U.S. Healthcare System's Electronic Health Records Security Threat Avoidance

Andualem Woldeyohannis
awoldeyohannis6256@ucumberlands.edu
University of the Cumberlands
School of Computer and Information Sciences
6178 College Station Drive, Williamsburg, KY 40769

Mary Lind
mary.lind@lsus.edu
Louisiana State University Shreveport
College of Business
1 University Drive
Shreveport, LA USA

Abstract

Security breaches of the U.S. healthcare system's electronic health records (EHRs) present a critical challenge in healthcare. Current literature indicates that healthcare professionals' poor cybersecurity behaviors are the leading cause of data breaches in the U.S. healthcare system. Using technology threat avoidance theory, this non-experimental quantitative correlational study aimed to determine to what extent U.S. healthcare professionals' perceived susceptibility, perceived severity, safeguard effectiveness, safeguard cost, self-efficacy, and threat perceptions of EHRs security breaches influenced their threat avoidance motivations and threat avoidance behaviors while using EHRs. The research findings indicated that perceived severity and perceived susceptibility significantly correlate with a user's threat perception. The cost of safeguarding measures and the user's self-efficacy were predictors of healthcare professionals' threat avoidance motivation. Perceived threat and safeguarding effectiveness were not proven to affect avoidance motivation significantly. Avoidance motivation strongly predicted healthcare professionals' EHRs security breach threat avoidance behavior.

Keywords: Electronic Health Records; Technology Threat Avoidance Theory; Data Breaches, Perceived Threat, Avoidance Motivation

1. INTRODUCTION

This study focused on electronic health record (EHR) use in the U.S. healthcare system. Recent reports indicate that most EHR data breaches in the U.S. healthcare system are caused by human factors (Chua, 2021; Gioulekas et al., 2022; Yeng et al., 2022). As EHR adoption increases, the sector must adopt comprehensive cybersecurity practices to protect patients' data (Yeng et al., 2022). However, effective cybersecurity practices rely on understanding human factors (Gioulekas et al., 2022; Yeng et al., 2022).

Healthcare professionals' access to sensitive personal data when using EHRs highlights the need to account for the human element when developing healthcare IT cybersecurity infrastructure (Gioulekas et al., 2022). Yeng et al. (2022) argued that robust EHR cybersecurity requires a combination of technical safeguards and human behavioral interventions. Seminal threat avoidance scholars have suggested

perceptions of threat susceptibility influence threat awareness, which, in turn, affects motivation and threat avoidance behaviors (Liang & Xue, 2010). As a critical component of designing comprehensive cybersecurity solutions for U.S. healthcare organizations, it is essential to understand healthcare professionals' threat awareness, motivation, and avoidance behaviors (Carpenter et al., 2019; Yeng et al., 2022).

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act spurred the adoption of EHR systems across the United States (Colicchio et al., 2019). The primary purpose of the HITECH Act was to encourage healthcare providers to use information technology in a meaningful and secure way (HHS Office for Civil Rights, 2017). One result of the HITECH Act was to increase healthcare providers' adoption of EHR (Colicchio et al., 2019).

As EHR adoption increased, cybersecurity became an even more significant concern for healthcare organizations (Colicchio et al., 2019). The healthcare system has become the top target of cybercriminals (Gioulekas et al., 2022), and cyber threats to the healthcare system have constantly increased (Colicchio et al., 2019). The susceptible nature of patient information, the development of highly interconnected medical and health information technologies, and the prevalence of large databases of diverse health data make cybersecurity a priority in the healthcare industry (Ronquillo et al., 2018). EHR security threats include healthcare provider carelessness/negligence, phishing/ransomware, malicious insiders, and hacking/unauthorized access to EHRs.

2. THEORETICAL FRAMEWORK

Liang and Xue's (2009) Technology Threat Avoidance Theory (TTAT) served as the study's theoretical framework. TTAT explains individual IT users' malicious information technology threat avoidance behavior (Liang & Xue, 2009, 2010). TTAT is one of the most integrated and well-developed theories used to explain information technology users' behavior regarding the avoidance of cybersecurity threats based on cybernetic and coping theory. TTAT defines avoidance behavior as the result of two cognitive processes: threat appraisal and coping appraisal (Liang & Xue, 2009). In the threat appraisal process, individuals perceive an information technology threat if they believe they are susceptible to a technology threat that poses a severe risk (Liang & Xue, 2009). Coping appraisal develops from threat perception, where individuals assess the degree to which individual information technology threats can be avoided (Liang & Xue, 2009).

TTAT also theorizes that individuals assess safeguarding measures based on their perceived effectiveness, cost, and the individuals' ability to take action (i.e., self-efficacy; Liang & Xue, 2009). TTAT postulates that when users perceive information technology threats and believe they are avoidable, they are motivated to take appropriate measures to avoid the threat (Liang & Xue, 2009). If users do not think they can prevent the threat with safeguarding measures, they will engage in emotion-based coping (Liang & Xue, 2009).

The original TTAT model included eight constructs: (a) perceived susceptibility, (b) perceived severity, (c) perceived threat, (d) safeguard effectiveness, (e) safeguard costs, (f) self-efficacy, (g) avoidance motivation, and (h) avoidance behavior. This study used all the core constructs of the TTAT model to understand the human behavior effect of U.S. healthcare system EHRs' security threats. Perceived threat refers to an individual's belief that malicious information technology is dangerous or harmful (Carpenter et al., 2019). Healthcare professionals develop EHR threat perceptions by detecting potential dangers and monitoring the computing environment.

TTAT indicates that two antecedents shape threat perception: perceived susceptibility and perceived severity (Carpenter et al., 2019; Liang & Xue, 2009, 2010). This study used TTAT to understand the influence of U.S. healthcare professionals' EHR security threat awareness on their threat avoidance motivations. As breaches caused by carelessness, negligence, phishing, ransomware, and malicious insiders are the leading cause of U.S. healthcare system data breaches, studying threat awareness was central to understanding how to improve EHR security.

The other TTAT construct, avoidance motivation, represents an individual's intent to avoid a security threat (Carpenter et al., 2019; Liang & Xue, 2009, 2010). In TTAT, threat perception, shaped by susceptibility and severity, is directly linked to threat avoidance motivation, a critical factor in effective cybersecurity solutions (Carpenter et al., 2019). Avoidance motivation was used in this study as a dependent variable affected by threat perception, but avoidance motivation also functioned as an independent variable influencing avoidance behavior.

Avoidance behavior was used in this research to study EHR security in the U.S. healthcare system. Avoidance behavior refers to actions taken to prevent a security breach (Carpenter et al., 2019; Liang & Xue, 2009, 2010). The present study examined the correlation between avoidance motivations and avoidance behavior, with avoidance motivation being the independent variable and avoidance behavior being the dependent variable. As any security measure's goal is actual threat avoidance, it was essential to focus on behavioral outcomes rather than just behavioral intentions. In this regard, understanding the effect of healthcare professionals' security threat awareness on their threat avoidance motivation and behavior is critical in designing adequate cybersecurity best practices for healthcare professionals and U.S. healthcare organizations (Carpenter et al., 2019).

Technology Threat Avoidance Theory (TTAT)

This study used the TTAT to analyze the correlation between U.S. healthcare professionals' EHR security threat awareness and their motivation to avoid security threats. Threat avoidance motivation was also correlated to threat avoidance behavior. The TTAT enabled the study to explain better U.S. healthcare professionals' behavior in avoiding EHR security threats (Liang & Xue, 2009).

TTAT is one of the most integrated theories developed to explain individual users' information technology behavior in avoiding malicious IT threats (Liang & Xue, 2009, 2010) based on cybernetic theory and coping theory. The TTAT defines avoidance behavior as a dynamic behavior, a positive feedback behavior loop, in which to decide how to cope with information technology threats, users go through two cognitive processes, threat appraisal and coping appraisal (Liang & Xue, 2009). In the threat appraisal mental process, individuals will perceive an IT threat if they believe they are susceptible to an IT threat that poses a severe threat. Coping appraisal develops from threat perception, where individuals assess the degree to which information technology threats can be avoided. The coping appraisal of the theory included components from Lazarus's (1966) coping orientations to problems experienced (COPE) framework. Individuals then asses the safeguarding measures based on their perceived effectiveness, cost of safeguarding measures, and self-efficacy in taking the actions. TTAT postulates that when users perceive information technology threats and believe that the IT threat is avoidable by taking appropriate safeguarding measures, they are motivated to avoid it. TTAT also postulates that if users think they cannot avoid the perceived threat with the safeguarding measures, they will engage in coping focused on emotion (Liang & Xue, 2009).

From a theoretical perspective, TTAT is based on two theories, the process, and the variance theory. Coping techniques are the primary tool for malicious technology threat avoidance in both process and variance theories (Liang & Xue, 2009). As per the theories, the TTAT model contextualization depends on the process and the variance theory models.

3. THEORETICAL MODEL

The original TTAT model included eight constructs. The original TTAT theory model had perceived susceptibility, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, and avoidance behavior as constructs to understand human behavior under information technology threats (Liang & Xue, 2009). Liang and Xue (2010) used the TTAT model (see Figure 1) in their study to understand the U.S. healthcare system professionals' EHR security threat awareness and the effect on their threat avoidance motivation and behavior. As human factor-related breaches caused by carelessness/negligence, phishing/ransomware, and malicious insider are the leading cause of U.S. healthcare system EHR data breaches, the theory constructs enabled the study to understand the relationship between the U.S. healthcare system professionals' EHR security threat awareness to their motivation to avoid them.

Figure 1

Technology Threat Avoidance Model (TTAT)

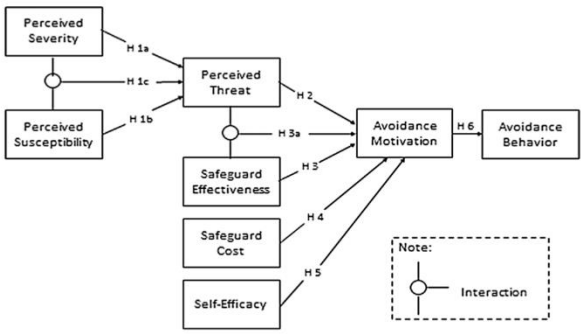

Figure 1 Note. Liang and Xue (2010). It is reprinted with permission.

Liang and Xue (2010) used TTAT to investigate personal computer users' information technology threat avoidance behavior by using safeguarding measures. The study tested a model developed from TTAT by using survey data. Consistent with the TTAT, they proposed that users' threat avoidance motivation is determined by their threat perception, which positively affects the user's threat avoidance behavior. The study also suggested that perceived severity, susceptibility, and interaction affect users' threat perception. In addition, the study hypothesized that avoidance motivation is directly determined by safeguard effectiveness, safeguard cost, and self-efficacy. The research results indicated that when individuals are threatened, they believe the safeguarding measures are effective (safeguarding effectiveness). They are confident in their self-efficacy with inexpensive safeguarding costs; they are more motivated to avoid the threat. The study also found negative interaction between avoidance motivation with perceived threat and safeguarding effectiveness, so when there is a higher perceived threat, there is a weaker relationship between safeguarding effectiveness and threat avoidance motivation, or on the other hand, when there is a high level of effective safeguarding measures, the weaker the relationship between perceived threat and the avoidance motivation. The study helped better understand the personal user's information technology threat avoidance behavior.

TTAT Constructs

Perceived severity is the first construct variable that predicts perceived threat and is the primary criterion variable of the avoidance behavior predictor variable. The perceived severity of a technology threat refers to an individual's subjective belief regarding the damage to their device and systems inflicted by malicious technology (Liang & Xue, 2009, 2010). Perceived severity measures to what extent an individual perceives the severity of the consequences of a malicious IT. The core of perceived severity correlation to a perceived threat is that users perceive that they are vulnerable to a threat and the threat consequence is severe (Liang & Xue, 2009). Falling to consider the vulnerability to a threat and its severity will lead to misunderstanding the threat perception. Alexandrou and Chen (2019) also described perceived severity as the degree to which an individual believes a compromised technology will have potential consequences. Young et al. (2016) and Carpenter et al. (2019) research results indicated that perceived severity is a strong indicator of perceived threat.

Perceived susceptibility is the second construct variable that predicts perceived threat and is the primary criterion variable of the avoidance behavior predictor variable. Perceived susceptibility to a technology threat refers to an individual's subjective belief that their device and system will likely be affected by a malicious technology (Liang & Xue, 2009). Alexandrou and Chen (2019) also define perceived susceptibility as an individual perception of how likely a threat to technology will occur. Liang and Xue (2009) indicated that research strongly supports perceived susceptibility to threat perception as positively correlated. Liang and Xue's (2010) study found a strong correlation between perceived susceptibility and threat. Alexandrou and Chen (2019) and Carpenter et al. (2019) also found that Perceived susceptibility positively impacts a perceived threat.

The interaction between perceived susceptibility and perceived security is a moderation phenomenon where perceived security positively moderates perceived susceptibility in the relationship between perceived susceptibility and perceived threat and vice versa (Liang & Xue, 2010). Both perceived susceptibility and perceived security, independently or together, influence an individual belief regarding the technology threat magnitude (Carpenter et al., 2019). As a function of perceived severity, the relationship between perceived severity and perceived threat can be seen as a positive relationship. The higher the perceived severity, the higher the relationship between perceived susceptibility and perceived threat (Alexandrou & Chen, 2019). The same logic works with the function of perceived susceptibility in the relationship between perceived severity and perceived threat. Liang and Xue's (2010) study found that although there is a positive effect of interaction between perceived susceptibility and perceived severity on the perceived threat, the correlation is not significant. Young et al. (2016) also found that the interaction effect of perceived susceptibility and perceived severity on a perceived threat is insignificant.

Perceived threat is the extent to which the individual understands malicious information technology as dangerous or harmful (Carpenter et al., 2019). Based on the cybernetic theory, a perceived threat indicates the users' current state's proximity to the undesired end state (Liang & Xue, 2009). Liang and Xue (2010) showed that threat perception is shaped by two antecedents: perceived susceptibility and perceived severity. According to Liang and Xue's TTAT model, threat perception outcome depends

on the threat's perceived severity, perceived susceptibility, and the safeguarding measure effectiveness available to cope with the IT threat. The main idea behind perceived threat in technology threat avoidance is that when an individual feels that the perceived threat increases, they are more inclined to apply security measures, such as following security measures seriously if they think there is too much phishing activity (Liang & Xue, 2009).

Safeguard effectiveness of TTAT influences avoidance motivation directly and interacts with a perceived threat. Safeguard effectiveness indicates the individual subjective assessment of how safeguarding measures can effectively be applied in protecting from technology threats (Liang & Xue, 2010). It is akin to the perception of outcome expectancy, which reflects the individual user's notion of objective outcome produced by using the safeguard measure (Liang & Xue, 2010). Individuals start the coping appraisal process after a threat is perceived to evaluate potential safeguarding measures. According to Liang and Xue (2010), individuals use safeguard effectiveness, safeguard cost, and self-efficacy to assess IT threat's avoidability.

The self-efficacy construct (end-users self confidence in using computers), an essential variable in avoidance motivation, indicates the user's confidence in taking the safeguarding measure (Liang & Xue, 2010). Liang and Xue (2010) showed that as users' self-efficacy increases, they are motivated to perform IT security behavior. In explaining the reasoning behind the inclusion of self-efficacy in their TTAT model, Liang and Xue (2010) demonstrated that in any given instance, self-efficacy and outcome beliefs would best predict threat avoidance behavior, including applying safeguarding measures such as turning off cookies, editing the computer registry file, installing antivirus software, and updating antivirus software are safeguarding measures. Many studies examining the relationship between self-efficacy and IT threat avoidance motivation indicated that end users are more motivated to apply safeguarding measures as their self-efficacy increases (Liang & Xue, 2009, 2010

Avoidance motivation indicates the intent to avoid a security threat that an individual believes to be a threat (Carpenter et al., 2019; Liang & Xue, 2009, 2010). In plain words, avoidance motivation in IT is the degree to which individual IT users are motivated to take safeguarding measures to avoid IT threats (Liang & Xue, 2009, 2010). Individuals' perception of a technology threat susceptibility, severity, and threat perception coupled with the safeguarding effectiveness, safeguarding cost, and self-efficacy determine an individual's threat avoidance motivation (Liang & Xue, 2009, 2010). According to Liang and Xue (2009), Maslow's hierarchy of needs indicates that the safety of one's property and resources is an individual basic human need; as such, IT users are motivated to avoid threats when they feel the threat will cause privacy and financial losses.

Individuals' understanding of susceptibility to a threat and its severity would lead to threat avoidance motivation and behavior, which is critical in designing effective cybersecurity solutions for both users and organizations (Carpenter et al., 2019). Individuals tend to increase their motivation to avoid a technology threat as the threat perception intensifies, and they believe the consequences of the threat outweigh the cost of the safeguarding measures. The study used the TTAT theory model to understand the correlation between perceived threat and avoidance motivation. The studies by Carpenter et al. (2019) and Liang and Xue (2010) showed a strong positive correlation between avoidance motivation and individuals' threat avoidance behavior.

Cybersecurity Threats in the Healthcare Systems

The healthcare industry is becoming more interconnected, making medical devices and clinical and business information electronically available 24/7 (Smith, 2018). EHRs are adopted across the United States healthcare system by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act (Ronquillo et al., 2018). The act increased the vulnerability of health I.T. Security, making it a growing concern for healthcare organizations (Ronquillo et al., 2018). The sensitive nature of patient information, including the availability of *Protected Health Information (PHI)* and *Personally Identifiable Information (PII),* makes cybersecurity a significant concern. The availability of PHI and PII, the development of highly interconnected medical and health information technologies, and the prevalence of large databases of diverse health data make cybersecurity a priority in the healthcare industry (Ayyagari, 2012).

Data Breaches in the U.S. Healthcare System

A data breach is unauthorized access and illegal disclosing information (Seh et al., 2020). The U.S.

health and human services define a health data breach as the illegal use or disclosure of confidential health information that compromises privacy or security under the privacy rule that poses a sufficient risk of financial, reputational, or other types of harm to the affected person (HHS, 2017). In addition to financial damage, data breaches cause tremendous reputation damage to healthcare organizations by lowering their trust level (Seh et al., 2020).

As EHR adoption increased, cybersecurity became an even more significant concern for healthcare organizations (Colicchio et al., 2019). The healthcare system has become the top target of cybercriminals (Gioulekas et al., 2022; Yeng et al., 2022), and cyber threats to the healthcare system have constantly increased (Colicchio et al., 2019). The susceptible nature of patient information, the development of highly interconnected medical and health information technologies, and the prevalence of large databases of diverse health data make cybersecurity a priority in the healthcare industry (Ronquillo et al., 2018). EHR security threats include healthcare provider carelessness/negligence, phishing/ransomware, malicious insiders, and hacking/unauthorized access to EHRs.

A variety of healthcare professionals handle EHRs. Human factors are the leading cause of data breaches in the U.S. healthcare system (Chua, 2021; Yeng et al., 2022). Thus, as doctors, nurses, administrative staff, and information technology workers access patient information, the potential security exposure of patients' health records increases. Poor human security practices cause most reported EHR breaches (Chua, 2021; Yeng et al., 2022). Yeng et al. (2022) indicated that unintentional insider threats cause more than twice the number of EHR breaches than external cyberattacks and theft with malicious intent. Yeng et al. cited phishing scams as the most common cause of breached patient records.

Enhancing Cybersecurity in the Healthcare

Maintaining the privacy, integrity, and accessibility of healthcare information and systems from internal and external threats should be the top priority of healthcare organizations. Several scholars have argued that the U.S. healthcare industry must develop a cybersecurity contingency plan that looks beyond the technical controls and includes human behavioral interventions to effectively protect sensitive patient data (Gioulekas et al., 2022; Yeo & Banfield, 2022). Healthcare organizations institute security policies to protect patient data. The Health Insurance Portability and Accountability Act (HIPPA) requires healthcare providers to use specified safeguards to protect the confidentiality, integrity, and availability of EHR that contain protected health information (CMS, 2021). Unfortunately, healthcare professionals fail to comply with EHRs' security policies for many reasons (Yeng et al., 2022). Yeng et al. (2022) suggested that healthcare professionals fail to comply with EHR security policies because they lack awareness of the severity of security threats.

4. RESEARCH FINDINGS

This nonexperimental, correlational, quantitative study aimed to determine the extent to which healthcare professionals' threat perceptions influenced their avoidance motivations and threat avoidance behaviors when using electronic health records (EHRs). The study filled a gap in the literature regarding U.S. healthcare professionals' perceptions of EHR security, threat avoidance motivations, and avoidance behaviors (Gioulekas et al., 2022; Yeng et al., 2022). The U.S. healthcare system faces significant EHR data security challenges due to healthcare professionals' poor understanding of security threats. Scholars have argued that improving healthcare professionals' understanding and awareness of security threats should be a core part of the U.S. healthcare systems' cybersecurity framework (Gioulekas et al., 2022; Yeng et al., 2022).

This study relied on the entire components of Liang and Xue's model constructs: perceived susceptibility, perceived severity, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior. The research examined nine research questions and corresponding sets of hypotheses to determine the extent of the relationships between healthcare professionals' perceptions of EHRs security threats, their motivations to avoid threats, and their threat avoidance behaviors when using EHRs. The hypotheses were as follows:

H_01. Perceived susceptibility does not significantly influence a U.S. healthcare professional's perceived threat when using EHRs.

H_a1. Perceived susceptibility significantly influences a U.S. healthcare professional's perceived threat when using EHRs.

H_02. Perceived severity does not significantly influence a U.S. healthcare professional's perceived threat when using EHRs.

H_a2. Perceived severity significantly influences a U.S. healthcare professional's perceived threat when using EHRs.

H_03. The interaction of perceived severity and perceived susceptibility does not significantly influence a U.S. healthcare professional's perceived threat when using EHRs.

H_a3. The interaction of perceived severity and perceived susceptibility significantly influences a U.S. healthcare professional's perceived threat when using EHRs.

H_04. Perceived threat does not significantly influence a U.S. healthcare professional's avoidance motivation when using EHRs.

H_a4. Perceived threat significantly influences a U.S. healthcare professional's avoidance motivation when using EHRs.

H_05. Safeguard effectiveness does not significantly influence a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_a5. Safeguard effectiveness significantly influences a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_06. The interaction of perceived threat and safeguard effectiveness does not significantly influence a U.S. healthcare professional's avoidance motivation when using EHRs.

H_a6. The interaction of perceived threat and safeguard effectiveness does not significantly influence a U.S. healthcare professional's avoidance motivation when using EHRs.

H_07. Safeguard cost does not significantly influence a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_a7. Safeguard cost significantly influences a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_08. Self-efficacy does not significantly influence a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_a8. Self-efficacy significantly influences a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_09. Avoidance motivation does not significantly influence a U.S. healthcare professional's threat avoidance behavior when using EHRs.

H_a9. Avoidance motivation significantly influences a U.S. healthcare professional's threat avoidance behavior when using EHRs.

Participants and Research Setting

The study's target population comprises healthcare professionals currently employed in U.S. healthcare organizations. The target population is inclusive and does not exclude or focus on any type of healthcare professional. The study involved participants above 18 years of age, and there was no exclusion based on gender, ethnicity, or health status. A total of N = 168 participants completed the survey. An a priori sample size calculation determined that a minimum of N = 166 participants were required to maintain a 95% confidence level to test the significance between the study's nine predictor variables. Thus, the sample size was adequate to test the hypotheses.

The sample was predominantly female, with males accounting for 29.8% of the sample. The sample's gender distribution was not considered an issue because the study was not focused on the potential moderating effects of demographic characteristics. The sample was evenly distributed by age. The largest age cohort (i.e., participants aged 31-35) represented 21.4% of the sample. The smallest age cohort (i.e., participants aged 61-65) represented only 4.2% of the sample. Participants' work experience ranged between less than five years and 25+ years. Most of the sample (73.2%) had six or more years of work experience.

Regression Assumption Tests

The instrument's reliability was tested following the mean, standard error, and standard deviation calculations. While Liang and Xue (2010) validated the instrument, Cronbach's alpha reliability coefficients were calculated to determine the reliability of the survey when used to collect data from U.S. healthcare professionals. A standard threshold of 0.70 was used as a baseline for acceptable reliability. Reliability of the constructs were in the .801 to .943 range. The reliability coefficient values were all higher than the coefficients reported by Tu et al. (2015). After the assumptions were tested (linearity,

independence of errors, homoscedasticity/homogeneity of variance, multicollinearity, and normality) and the data were determined to be suitable for multiple linear regression.

Based on the analysis, perceived susceptibility and perceived severity significantly influenced perceived threat. Safeguard cost and self-efficacy significantly influenced avoidance motivation, and avoidance motivation significantly influenced avoidance behavior.

Assessment of Hypotheses

The research questions' findings are discussed in this practical assessment of the research questions section. The results of each research question's alignment or difference from other scholarly published literature on the topic were discussed. In addition, unusual findings as well are discussed under each research question results discussion (Table 1).

Table 1

HQ	Variable Relationship	Null Result
1	Perceived susceptibility -> Perceived threat	Rejected
2	Perceived severity -> Perceived threat	Rejected
3	Perceived susceptibility/Perceived severity -> Perceived threat	Not Rejected
4	Perceived threat -> Avoidance motivation	Not Rejected
5	Safeguard effectiveness -> Avoidance motivation	Not Rejected
6	Perceived threat/Safeguard effectiveness -> Avoidance motivation	Not Rejected
7	Safeguard cost-> Avoidance motivation	Rejected
8	Self-efficacy -> Avoidance motivation	Rejected
9	Avoidance motivation -> Avoidance behavior	Rejected

Hypothesis one assessed perceived severity influence on U.S. healthcare professionals' perceived threat to security breaches while using EHRs. Based on the first regression model of the study, perceived susceptibility significantly influenced perceived threat. The model result indicated that as perceived susceptibility increased, perceived threat also increased (positive *b* value). The research finding supported Liang & Xue's (2010) finding that perceived susceptibility has a significant positive effect on perceived threat (β = .41, p < .01). The finding of the study also supported Carpenter et al. (2019) finding that showed both direct path from perceived susceptibility to a perceived threat (β = .18, ρ < 0.001), and indirect route from perceived susceptibility to perceived severity and then perceived threat, had a significant and positive effect on a perceived threat (β = .37, ρ < 0.001).

Hypothesis two, which investigated the relationship between perceived severity of security breaches and perceived threat, found perceived severity of security breaches while using EHRs positively affects perceived threat. The study finding supported Liang and Xue's (2010) finding of a strong positive relationship between perceived severity and perceived threat (β = .27, p < .01). On the other hand, the modified TTAT model by Carpenter et al. (2019), which correlated perceived susceptibility to perceived severity and then to a perceived threat, found perceived severity partially influences perceived threat.

Hypothesis three assessed the interaction effect of perceived severity and perceived susceptibility to U.S. healthcare professionals' perceived threat to security breaches while using EHRs. The study result did not find a significant relationship. The study results supported Liang and Xue's (2010) finding that correlation between perceived susceptibility and perceived severity of a security breach while using EHRs does not have a significant interaction effect on the perceived threat (β = .10, p > .05). Previous studies that tested the full TTAT model found differing outcomes on different hypotheses, including the interaction effect of perceived susceptibility and perceived severity on the perceived threat (Chen & Zahedi, 2016; Young et al., 2016).

Hypothesis four used the study model two to assess perceived threat influence on U.S. healthcare professionals' security breaches and threat avoidance motivation while using EHRs. The study did not find a significant relationship between perceived threat and avoidance motivation. The correlation between perceived threat and avoidance motivation was one of the hypothesis test results that a significant relationship was expected based on prior study results, but it was not found. Liang and Xue (2010) found that perceived threat significantly determines avoidance motivation. The Liang and Xue (2010) study results indicated that perceived threat positively affects avoidance motivation (β

= .26, $p < .01$). Simple linear regression between perceived threat and avoidance motivation test showed a strong positive correlation between perceived threat and avoidance motivation. Carpenter et al. (2019) revised TTAT research model did not include the interaction effect of the perceived threat and safeguard effectiveness to avoidance motivation. They tested avoidance motivation with other independent variables, including perceived threat. However, without the inclusion of the interaction effect, Carpenter et al. (2019) found that perceived threat significantly determines perceived motivation ($\beta = .12$, $\rho < 0.01$). In the current research model two also, when the interaction between perceived threat and safeguard effectiveness was not included, the model result showed that all the independent variables, including perceived threat, have a significant positive relationship with avoidance motivation. Hence, the inclusion of the interaction effect in the model caused the model's results to be different from the expected. Chen and Zahedi (2016) study also supported the impact of perceived threat on avoidance motivation.

Hypothesis five of the study assessed safeguard effectiveness influence on U.S. healthcare professionals' threat avoidance motivation to security breaches while using EHRs. The current study results did not support this hypothesis. The correlation between safeguard effectiveness and avoidance motivation was another hypothesis question that the study was expecting a significant relationship based on previous studies but did not find. Liang and Xue (2010) study found avoidance motivation is significantly determined by safeguard effectiveness ($\beta = .33$, $p < .01$). Carpenter et al. (2019) also found safeguard effectiveness was significantly associated with avoidance motivation ($\beta = .41$, $\rho < 0.001$). However, Carpenter et al. (2019) revised TTAT model did not include the interaction effect of the perceived threat and safeguard effectiveness on avoidance motivation. To understand the cause of the unexpected result of model two, the Model 2 multi-regression test was done without including the interaction effect of the perceived threat and safeguard effectiveness. The regression model showed a strong positive correlation between avoidance motivation and safeguard effectiveness.

Hypothesis six was to what extent the interaction of perceived threat and safeguard effectiveness influences U.S. healthcare professionals' perceived threat avoidance motivation to security breaches while using EHRs. The perceived danger of EHRs security breaches interaction with safeguarding effectiveness of EHRs security has a negative interaction impact on avoidance motivation was the hypothesis of Liang and Xue (2009). The finding of Liang and Xue (2010) confirmed there is a significant negative ($\beta = -.18$, $p < .05$) interaction between perceived threat and safeguard effectiveness with avoidance motivation. The current study results also indicated a negative correlation between avoidance motivation and the interaction effect of the perceived threat and safeguard effectiveness. However, the interaction effect found was not significant. Carpenter et al. (2019) modified TTAT model did not include the interaction between perceived threat and safeguard effectiveness effect on avoidance motivation testing.

Hypothesis seven used Model 2 of the study to assess safeguard cost influences on U.S. healthcare professionals' threat avoidance motivation to security breaches while using EHRs. Safeguarding cost against EHRs security breaches negatively affects avoidance motivation, according to Liang and Xue's (2009) hypothesis. The current study results supported this hypothesis. Liang and Xue (2010) found out avoidance motivation is significantly determined by safeguard cost ($\beta = -.14$, $p < .05$), confirming their hypothesis. Carpenter et al. (2019) TTAT refined model also found safeguard cost significantly affects avoidance motivation cost ($\beta = -.33$, $\rho < 0.001$). The negative β values on both Liang and Xue (2010) and Carpenter et al. (2019) safeguard cost versus avoidance motivation shows that when the cost of safeguarding a threat increases, the avoidance motivation decreases, meaning people tend to accept the consequences of a threat to their security, rather than paying for the safeguarding measure. The study's results also confirmed a significant negative relationship between safeguarding cost and avoidance motivation. The significant correlation between safeguarding cost and avoidance motivation found in the current study makes safeguarding the cost of the TTAT model one of the constructs supported by all the prior TTAT-based research results reviewed by the researcher.

Hypothesis 8 analyzed by model two of the study was question eight, which assessed self-efficacy influences on U.S. healthcare professionals' threat avoidance motivation to security breaches while using EHRs. Self-efficacy in taking safeguard measures against EHRs security breaches positively affects avoidance motivation (Liang & Xue, 2010). The study results supported this hypothesis. Liang and Xue's (2010) study results showed avoidance motivation was

significantly determined by self-efficacy (β = .19, p < .05). Carpenter et al. (2019) result, however, did not support the hypothesis. Carpenter et al. (2019) result indicated that self-efficacy was not significantly associated with avoidance motivation (β = .03, p < 0.28). The current study results are aligned with Liang and Xue's (2010) findings and do not support the findings of Carpenter et al. (2019).

Hypothesis 9 assessed avoidance motivation influence on U.S. healthcare professionals' threat avoidance behavior to security breaches while using EHRs. Avoidance motivation of EHRs security breaches threats positively affects healthcare professionals' avoidance behavior while using safeguards (Liang & Xue, 2010). The study results supported the hypothesis. The independent variable of this hypothesis was avoidance motivation, and the dependent variable was avoidance behavior. The study by Liang and Xue (2010) found that avoidance motivation significantly influences avoidance behavior (β = .43, p < .01). In addition, Carpenter et al. (2019) and Arachchilage and Love's (2014) also found that avoidance motivation was highly positively associated with avoidance behavior (β = .82, p < 0.001), supporting the results of this study.

5. DISCUSSION AND IMPLICATIONS

Cybersecurity, by its nature, has a global effect and healthcare security breaches are not also different in their global nature. Considering such an effect, the current study has implications for future studies in expanding the scope of the target population globally instead of limiting it to the U.S. healthcare system. In line with the expansion of the target population sample, the study could also be used to expand the targeted healthcare professionals' sample group to include doctors and all other healthcare professionals handling patient healthcare information.

The study used Liang and Xue's (2010) TTAT model and instrument to answer the research questions. The model hypothesized the interaction of perceived susceptibility and perceived severity to predict perceived threat and the interaction of perceived threat and safeguard effectiveness to predict avoidance motivation. The integration of the interaction effect on the models affected the significance of the relationship on their respective dependent variables and the significance of other variables' impact on their dependent variables. Case in point, when the survey data of model 2 of the current research was tested without considering the interaction effect of the perceived threat and safeguard effectiveness against avoidance motivation, the model result showed a significant impact of all four constructs on avoidance motivation; however, with the inclusion of the interaction effect (current model design), perceived threat and safeguard effectiveness variables were not significant in their effect against avoidance motivation. In their refining TTAT research, Carpenter et al. (2019) did not consider the interaction effect of the perceived threat and safeguard effectiveness on threat avoidance motivation. Future research on further refining Liang and Xue's (2010) TTAT model and instrument would possibly produce a better TTAT model design regarding the interaction of constructs. As Carpenter et al. (2019) added additional variables in their refining TTAT study, the current study would have future implications of expanding the present study using more variables and developed models that could potentially result in a comprehensive prediction of the technology threat avoidance behavior in U.S. healthcare system security breaches.

Implication for Practice

The study examined U.S. healthcare system healthcare professionals' security breach threat avoidance behavior while using EHRs. As indicated earlier in the document, most security breaches in the U.S. healthcare system are related to or caused by human behavior mistakes. In this regard, U.S. healthcare organizations must incorporate human behavioral study considerations while implementing their security governance programs. The practical implication of the study will provide the necessary study output of healthcare professionals' security breach threat avoidance behavior while using EHRs.

U.S. healthcare organizations can use the study to understand the effect of human behavior on security breaches and make the necessary consideration while designing and implementing their centralized or decentralized IT security governance. Centralized security practices are implemented, controlled, and managed at the enterprise level, where healthcare professionals have no option of avoiding them. In centralized security systems, healthcare professionals' awareness of security breach threats of EHRs is essential as they would be targeted by email phishing-related security breach threats, which are the leading causes of data breaches in the U.S. healthcare system. In a decentralized security system, healthcare professionals engage in voluntary security breach protective measures, such as updating their own antivirus/ antispyware

software, enabling their firewall, and implementing HIPPA Security and Privacy measures while using electronic patient health records (ePHR). In decentralized IT security, healthcare professionals are more likely to engage in unsafe security behaviors and become a weak link for the healthcare organization's security system. For healthcare professionals in a decentralized security system, it is imperative to provide them with regular security awareness, education, and training to prepare them better to cope with security breach threats while using EHRs (Warkentin & Johnston, 2006).

The study's practical application in healthcare IT security programs extends in several ways. Most importantly, the study endorses the importance of healthcare professionals' security awareness, education, and training. Healthcare professionals would be more motivated to avoid security breach threats and opt to use safeguarding measures if these programs help them develop threat perception, with effective safeguarding measures with low safeguarding cost and high self-efficacy.

Summary

This non-experimental quantitative correlational study determined to what extent U.S. healthcare professionals' perceived susceptibility, perceived severity, safeguard effectiveness, safeguard cost, self-efficacy, and threat perceptions of EHRs security breaches influenced their threat avoidance motivations and threat avoidance behaviors while using EHRs. Technology threat avoidance theory served as the study's theoretical framework. Liang and Xue's (2010) TTAT model and validated survey instrument were used to collect a total of 168 respondents' survey data for the study's simple and multiple regression analysis. The research findings indicated that perceived severity and perceived susceptibility significantly correlate with a user's perception of threat. The cost of safeguarding measures and the user's self-efficacy were predictors of healthcare professionals' threat avoidance motivation. Perceived threat and safeguarding effectiveness were not proven to affect avoidance motivation significantly. Avoidance motivation strongly predicted healthcare professionals' EHRs security breach threat avoidance behavior. The study findings contribute significantly to understanding U.S. healthcare professionals' security breaches and threat avoidance behavior while using EHRs. The current study can be expanded and improved by testing TTAT more comprehensively, including other constructs like perceived avoidance, and developing and validating other TTAT models and instruments with the potential of better interaction among the constructs.

9. REFERENCES

Alexandrou, A., & Chen, L. C. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Security Journal*, 32(4), 410-434. https://doi.org/10.1057/s41284-019-00170-0

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Argaw, S. T., Bempong, N., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Medical Informatics and Decision Making,* 19. http://dx.doi.org/10.1186/s12911-018-0724-5

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

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 44. doi: 10.17705/1CAIS.04422

Chamroonsawasdi, K., Chottanapund, S., Pamungkas, R. A., Tunyasitthisundhorn, P., Sornpaisarn, B., & Numpaisan, O. (2020). Protection motivation theory to predict the intention of healthy eating and sufficient physical activity to prevent diabetes mellitus in Thai population: A path analysis. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 15(1), 121-127.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet security perceptions and behaviors: Poly-contextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205-222.

Chua, J. A. (2021). Cybersecurity in the healthcare industry. *Physician Leadership Journal*, 8(1).

CMS (2021). HIPPA Basics for Providers: Privacy, Security, & Breach Notification Rules. *The Medicare Learning Network,* MLN909001.

Colicchio, T. K., Cimino, J. J., & Fiol, G. D. (2019). Unintended Consequences of Nationwide Electronic Health Record Adoption: Challenges and Opportunities in the Post-Meaningful Use Era. *Journal of Medical Internet Research,* 2(6). https://doi.org/10.2196/13313

Coventry, L. & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, 113, 48-52. http://dx.doi.org/10.1016/j.maturitas.2018.04.008

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., & Marin, S. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*, 327. https://doi.org/10.3390/healthcare10020327

HHS Office for Civil Rights (2017). HITECH Act Enforcement Interim Final Rule. *U.S. Health and Human Services* https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

Lazarus, R. S. (1996). The role of coping in the emotions and how coping changes over the life course. In C. Magai & S. H. McFadden (Eds.), *Handbook of emotion, adult development, and aging* (pp. 289–306). Academic Press. https://doi.org/10.1016/B978-012464995-8/50017-0

Li, Q., Liu, Q., Chen, X., Tan, X., Zhang, M., Tuo, J,. & Zhu, Z. (2020). Protection motivation theory in predicting cervical cancer screening participation: A longitudinal study in rural Chinese women. Psycho-oncology, 29(3), 564-571.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.

Ronquillo, J. G., Winterholler, J. E., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. Oxford University Press on behalf of the American Medical Informatics Association, *JAMIA Open*, 1(1), 15–19.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). Plenum Press.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R. & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8, 133. https://doi.org/10.3390/healthcare8020133

Smith, C. (2018). Cybersecurity implications in an interconnected healthcare system. *Frontiers of Health Services Management*, 35(1), 37-40. http://dx.doi.org/10.1097/HAP.0000000000000039

Steen, M., & Steen, M. (2019). Health Care industry increasingly faces cybersecurity breaches. In I. Gonzales, K. Joaquin Jay, & Roger L. (Eds.), Cybersecurity: current writings on threats and protection. *McFarland*. Credo Reference: https://go.openathens.net/redirector/ucumberlands.edu?url=https%3A%2F%2Fsearch.credoreference.com%2Fcontent%2Fentry%2Fmcfccwotap%2Fhealth_care_industry_increasingly_faces_cybersecurity_breaches%2F0%3FinstitutionId%3D4309

Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial Intelligence and Cybersecurity: Past, Presence, and Future. *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, 1056.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52, 506-517. doi:10.1016/j.im.2015.03.002

ISSN: 2473-4901
v9 n6000

Warkentin, M. & Johnston, A. C. (2006). IT Security Governance and Centralized Security Controls, in Warkentin, M. and Vaughn, R. (Eds.) *Enterprise Information Assurance and System Security: Managerial and Technical Issues*, Hershey, PA: Idea Group Publishing, pp. 16-24.

Yeng, P. K., Fauzi, M. A. & Yang, B. A. (2022). Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. *Information*, *13*, 335. https://doi.org/10.3390/info13070335

Yeo, L. H. & Banfield J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspect Health Inf Manag*, 19(2).

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, 2(6), 1-17.