Decision-Making processes in social contexts. *Annual Review of Sociology, 43*(1), 207-227. doi:10.1146/annurev-soc-060116-053622

Camp, L. J. (2006). Mental models of privacy and security. *SSRN Electronic Journal,* . doi:10.2139/ssrn.922735

Capeheart, L., & Milovanovic, D. (2007). *Social justice: Theories, issues, and movements*. New Brunswick, NJ: Rutgers University Press.

Carlson, K. D., & Herdman, A. O. (2010). Understanding the impact of convergent validity on research results. *Organizational Research Methods, 15*(1), 17-32. doi:10.1177/1094428110392383

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality-social, clinical, and health psychology. *Psychological Bulletin, 92*(1), 111-135. doi:10.1037//0033-2909.92.1.111

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*(2), 40-48. doi:10.1287/isre.14.2.189.16018

Chowdhury, F., Ferdous, S. (2017). Modelling cyber attacks. *International Journal of Network Security & Its Applications*, 9(4).

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An options approach to cybersecurity investment. *IEEE Access, 6*, 12175-12186. doi:10.1109/access.2017.2773366

Claar, Chester L. (2011). The adoption of computer security: An analysis of home personal computer user behavior using the health belief model. *All Graduate Theses and Dissertations.* Paper 878.

Conaty-Buck, S. (2017, September 26). *Cybersecurity and Healthcare Records.* My American Nurse. https://www.myamericannurse.com/cybersecurity-healthcare-records/

Denny, W. R. (2016, June 20). *Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act*. American Bar Association. https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_denny/

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers*. doi:10.1007/s10796-017-9774-y

Edemekong, P. F., & Haydel, M. J. (2019, June 18). *Health Insurance Portability and Accountability Act (HIPAA).* National Center for Biotechnology Information. https://www.ncbi.nlm.nih.gov/books/NBK500019/

Engestrom, Y. (2009). Studies of expansive learning: Foundations, findings and future challenges. *Studies in Expansive Learning,* 35-78. doi:10.1017/cbo9781316225363.004

Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. A., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46,* 541-562. doi:dx.doi.org/10.1016/j.jbi.2012.12.003

Ferrer, R. A., Klein, W. M., Avishai, A., Jones, K., Villegas, M., & Sheeran, P. (2018). When does risk perception predict protection motivation for health threats? A person-by-situation analysis. *Plos One, 13*(3). doi:10.1371/journal.pone.0191994

Fornell, C., & Larcker, D. (1981), Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18* (1), 39–50.

Fotinger, C. S., & Ziegler, W. (n.d.). *Understanding a hacker's mind: A psychological insight into the hijacking of identities* (Tech.). RSA Security.

Garson, D. G. (2014). *Partial least squares: Regression & structural equation models* (2016 ed.). Statistical Associates Publishing.

Goode, S., & Cruise, S. (2006). What motivates software crackers? *J Bus Ethics Journal of Business Ethics, 65*(2), 173-201. doi:10.1007/s10551-005-4709-9

Gregg, M. C. (2006). *Certified Ethical Hacker Exam Prep*. Pearson Certification.

Guterman, J. T., & Kirk, M. A. (1999). Mental health counselors and the internet. *Journal of Mental Health Counseling*, *21*(4), 309-325.

Hair, J. F., Jr., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (pls-sem). *European Business Review*, *26*(2), 106-121. doi:10.1108/ebr-10-2013-0128

Harpe, S. E. (2015) How to analyze Likert and other rating scale data. *Currents in Pharmacy Teaching and Learning*, 7(6), 836–850. doi:10.1016/j.cptl.2015.08.001.

Federal Trade Commission (2016, August 01) *Health information technology ("HITECH") provisions of american recovery and reinvestment Act of 2009, Title XIII, Subtitle D.* https://www.ftc.gov/enforcement/statutes/health-information-technology-hitech-provisions-american-recovery-and

Hecker, L. L., & Edwards, A. B. (2014). The impact of HIPAA and HITECH: New standards for confidentiality, security, and documentation for marriage and family therapists. *The American Journal of Family Therapy*, *42*(2), 95-113. doi:10.1080/01926187.2013.792711

Henseler, J., Ringle, C., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43(1),* 115–135. doi:10.1007/s11747-014-0403-8.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems Eur J Inf Syst, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Hoffman, S., & Podgurski, A. (2007). In sickness, health, and cyberspace: Protecting the security of electronic private health information. *Boston College Law Review, 43*(2), 331-385.

Howard, J. L., Jawahar, I. M. (2002). Risk management for small business. *Entrepreneurial Executive*, 7(11), 24-28.

Hussain, S., Fangwei, Z., Siddiqi, A., Ali, Z., & Shabbir, M. (2018). Structural equation model for evaluating factors affecting quality of social infrastructure projects. *Sustainability, 10*(5), 1415. doi:10.3390/su1005141

Hydari, M. Z., Telang, R., & Marella, W. M. (2015). Economic and business dimensions: Electronic health records and patient safety. *Communications of the ACM, 58*(11), 30-32. doi:10.1145/2822515

Jordan, N. A., Russell, L., Afousi, E., Chemel, T., Mcvicker, M., Robertson, J., & Winek, J. (2013). The ethical use of social media in marriage and family therapy: Recommendations and future directions. *The Family Journal, 22*(1), 105-112. doi:10.1177/1066480713505064

Katz, D., & Kahn, R. L. (1978). *The Social Psychology of Organizations*. New York: Wiley.

Kidwell, R., & Jewell, R. D. (2003). An examination of perceived behavioral control: Internal and external influences on intention. *Psychology and Marketing, 20*(7), 625-642. doi:10.1002/mar.10089

Kissel, R. (2006). *Glossary of key information security terms* (2nd ed.) (United States, U.S Department of Commerce, National Institute of Standards and Technology). doi:10.6028/NIST.IR.7298

Kobus, T. J., III (2015). *Data Breach Charts*. Rep. Cleveland: Baker & Hostetler LLP.

Kock, N. (2017). Structural equation modeling with factors and composites: A comparison of four methods. *International Journal of E-Collaboration, 13*(1), 1-9. doi:10.4018/ijec.2017010101

Kumar, M., & Wambugu, S. (2017). *A primer on the privacy, security, and confidentiality of electronic health records*. Chapel Hill, NC: Measure Evaluation, University of North Carolina.

Lee, S. M., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718. doi:10.1016/j.im.2003.08.008

Leonard, P. (2013). A revolution in code? Hari Kunzru's transmission and the cultural politics of hacking. *Textual Practice, 28*(2), 267-287. doi:10.1080/0950236x.2013.824501

Locke, Edwin A. (1996) Motivation through conscious goal setting. *Applied and Preventive Psychology*, *5*(2), 117–124., doi:10.1016/s0962-1849(96)80005-9.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication, 57*(2), 123-146. doi:10.1109/tpc.2014.2312452

Luxton, D. D., Mccann, R. A., Bush, N. E., Mishkind, M. C., & Reger, G. M. (2011). MHealth for mental health: Integrating smartphone technology in behavioral healthcare. *Professional Psychology: Research and Practice, 42*(6), 505-512. doi:10.1037/a0024485

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9. doi:10.1177/0146167292181001

Nikitina, Svetlana (2012). Hackers as tricksters of the digital age: creativity in hacker culture. *The Journal of Popular Culture 45*(1), 133-52. doi:10.1111/j.1540-5931.2011.00915.x.

Pardau, S. L., & Edwards, B. (2017). The FTC, the unfairness doctrine, and privacy by design: New legal frontiers in cybersecurity. *Journal of Business & Technology Law, 12*(2), 5

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4).

Recupero, P., & Rainey, S. E. (2005). Law and psychiatry: Forensic aspect of e-therapy. *Journal of Psychiatric Practice, 11*(6).

Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826. doi:10.1016/j.cose.2009.05.008

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2017). Partial least squares structural equation modeling. *Handbook of Market Research, 40*(1). doi:10.1007/978-3-319-05542-8_15-1

Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). Scientific knowledge of the human side of information security as a basis for sustainable trainings in organizational practices. *Proceedings of the 51st Hawaii International Conference on System Sciences*. doi:10.24251/hicss.2018.280

Secretary, H. O. (n.d.). HITECH Act Enforcement Interim Final Rule. Retrieved from http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Selznick, L., & LaMacchia, C. (2017). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law, 13*(2)

Smyslova, O., & Voiskounsky, A., (2009). "Usability studies: To meet or not to meet intrinsic motivation. *PsychNology Journal 7(3)*, 303-24.

Swan, D. (2016). Hacker Motivations and Mitigating Risk (Rep.). University of Maryland.

Swanson, M. (2001). *Security self-assessment guide for information technology systems.* National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-26/archive/2001-11-01

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(05), 571-588. doi:10.1142/s021848850200165x

Tschider, C. A. (2017). Enhancing Cybersecurity for the Digital Health Marketplace. *Annals of Health Law*, 26(1). 1-38.

United States, National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity (1.1st ed.).

United States, Department of Health and Human Services, The Office of the National Coordinator for Health Information Technology. (2015). *Guide to Privacy and Security of Electronic Health Information* (pp. 26-31).

United States, Federal Trade Commission, Bureau of Consumer Protection. (2010). *Complying with the FTC's health breach notification rule* (pp. 1-8).

Van Deursen, A., Van Dijk, J. (2010). Internet skills and the digital divide. *New Media & Society*, 13(6), 893-911. doi:10.1177/1461444810386774

Van Schaik, P. V., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior, 75*, 547-559. doi:10.1016/j.chb.2017.05.038

Vidalis, S., and Jones, A. (2005). Analyzing threat agents and their attributes. Technical Report: CS-05-04. Wales, UK: University of Glamorgan.

Vulnerability (computing). (2020, March 26). Retrieved July 25, 2016, from https://en.wikipedia.org/wiki/Vulnerability_(computing)

West, R. (2008). The psychology of security. *Communications of the ACM Commun. ACM, 51*(4), 34-40. doi:10.1145/1330311.1330320

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law & Society Review, 20*(4), 545. doi:10.2307/3053466

Wong, K. K. (2013). Partial least squares structural equation modeling (pls-sem) techniques using SmartPLS. *Computer Science, 24*(1).

Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. *The Academy of Management Review, 14*(3), 361. doi:10.2307/258173

Appendix A: Cyber Security in Mental Health Questionnaire

Demographics

Q2 Are you a licensed mental health professional?

Q3 Please identify your license category.

Q4 Please identify your geographic region:

Q5 Gender

Q6 Age

Q7 Highest Level of Education

Q8 Primary Employment Setting

Q9 Primary Employment Location

Q10 Number of Years in Practice

Q11 Number of Therapists in Practice

Knowledge

Q12 Knowledge of Federal law.

Q13 Knowledge of State law

Q14 Knowledge of Ethical requirements

Q18 Liability insurance

Knowledge Behavioral Intent

Q15 Protecting sensitive information

Q16 Risk of compromise

Q17 Risk assessment

Q18 Liability insurance alone for protection

Q19 All protective measures of sensitive digital information

Q20 Reduce the risk of compromise

Q21 Review of cyber security policies, processes, technologies

Q22 Knowledge of HIPAA, HITECH, FTC, state laws and ethical guidelines.

Self-efficacy

Q23 Confident in my skills

Q24 Confident in designing policies and processes

Q25 Confident about risk assessments

Q26 I can make a difference

Q27 Confident in implementing protections

Q28 Confident in reducing risks

Self-efficacy: Behavioral Intent

Q29 Attention to cyber security

Q30 Steps to ensure security

Q31 Steps to mitigate a breach

Q32 Ensure policies are followed

Threat

Q33 Systems are susceptible to attack

Q34 Threats are controllable

Q35 Violations result in losses

Q36 Sensitive data loss in security violations

Q37 Information security affects my practice

Q38 Information security is exaggerated

Threat: Behavioral Intent

Q39 Understanding capabilities of attackers

Q40 Information security inseparable from practice

Q41 Threat actor motivations

Q42 Awareness of the threats

Norms

Q43 I care about laws and ethical guidelines

Q44 Aligning actions with law and ethical guidelines

Q45 Professional organization follows legal/ethical codes

Q46 Colleagues follow laws and ethics

Q47 Others follow laws/ethics

Q48 Aligning practices upholds professional commitments

Norms: Behavioral Intent

Q49 Compliance with the legal/ethical codes

Q50 Practice standards and peers.

Q51 Dedicating resources to information systems

Q52 I follow legal and ethical policies

Penalties

Q53 There are penalties

Q54 Security breaches have consequences

Q55 Productivity is threatened by incident

Q56 Profitability is threatened by incident

Q57 Understanding consequences of a breach

Penalties: Behavioral Intent

Q58 Reduce penalties

Q59 Resources reduce penalties

Q60 Attention to security takes time

Q61 Aligning security with laws and ethics

Q62 Professional alignment

Appendix B: Composite Statistics

Table B1

Composite Convergent Reliability Outer Loadings

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q12 Knowledge	0.842	0.805	0.092	9.143	0.000
Q13 Knowledge	0.897	0.861	0.072	12.481	0.000
Q14 Knowledge	0.628	0.584	0.191	3.291	0.001
Q15 Composite BHI	0.385	0.367	0.110	3.512	0.000
Q16 Composite BHI	0.175	0.171	0.086	2.038	0.042
Q17 Composite BHI	0.459	0.448	0.054	8.494	0.000
Q18 Knowledge	0.189	0.180	0.162	1.167	0.243
Q20 Composite BHI	0.308	0.300	0.114	2.718	0.007
Q21 Composite BHI	0.337	0.332	0.061	5.569	0.000
Q22 Composite BHI	0.526	0.517	0.084	6.250	0.000
Q23 Self-efficacy	0.742	0.724	0.084	8.875	0.000
Q24 Self-efficacy	0.765	0.749	0.071	10.725	0.000
Q25 Self-efficacy	0.669	0.659	0.060	11.080	0.000
Q26 Self-efficacy	0.734	0.721	0.074	9.925	0.000
Q27 Self-efficacy	0.866	0.846	0.050	17.145	0.000
Q28 Self-efficacy	0.753	0.732	0.081	9.351	0.000
Q29 Composite BHI	0.696	0.694	0.054	12.988	0.000
Q30 Composite BHI	0.695	0.697	0.057	12.250	0.000
Q31 Composite BHI	0.754	0.749	0.050	15.036	0.000
Q32 Composite BHI	0.746	0.737	0.056	13.439	0.000
Q33 Threat	-0.198	-0.191	0.112	1.770	0.077
Q34 Threat	0.531	0.507	0.122	4.356	0.000
Q35 Threat	0.328	0.314	0.124	2.640	0.008
Q36 Threat	-0.046	-0.047	0.157	0.293	0.770
Q37 Threat	0.763	0.763	0.091	8.367	0.000
Q38 Threat	0.632	0.609	0.114	5.525	0.000
Q39 Composite BHI	0.449	0.460	0.078	5.787	0.000
Q40 Composite BHI	0.567	0.568	0.061	9.225	0.000
Q41 Composite BHI	0.431	0.434	0.063	6.873	0.000
Q42 Composite BHI	0.654	0.650	0.063	10.408	0.000

Q43 Norms	0.742	0.730	0.007	10.529	0.000
Q44 Norms	0.809	0.805	0.059	13.805	0.000
Q45 Norms	0.467	0.459	0.098	4.769	0.000
Q46 Norms	0.648	0.639	0.067	9.647	0.000
Q47 Norms	0.346	0.342	0.064	5.437	0.000
Q48 Norms	0.680	0.672	0.074	9.227	0.000
Q49 Composite BHI	0.652	0.648	0.069	9.489	0.000
Q50 Composite BHI	0.219	0.219	0.075	2.941	0.003
Q51 Composite BHI	0.602	0.603	0.060	10.058	0.000
Q52 Composite BHI	0.645	0.631	0.075	8.615	0.000
Q53 Penalties	0.319	0.312	0.157	2.028	0.043
Q54 Penalties	0.405	0.444	0.128	3.508	0.000
Q55 Penalties	0.422	0.409	0.136	3.108	0.002
Q56 Penalties	0.518	0.501	0.117	4.431	0.000
Q57 Penalties	0.939	0.907	0.057	16.432	0.000
Q58 Composite BHI	0.647	0.649	0.052	12.365	0.000
Q59 Composite BHI	0.462	0.466	0.064	7.228	0.000
Q60 Composite BHI	-0.251	-0.240	0.077	3.270	0.001
Q61 Composite BHI	0.672	0.674	0.057	11.766	0.000

Table B2

Composite Convergent Reliability Outer Weights

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q12 Knowledge	0.403	0.388	0.180	2.237	0.025
Q13 Knowledge	0.558	0.543	0.180	3.102	0.002
Q14 Knowledge	0.224	0.192	0.243	0.920	0.358
Q15 Composite BHI	0.057	0.054	0.015	3.779	0.000
Q16 Composite BHI	0.026	0.025	0.013	2.051	0.040
Q17 Composite BHI	0.068	0.066	0.010	6.688	0.000
Q18 Knowledge	0.107	0.101	0.143	0.752	0.452
Q20 Composite BHI	0.045	0.043	0.015	3.053	0.002
Q21 Composite BHI	0.050	0.049	0.010	4.905	0.000
Q22 Composite BHI	0.077	0.076	0.010	7.537	0.000
Q23 Self-efficacy	0.174	0.166	0.151	1.148	0.251
Q24 Self-efficacy	0.052	0.060	0.145	0.357	0.721
Q25 Self-efficacy	0.216	0.213	0.096	2.256	0.024
Q26 Self-efficacy	0.380	0.377	0.112	3.402	0.001
Q27 Self-efficacy	0.439	0.424	0.115	3.827	0.000
Q28 Self-efficacy	0.037	0.032	0.142	0.261	0.794
Q29 Composite BHI	0.102	0.102	0.008	13.051	0.000
Q30 Composite BHI	0.102	0.102	0.007	13.875	0.000
Q31 Composite BHI	0.111	0.110	0.008	13.624	0.000
Q32 Composite BHI	0.110	0.108	0.008	13.624	0.000
Q33 Threat	-0.151	-0.146	0.105	1.441	0.150
Q34 Threat	0.325	0.312	0.116	2.802	0.005
Q35 Threat	0.219	0.209	0.124	1.766	0.077
Q36 Threat	-0.206	-0.203	0.145	1.415	0.157
Q37 Threat	0.561	0.542	0.127	4.432	0.000
Q38 Threat	0.456	0.441	0.130	3.502	0.000
Q39 Composite BHI	0.066	0.067	0.010	6.379	0.000
Q40 Composite BHI	0.083	0.083	0.008	10.167	0.000
Q41 Composite BHI	0.063	0.064	0.009	7.183	0.000
Q42 Composite BHI	0.096	0.095	0.009	10.491	0.000
Q43 Norms	0.284	0.280	0.083	3.413	0.001

Q44 Norms	0.467	0.479	0.076	6.251	0.000
Q45 Norms	0.071	0.065	0.067	1.057	0.291
Q46 Norms	0.250	0.242	0.084	2.976	0.003
Q47 Norms	0.082	0.082	0.059	1.389	0.165
Q48 Norms	0.265	0.261	0.085	3.114	0.002
Q49 Composite BHI	0.096	0.095	0.008	12.117	0.000
Q50 Composite BHI	0.032	0.032	0.011	2.874	0.004
Q51 Composite BHI	0.089	0.089	0.011	8.033	0.000
Q52 Composite BHI	0.095	0.093	0.010	9.443	0.000
Q53 Penalties	-0.069	-0.060	0.164	0.418	0.676
Q54 Penalties	0.093	0.098	0.176	0.529	0.597
Q55 Penalties	0.057	0.050	0.156	0.366	0.715
Q56 Penalties	0.276	0.268	0.145	1.900	0.057
Q57 Penalties	0.866	0.828	0.085	10.132	0.000
Q58 Composite BHI	0.095	0.096	0.010	9.058	0.000
Q59 Composite BHI	0.068	0.069	0.011	5.920	0.000
Q60 Composite BHI	-0.037	-0.035	0.011	3.225	0.001
Q61 Composite BHI	0.099	0.099	0.008	11.921	0.000

Appendix C: Knowledge Statistics

Table C1

Knowledge Outer Loadings

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q12 Knowledge	0.877	0.851	0.070	12.585	0.000
Q13 Knowledge	0.861	0.835	0.069	12.475	0.000
Q14 Knowledge	0.521	0.502	0.154	3.385	0.001
Q15 Behavioral Intent	0.243	0.240	0.117	2.083	0.037
Q16 Behavioral Intent	0.303	0.292	0.095	3.209	0.001
Q17 Behavioral Intent	0.499	0.478	0.072	6.925	0.000
Q18 Knowledge	0.307	0.288	0.153	2.011	0.044
Q20 Behavioral Intent	0.234	0.235	0.108	2.168	0.030
Q21 Behavioral Intent	0.334	0.325	0.086	3.870	0.000
Q22 Behavioral Intent	0.246	0.249	0.111	2.211	0.027

Table C2

Knowledge Outer Weights

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q12 Knowledge	0.521	0.513	0.143	3.642	0.000
Q13 Knowledge	0.499	0.484	0.157	3.189	0.001
Q14 Knowledge	0.087	0.071	0.184	0.472	0.637
Q15 Behavioral Intent	0.253	0.239	0.103	2.453	0.014
Q16Behavioral Intent	0.315	0.304	0.106	2.969	0.003
Q17Behavioral Intent	0.518	0.497	0.076	6.804	0.000
Q18 Knowledge	0.220	0.209	0.143	1.534	0.125
Q20Behavioral Intent	0.243	0.239	0.097	2.505	0.012
Q21Behavioral Intent	0.347	0.334	0.075	4.599	0.000
Q22Behavioral Intent	0.256	0.246	0.098	2.620	0.009

Appendix D: Self-efficacy Statistics

Table D1

Self-efficacy Outer Loadings

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q23 Self-efficacy	0.752	0.730	0.084	8.920	0.000
Q24 Self-efficacy	0.754	0.734	0.074	10.199	0.000
Q25 Self-efficacy	0.606	0.594	0.064	9.473	0.000
Q26 Self-efficacy	0.769	0.750	0.081	9.496	0.000
Q27 Self-efficacy	0.839	0.819	0.065	12.858	0.000
Q28 Self-efficacy	0.809	0.791	0.070	11.613	0.000
Q29 Behavioral Intent	0.816	0.816	0.051	16.019	0.000
Q30 Behavioral Intent	0.778	0.785	0.060	13.010	0.000
Q31 Behavioral Intent	0.805	0.800	0.060	13.456	0.000
Q32 Behavioral Intent	0.865	0.848	0.056	15.552	0.000

Table D2

Self-efficacy Outer Weights

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q23 Self-efficacy	0.191	0.175	0.162	1.178	0.239
Q24 Self-efficacy	0.050	0.052	0.144	0.347	0.729
Q25 Self-efficacy	0.118	0.120	0.094	1.255	0.210
Q26 Self-efficacy	0.408	0.405	0.094	3.232	0.001
Q27 Self-efficacy	0.346	0.334	0.126	2.446	0.015
Q28 Self-efficacy	0.177	0.178	0.142	1.073	0.283
Q29 Behavioral Intent	0.289	0.292	0.025	11.719	0.000
Q30 Behavioral Intent	0.275	0.279	0.016	17.664	0.000
Q31 Behavioral Intent	0.285	0.285	0.015	19.349	0.000
Q32 Behavioral Intent	0.306	0.303	0.020	15.590	0.000

Appendix E: Threat Statistics

Table E1

Threat Outer Loadings

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q33 Threat	-0.068	-0.056	0.152	0.448	0.654
Q34 Threat	0.574	0.542	0.125	4.584	0.000
Q35 Threat	0.303	0.285	0.138	2.194	0.028
Q36 Threat	0.046	0.041	0.153	0.301	0.763
Q37 Threat	0.812	0.772	0.091	8.929	0.000
Q38 Threat	0.596	0.572	0.130	4.602	0.000
Q39 Behavioral Intent	0.604	0.604	0.094	6.419	0.000
Q40 Behavioral Intent	0.812	0.795	0.085	9.540	0.000
Q41 Behavioral Intent	0.604	0.601	0.084	7.173	0.000
Q42 Behavioral Intent	0.485	0.482	0.113	4.284	0.000

Table E2

Threat Outer Weights

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q33 Threat	-0.027	-0.015	0.146	0.183	0.855
Q34 Threat	0.383	0.365	0.126	3.029	0.002
Q35 Threat	0.092	0.081	0.151	0.606	0.544
Q36 Threat	-0.085	-0.083	0.155	0.549	0.583
Q37 Threat	0.631	0.605	0.132	4.793	0.000
Q38 Threat	0.407	0.387	0.146	2.781	0.005
Q39 Behavioral Intent	0.323	0.325	0.048	6.785	0.000
Q40 Behavioral Intent	0.433	0.426	0.050	8.700	0.000
Q41 Behavioral Intent	0.323	0.324	0.042	7.627	0.000
Q42 Behavioral Intent	0.259	0.258	0.057	4.582	0.000

Appendix F: Norms Statistics

Table F1

Norms Outer Loading

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q43 Norms	0.768	0.754	0.077	10.010	0.000
Q44 Norms	0.711	0.706	0.073	9.730	0.000
Q45 Norms	0.390	0.387	0.110	3.533	0.000
Q46 Norms	0.699	0.693	0.062	11.357	0.000
Q47 Norms	0.401	0.396	0.062	6.460	0.000
Q48 Norms	0.721	0.709	0.063	11.457	0.000
Q49 Behavioral Intent	0.814	0.809	0.053	15.270	0.000
Q50 Behavioral Intent	0.379	0.376	0.074	5.134	0.000
Q51 Behavioral Intent	0.518	0.519	0.076	6.803	0.000
Q52 Behavioral Intent	0.680	0.674	0.072	9.391	0.000

Table F2

Norms Outer Weights

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q43 Norms	0.342	0.337	0.092	3.710	0.000
Q44 Norms	0.329	0.328	0.078	4.226	0.000
Q45 Norms	-0.037	-0.037	0.081	0.460	0.645
Q46 Norms	0.354	0.353	0.086	4.102	0.000
Q47 Norms	0.111	0.106	0.055	2.023	0.043
Q48 Norms	0.313	0.306	0.073	4.275	0.000
Q49Behavioral Intent	0.458	0.457	0.032	14.231	0.000
Q50Behavioral Intent	0.213	0.214	0.043	4.985	0.000
Q51Behavioral Intent	0.292	0.292	0.038	7.721	0.000
Q52Behavioral Intent	0.383	0.380	0.029	13.368	0.000

Appendix G: Penalties Statistics

Table G1

Penalties Outer Loadings

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q53 Penalties	0.315	0.305	0.150	2.096	0.036
Q54 Penalties	0.551	0.529	0.136	4.058	0.000
Q55 Penalties	0.412	0.399	0.154	2.673	0.008
Q56 Penalties	0.524	0.508	0.136	3.842	0.000
Q57 Penalties	0.917	0.877	0.074	12.324	0.000
Q58 Behavioral Intent	0.837	0.826	0.068	12.246	0.000
Q59 Behavioral Intent	0.702	0.693	0.097	7.227	0.000
Q60 Behavioral Intent	-0.212	-0.200	0.149	1.425	0.154
Q61 Behavioral Intent	0.770	0.758	0.096	7.992	0.000

Table G2

Penalties Outer Weights

	Original Sample (0)	Sample Means (M)	Standard Deviation	T Statistics	P Values
Q53 Penalties	-0.111	-0.100	0.155	0.714	0.475
Q54 Penalties	0.245	0.235	0.177	1.380	0.168
Q55 Penalties	0.011	0.005	0.214	0.052	0.958
Q56 Penalties	0.268	0.267	0.211	1.273	0.203
Q57 Penalties	0.823	0.784	0.109	7.522	0.000
Q58 Behavioral Intent	0.414	0.411	0.033	12.545	0.000
Q59 Behavioral Intent	0.347	0.343	0.044	7.809	0.000
Q60 Behavioral Intent	-0.105	-0.103	0.074	1.411	0.159
Q61 Behavioral Intent	0.380	0.378	0.042	8.978	0.000

Appendix H: Frequency Table

Table H1

Frequencies

Q12: Knowledge of federal Law

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	161	76.7	76.7	76.7
No	49	23.3	23.3	100.0
Total	210	100.0	100.0	

Q13: Knowledge of state Law

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	148	70.5	70.5	70.5
No	58	27.6	27.6	98.1
I don't know	4	1.9	1.9	100.0
Total	210	100.0	100.0	

Q14: Knowledge of ethical requirements

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	190	90.5	90.5	90.5
No	20	9.5	9.5	100.0
Total	210	100.0	100.0	

Q15: Protecting sensitive information

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	196	93.3	93.3	93.3
No	12	5.7	5.7	99.0
I don't know	2	1.0	1.0	100.0
Total	210	100.0	100.0	

Q16: Risk of compromise

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	136	64.8	64.8	64.8
No	7	34.8	34.8	99.5
I don't know	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q17: Risk assessment

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	68	32.4	32.4	32.4
No	142	67.6	67.6	100.0
Total	210	100.0	100.0	

Q18: Liability insurance alone for protection

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	45	21.4	21.4	21.4
No	165	78.6	78.6	100.0
Total	210	100.0	100.0	

Q19: All protective measures of sensitive digital information

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	3	1.4	1.4	1.4
No	207	98.6	98.6	100.0
Total	210	100.0	100.0	

Q20: Reduce the risk of compromise

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	202	96.2	96.2	96.2
No	8	3.8	3.8	100.0
Total	210	100.0	100.0	

Q21: Review of cyber security policies, processes, technologies

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	56	26.7	26.7	26.7
No	153	72.9	72.9	99.5
I don't know	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q22: Knowledge of HIPPA, HITECH, FTC, state laws and ethical guidelines

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	144	68.6	68.6	68.6
Somewhat agree	55	26.2	26.2	94.8
Neither agree nor disagree	11	5.2	5.2	100.0
Total	210	100.0	100.0	

Q23: Confident in my skills

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	60	28.6	28.6	28.6
Somewhat agree	107	51.0	51.0	79.5
Neither agree nor disagree	20	9.5	9.5	89.0
Somewhat disagree	16	7.6	7.6	96.7
Strongly disagree	7	3.3	3.3	100.0
Total	210	100.0	100.0	

Q24: Confident in designing policies and processes

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	60	28.6	28.6	28.6
Somewhat agree	107	51.0	51.0	79.5
Neither agree nor disagree	20	9.5	9.5	89.0
Somewhat disagree	16	7.6	7.6	96.7
Strongly disagree	7	3.3	3.3	100.0
Total	210	100.0	100.0	

Q25: Confident about risk assessment

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	104	49.5	49.5	49.5
No	106	50.5	50.5	100.0
Total	210	100.0	100.0	

Q26: I can make a difference

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	132	62.9	62.9	62.9
Somewhat agree	64	30.5	30.5	93.3
Neither agree nor disagree	10	4.8	4.8	98.1
Somewhat disagree	3	1.4	1.4	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q27: Confident in implementing protective

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	71	33.8	33.8	33.8
Somewhat agree	92	43.8	43.8	77.6
Neither agree nor disagree	17	8.1	8.1	85.7
Somewhat disagree	24	11.4	11.4	97.1
Strongly disagree	6	2.9	2.9	100.0
Total	210	100.0	100.0	

Q28: Confident in reducing risk

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	92	43.8	43.8	43.8
Somewhat agree	85	40.5	40.5	84.3
Neither agree nor disagree	11	5.2	5.2	89.5
Somewhat disagree	21	10.0	10.0	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q29: Attention to cyber security

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	123	58.6	58.6	58.6
Somewhat agree	59	28.1	28.1	86.7
Neither agree nor disagree	21	10.0	10.0	96.7
Somewhat disagree	4	1.9	1.9	98.6
Strongly disagree	3	1.4	1.4	100.0
Total	210	100.0	100.0	

Q30: Steps to ensure security

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	153	72.9	72.9	72.9
Somewhat agree	42	20.0	20.0	92.9
Neither agree nor disagree	12	5.7	5.7	98.6
Somewhat disagree	1	0.5	0.5	99.0
Strongly disagree	2	1.0	1.0	100.0
Total	210	100.0	100.0	

Q31: Steps to mitigate a breach

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	158	75.2	75.2	75.2
Somewhat agree	36	17.1	17.1	92.4
Neither agree nor disagree	14	6.7	6.7	99.0
Somewhat disagree	1	0.5	0.5	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q32: Ensure policies are followed

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	157	74.8	74.8	74.8
Somewhat agree	42	20.0	20.0	94.8
Neither agree nor disagree	9	4.3	4.3	99.0
Somewhat disagree	1	0.5	0.5	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q33: Systems are susceptible to attack

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	34	16.2	16.2	16.2
Somewhat agree	71	33.8	33.8	50.0
Neither agree nor disagree	45	21.4	21.4	71.4
Somewhat disagree	42	20.0	20.0	91.4
Strongly disagree	18	8.6	8.6	100.0
Total	210	100.0	100.0	

Q34: Threats are controllable

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	19	9.0	9.0	9.0
Somewhat agree	102	48.6	48.6	57.6
Neither agree nor disagree	39	18.6	18.6	76.2
Somewhat disagree	44	21.0	21.0	97.1
Strongly disagree	6	2.9	2.9	100.0
Total	210	100.0	100.0	

Q35: Violations result in losses

	Frequency	Percent	Valid Percent	Cumulative Percent
Extremely likely	17	8.1	8.1	8.1
Somewhat likely	55	26.2	26.2	34.3
Neither likely nor unlikely	57	27.1	27.1	61.4
Somewhat unlikely	52	24.8	24.8	86.2
Strongly unlikely	29	13.8	13.8	100.0
Total	210	100.0	100.0	

Q36: Sensitive data loss in security violations?

	Frequency	Percent	Valid Percent	Cumulative Percent
Extremely likely	11	5.2	5.2	5.2
Somewhat likely	41	19.5	19.5	24.8
Neither likely nor unlikely	42	20.0	20.0	44.8
Somewhat unlikely	80	38.1	38.1	82.98
Strongly unlikely	36	17.1	17.1	100.0
Total	210	100.0	100.0	

Q37: Information security affects my practice

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	58	27.6	27.6	27.6
Somewhat agree	75	35.7	35.7	63.3
Neither agree nor disagree	42	20.0	20.0	83.3
Somewhat disagree	23	11.0	11.0	94.3
Strongly disagree	12	5.7	5.7	100.0
Total	210	100.0	100.0	

Q38: Information security is exaggerated

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	2	1.0	1.0	1.0
Somewhat disagree	29	13.8	13.8	14.8
Neither agree nor disagree	40	19.0	19.0	33.8
Somewhat agree	63	30.0	30.0	63.8
Strongly agree	76	36.2	36.2	100.0
Total	210	100.0	100.0	

Q39: Understanding capabilities of attackers

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	60	28.6	28.6	28.6
Somewhat agree	92	43.8	43.8	72.4
Neither agree nor disagree	43	20.5	20.5	92.9
Somewhat disagree	13	6.2	6.2	99.0
Strongly disagree	2	1.0	1.0	100.0
Total	210	100.0	100.0	

Q40: Information security inseparable from practice

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	116	55.2	55.2	55.2
Somewhat agree	75	35.7	35.7	91.0
Neither agree nor disagree	13	6.2	6.2	97.1
Somewhat disagree	6.0	2.9	2.9	100.0
Total	210	100.0	100.0	

Q41: Threat actor motivations

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	82	39.0	39.0	39.0
Somewhat agree	89	42.4	42.4	81.4
Neither agree nor disagree	34	16.2	16.2	97.6
Somewhat disagree	4	1.9	1.9	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q42: Awareness of threat

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	177	84.3	84.3	84.3
No	33	15.7	15.7	100.0
Total	210	100.0	100.0	

Q43: I care about laws and ethical guidelines

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	174	82.9	82.9	82.9
Somewhat agree	33	15.7	15.7	98.6
Neither agree nor disagree	3	1.4	1.4	100.0
Total	210	100.0	100.0	

Q44: Threat actor motivation

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	135	64.3	64.3	64.3
Somewhat agree	55	26.2	26.2	90.5
Neither agree nor disagree	16	7.6	7.6	98.1
Somewhat disagree	4	1.9	1.9	100.0
Total	210	100.0	100.0	

Q45: Professional organization follows legal/ethical code

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	180	85.7	85.7	85.7
Somewhat agree	20	9.5	9.5	95.2
Neither agree nor disagree	8	3.8	3.8	99.0
Somewhat disagree	2	1.0	1.0	100.0
Strongly disagree	76	36.2	36.2	100.0
Total	210	100.0	100.0	

Q46: Colleagues follow laws and ethics

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	128	61.0	61.0	61.0
Somewhat agree	59	28.1	28.1	89.0
Neither agree nor disagree	18	8.6	8.6	97.6
Somewhat disagree	5	2.4	2.4	100.0
Total	210	100.0	100.0	

Q47: Others follow laws and ethics

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	88	41.9	41.9	41.9
No	121	57.6	57.6	99.5
I don’t know	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q48: Aligning practice upholds professional commitments

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	155	73.8	73.8	73.8
Somewhat agree	46	21.9	21.9	95.7
Neither agree nor disagree	8	3.8	3.8	99.5
Somewhat disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q49: Compliance with the legal/ethical codes

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	179	85.2	85.2	85.2
Somewhat agree	21	10.0	10.0	95.2
Neither agree nor disagree	10	4.8	4.8	100.0
Total	210	100.0	100.0	

Q50: Practice standards and peer

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	99	47.1	47.1	47.1
Somewhat agree	64	30.5	30.5	77.6
Neither agree nor disagree	30	14.3	14.3	91.9
Somewhat disagree	14	6.7	6.7	98.6
Strongly disagree	3	1.4	1.4	100.0
Total	210	100.0	100.0	

Q51: Dedicating resources to information/stems

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	119	56.7	56.7	56.7
Somewhat agree	68	32.4	32.4	89.0
Neither agree nor disagree	19	9.0	9.0	98.1
Somewhat disagree	2	1.0	1.0	99.0
Strongly disagree	2	1.0	1.0	100.0
Total	210	100.0	100.0	

Q52: I follow legal and ethical policies

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	138	65.7	65.7	65.7
Somewhat agree	58	27.6	27.6	93.3
Neither agree nor disagree	10	4.8	4.8	98.1
Somewhat disagree	4	1.9	1.9	99.5
Total	210	100.0	100.0	

Q53: There are penalties

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	147	70.0	70.0	70.0
Somewhat agree	43	20.5	20.5	90.5
Neither agree nor disagree	16	7.6	7.6	98.1
Somewhat disagree	3	1.4	1.4	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q54: Security breaches have consequences

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	128	61.0	61.0	61.0
Somewhat agree	59	28.1	28.1	89.0
Neither agree nor disagree	18	8.6	8.6	97.6
Somewhat disagree	4	1.9	1.9	99.5
Strongly disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q55: Productivity is threatened by incidents

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	106	50.5	50.5	50.5
Somewhat agree	69	32.9	32.9	83.3
Neither agree nor disagree	20	9.5	9.5	92.9
Somewhat disagree	12	5.7	5.7	98.6
Strongly disagree	3	1.4	1.4	100.0
Total	210	100.0	100.0	

Q56: Profitability is threatened by incidents

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	96	45.7	45.7	45.7
Somewhat agree	75	35.7	35.7	81.4
Neither agree nor disagree	20	9.5	9.5	91.0
Somewhat disagree	14	6.7	6.7	97.6
Strongly disagree	5	2.4	2.4	100.0
Total	210	100.0	100.0	

Q57: Understanding consequences of a breach

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	71	33.8	33.8	33.8
Somewhat agree	93	44.3	44.3	78.1
Neither agree nor disagree	18	8.6	8.6	97.6
Somewhat disagree	20	9.5	9.5	96.2
Strongly disagree	8	3.8	3.8	100.0
Total	210	100.0	100.0	

Q58: Reduce penalties

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	132	62.9	62.9	62.9
Somewhat agree	60	28.6	28.6	91.4
Neither agree nor disagree	17	8.1	8.1	99.5
Somewhat disagree	1	0.5	0.5	100.0
Total	210	100.0	100.0	

Q59: Resources to reduce penalties

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	101	48.1	48.1	48.1
Somewhat agree	71	33.8	33.8	81.9
Neither agree nor disagree	29	13.8	13.8	95.7
Somewhat disagree	7	3.3	3.3	99.0
Strongly disagree	2	1.0	1.0	100.0
Total	210	100.0	100.0	

Q60: Attention to security takes time

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	39	18.6	18.6	18.6
Somewhat agree	74	35.2	35.2	53.8
Neither agree nor disagree	43	20.5	20.5	74.3
Somewhat disagree	35	16.7	16.7	91.0
Strongly disagree	19	9.0	9.0	100.0
Total	210	100.0	100.0	

Q61: Aligning security with laws and ethics

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly agree	139	66.2	66.2	66.2
Somewhat agree	51	24.3	24.3	90.5
Neither agree nor disagree	18	8.6	8.6	99.0
Somewhat disagree	2	1.0	1.0	100.0
Total	210	100.0	100.0	