# ANALYZING THREAT PERCEPTIONS IN THE CONTEXT OF FITNESS DATA: REFINING THE THREAT CALCULUS IN TECHNOLOGY THREAT AVOIDANCE THEORY

by

Sara D. Boysen, B.A.

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Health Information Management
with a Major in Health Information Management
May 2018

Committee Members:

Alexander J. McLeod, Chair

David L. Gibbs

Barbara A. Hewitt

# FAIR USE AND AUTHOR'S PERMISSION STATEMENT

## Fair Use

## Duplication Permission

# DEDICATION

This thesis is dedicated to my family, whose support made it possible. You provided the encouragement and inspiration I needed to keep my eyes on the goal. To Karl, thank you for stepping in to fill both of our roles when needed, and for never making me feel like I was neglecting my responsibilities. Your encouraging words and unwavering support truly helped me get to the finish line. You always knew when I needed to hear “You’re doing a great job” or “I’m proud of you,” and didn’t hesitate to say it. To Hagan and Elijah, thank you for inspiring me to set a good example and for never begrudging me of this journey. I hope you will also learn to value and put forth the effort it takes to be successful once you set out to achieve a goal. I would also like to thank my parents and sisters for always being supportive, especially during this process.

## ACKNOWLEDGEMENTS

First, I am forever grateful to my thesis chair, Dr. Alex McLeod, for his support, guidance, and patience throughout this process. His encouragement helped me continue toward the goal when the task ahead seemed insurmountable. I especially appreciate his willingness to let me stop by for a “quick question” so I could continue making progress. I would also like to acknowledge my thesis committee members, Dr. Barbara Hewitt and Dr. David Gibbs, who provided timely feedback and suggestions that always helped improve the final product. Their keen eyes and research experience were always appreciated.

To the faculty in the Health Information Management department, the knowledge imparted to me throughout this program helped me grow as a student and pinpoint areas of research that interested me. Ms. Jackie Moczygemba, Dr. Tiankai Wang, Dr. Diane Dolezel, and Ms. Jennifer Teal, I am thankful to have had the opportunity to learn from such an outstanding group of intellectuals.

I would also like to acknowledge the College of Health Professions Dean, Dr. Ruth B. Welborn, who encouraged me throughout this journey. Her support was integral in helping me finally achieve this goal. Finally, I would like to recognize my fellow learners in this program, especially Samantha Banda, Tina King, and Melissa Walston-Sanchez. I am indebted to them for their support and for never hesitating to provide a listening ear, and I am grateful to know such kind and intelligent women. The bonds of friendship we developed throughout this program will surely last a lifetime.

# TABLE OF CONTENTS

**Page**

## LIST OF TABLES

**Table** **Page**

# LIST OF FIGURES

**Figure** **Page**

# ABSTRACT

The number of people using fitness devices and mobile health applications creates unprecedented amounts of health-related fitness data.  The data collected via these devices are not considered protected health information, therefore they are not provided the same legal protections.  In the absence of legal provisions, users are responsible for ensuring their data are safe from potential data breaches and malicious activities.

This study uses a revised Technology Threat Avoidance Theory (TTAT) model to analyze users' motivations to implement safeguarding measures aimed at protecting their health-related fitness data.  A revision was made to the threat calculus contained in the original TTAT model, and a privacy concerns construct was added as an antecedent to avoidance motivation.

Students at a large university responded to a survey instrument evaluating how they form their threat perceptions and other factors influencing avoidance motivations. Results supported the revised threat calculus in the TTAT model.  All of the original TTAT model constructs were upheld, except for safeguard cost.  The privacy concerns construct was not significant in predicting avoidance motivations.

# 1. INTRODUCTION

In recent years, products for tracking fitness and health-related data have inundated the wearable technology market. Moar's whitepaper, "Fitness Wearables: Time to Step Up" (2016), estimated by the year 2019 there will be over 110 million fitness device users globally. The whitepaper also estimated 130 million additional users will engage with their fitness data via smart watches. The acceptance and use of these new devices and mobile health applications generates an unprecedented amount of data related to individual health and fitness activities. This increase in data presents new opportunities for health information in the form of individual fitness data to be compromised via security breaches and other malicious activities (Barcena, Wueest, & Lau, 2014).

## User Perceptions

User perceptions regarding data generated by wearable technologies are critical when determining appropriate protections for health information. Personal data are increasingly vulnerable when collected via wearable technologies, because associated applications routinely share collected data with external entities without user consent (Ouyang, 2016). The absence of regulations and protections for health information collected via wearable fitness devices creates a prime opportunity for users to fall victim to malicious activities. How users perceive their data and the steps they take to protect their information play a key role in minimizing threats.

## Data Breach Potential

According to Yaraghi (2016), health information data hold a greater value for hackers, because highly sought after information such as legal names, birth dates, and social security numbers are typically contained in the health record. Unauthorized access to protected health information via interconnected systems provides the information needed to file fraudulent medical claims and receive unauthorized payments (Yaraghi, 2016). In a study conducted by Verizon in 2015, it was discovered that data breaches have compromised the protected health information of one out of two people in the United States (Widup, Bassett, Hylender, Rudis, & Spitler, 2015). While it has been determined that personal fitness data do not fit into the legal confines of protected health information, wearable technology applications collect many related data elements. For example, fitness applications often collect information such as users' full names, birthdates, mailing addresses, email addresses, and photographs (Barcena et al., 2014). In the absence of the protections provided by the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, and other regulations, it becomes the responsibility of users to take the necessary steps to protect their data.

With the burden of protecting fitness data falling to the user, it is essential to understand what motivates users to take protective actions. Researchers have used various theoretical models to analyze user motivations to adopt technologies or avoid threats. The two theories most commonly used are Protection Motivation Theory (Rogers, 1975) and Technology Threat Avoidance Theory (Liang & Xue, 2010). In Technology Threat Avoidance Theory, perceived severity and perceived susceptibility are key constructs for evaluating threat perceptions and predicting user avoidance behaviors.

## Purpose Statement

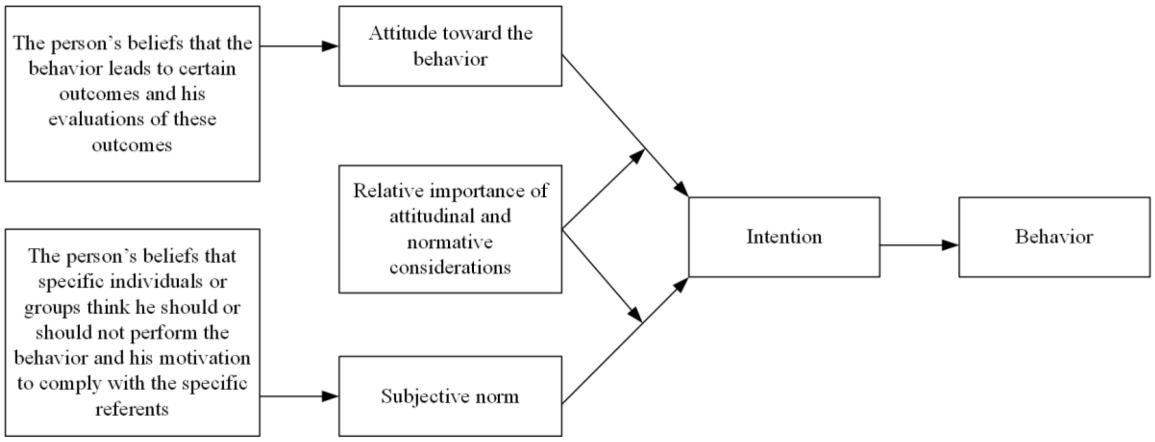
The purpose of this study was to examine the effect of perceived susceptibility on perceived threat, as mediated by perceived severity, and the resulting threat avoidance motivations and behaviors. An extension of the Technology Threat Avoidance Theory was used to examine how users behave in the presence of a threat, what motivates them, how they perceive and react to threats, and what safeguards, costs, and concerns influence those motivations and behaviors.

## 2. LITERATURE REVIEW

The model for this study was an extension of the Technology Threat Avoidance Theory (TTAT). In order to fully understand the key constructs that drive users to implement measures aimed at protecting their data collected via wearable fitness devices and avoid online threats, it is first crucial to understand the foundational theories for TTAT. These theories developed over time in a non-linear fashion and in many different contexts, with extensions of the theories tested across a variety of disciplines. Related theories include the Theory of Reasoned Action (Fishbein, 1979), Theory of Planned Behavior (Ajzen, 1985), Technology Acceptance Model (Davis, 1986), and Protection Motivation Theory (Rogers, 1975).

### Theory of Reasoned Action

Fishbein (1979) proposed the Theory of Reasoned Action (TRA) as a general framework to describe what causes individuals to develop intentions to perform behaviors. While Fishbein acknowledged behaviors generally align with intentions, he recognized the need to explain what leads to the development of individual intentions. TRA suggests that attitudes toward a behavior and subjective norms are mediated by intentions to predict behaviors. Fishbein observed the proliferation of theories that applied to narrow contexts, and proposed TRA in an attempt to provide a theoretical framework applicable to many contexts and across disciplines (Fishbein, 1979). Figure 1 details Fishbein’s Theory of Reasoned Action.


The person's beliefs that the behavior leads to certain outcomes and his evaluations of these outcomes
Attitude toward the behavior
Relative importance of attitudinal and normative considerations
The person's beliefs that specific individuals or groups think he should or should not perform the behavior and his motivation to comply with the specific referents
Subjective norm
Intention
Behavior

Note: Arrows indicate the direction of influence.

Figure 1 - The Theory of Reasoned Action (Fishbein, 1979)

As Fishbein expected, researchers have used TRA as the theoretical framework for various contexts, including coupon usage, infant-feeding intentions and behaviors, and health behaviors such as dietary choices and safe-sex practices (Albarracin, Johnson, Fishbein, & Muellerleile, 2001; Bagozzi, Wong, Abe, & Bergami, 2000; Fisher, Fisher, & Rye, 1995; Manstead, Proffitt, & Smart, 1983; Shimp & Kavas, 1984). Additionally, TRA has been used as the framework for predicting behaviors related to technology adoption (Karahanna, Straub, & Chervany, 1999; Mishra, Akman, & Mishra, 2014; Ramayah, Rouibah, Gopi, & Rangel, 2009; Rehman et al., 2007).

Karahanna et al. (1999) used TRA to describe information technology (IT) adoption behaviors within an organizational setting. Their study included two groups, users who had not yet adopted the technology and those who had already implemented it. Using these two groups, they examined pre-adoption intentions and the resulting behaviors as compared to the intention of current users to continue utilizing the technology. This work confirmed the ability of attitudes toward a behavior and subjective norms to predict behaviors, as mediated by intentions. However, they also found the relative importance of attitude versus subjective norm varied, dependent upon the participant’s pre-adoption and current usage status. Participants who had yet to adopt the IT were more influenced by subjective norms, while participants with experience using the IT tended to form their intentions and behaviors based on their attitudes toward the IT usage (Karahanna et al., 1999).

More recently, TRA was used to examine the adoption of “green” IT behaviors. Mishra et al. (2014) recognized the impact of IT on the environment, including the increase in power usage, disposal of outdated hardware, and the effect of manufacturers on the environment. Their study attempted to determine the attitudes and subjective norms that influence intentions and behaviors related to the adoption of green IT initiatives. This work supported the use of behavioral attitudes and social norms to predict intentions and actual behaviors. Therefore, individuals who had a positive attitude toward green IT behaviors and those who felt social pressure to implement those behaviors reported a higher intention to do so. Subsequently, they also adopted green IT behaviors at a higher rate (Mishra et al., 2014). While TRA initiated explanatory theories of intentions and behaviors, it required refinement and extension to improve understanding.

## Theory of Planned Behavior

Although TRA provided a theoretical framework in many contexts across multiple disciplines, researchers found that an additional construct would increase their ability to predict behaviors when individuals perceive there are factors beyond their volitional control (Ajzen, 1985). Thus, Ajzen proposed the Theory of Planned Behavior (TPB), an extension of TRA. TPB added perceived behavioral control as an integral construct for predicting intention and behavior. According to Ajzen, perceived behavioral control is defined as the individual's perception regarding the ability to perform the behavior. While individuals may have strong attitudes toward the behavior and feel social pressure to perform the behavior, they will also factor in the ability to do so considering external barriers beyond their control. Ajzen suggested that perceived behavioral control might have a direct relationship with intention and actual behavior (Ajzen, 1985). Figure 2 illustrates the TPB framework.

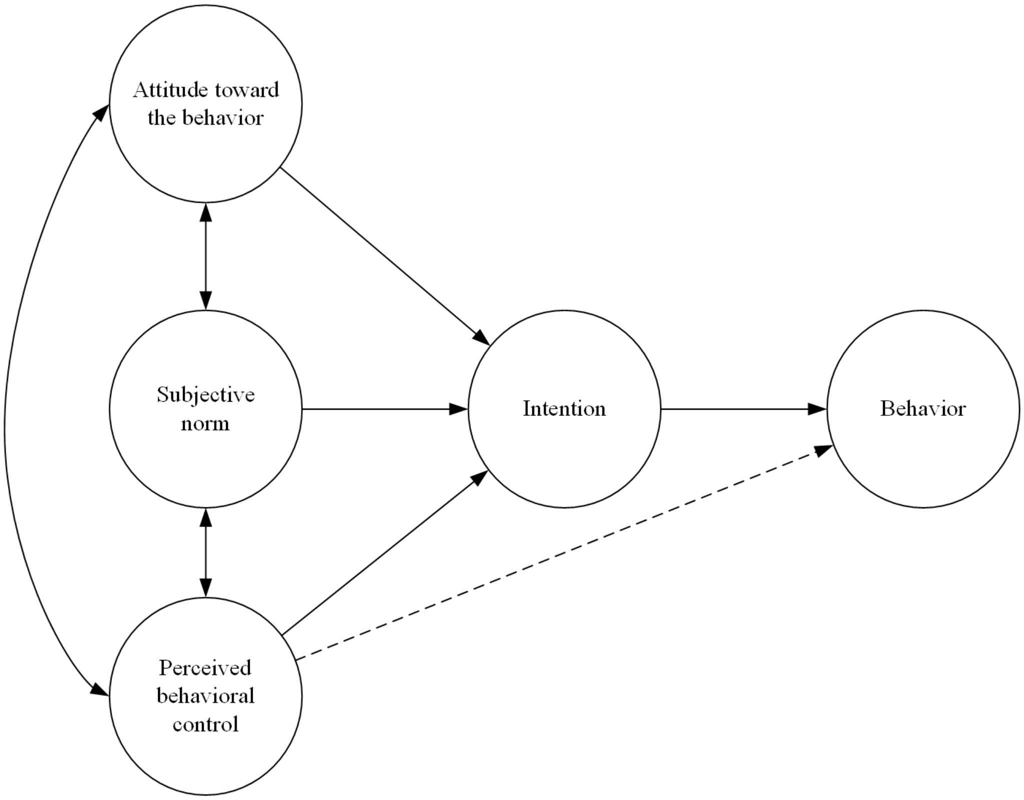


Figure 2 - The Theory of Planned Behavior (Ajzen, 1991)

As an extension of TRA, TPB has multi-discipline applicability. It has been used to predict health behaviors, such as weight-loss and females' intentions to perform self-breast exams (Orbeil, Hodgkins, & Sheeran, 1997; Schifter & Ajzen, 1985). Predictions regarding intentions to exercise can also be made using TPB. According to Godin, Valois, and Lepage (1993), attitude, perceived behavioral control, and habit, an additional construct they added, directly influence participants' intention to exercise. However, their study returned mixed results on the relationship between intention and actual behavior. One group study demonstrated a relationship between intention and actual behavior, while the other did not. Neither group supported social norms as an indicator of intention (Godin et al., 1993). Norman and Conner (2005) found similar results, and asserted that attitude and perceived behavioral control significantly influence individual intentions to exercise. Likewise, they discovered subjective norm was not significant in predicting intentions.

TPB also has applicability in studies related to technology adoption. For example, Venkatesh, Morris, and Ackerman (2000) used TPB to examine the influence of gender on the adoption of new technology in the workplace. Specifically, the study examined whether gender was a determinant of the constructs that predicted intention. The results showed men's intentions were predicted by attitude, but subjective norm did not have a significant effect. Conversely, women's intentions were predicted by subjective norm and perceived behavioral control. However, gender did not significantly influence short-term or long-term usage. Rather, gender determined the importance placed on the antecedents to intention (Venkatesh et al., 2000). Other studies utilizing TPB examined the influence of privacy perceptions on Internet purchasing and the adoption of cloud computing (Arpaci, Kilicer, & Bardakci, 2015; George, 2004; Pavlou & Fygenson, 2006). Related to this research, each of these studies validated the constructs of TPB in predicting technology adoption as mediated by beliefs about privacy and security.

## Technology Acceptance Model

While TRA and TPB predicted behaviors, a framework was needed to consistently explain why individuals adopt various technologies. Davis (1986) introduced the Technology Acceptance Model (TAM) to determine the integral constructs for predicting technology adoption. Similar to TRA and TPB, TAM suggested behavioral intention was predictive of actual technology usage. As illustrated in Figure 3, the antecedents for behavioral intentions varied from those in TRA and TPB. Specifically, perceived usefulness of the technology and perceived ease of use directly influenced intentions, which in turn influenced usage (Davis, 1986).

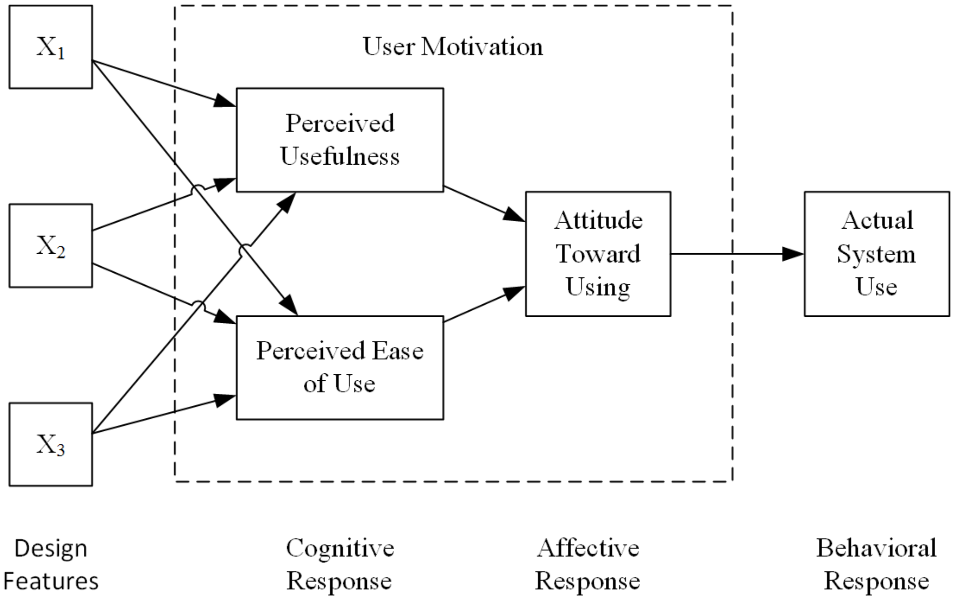


Figure 3 - Technology Acceptance Model (Davis, 1986)

Hu, Chau, Sheng, and Tam (1999) used TAM to explore the implementation of telemedicine by physicians in Hong Kong who had a strong inclination to use new and cutting-edge technologies for increasing access to healthcare. The resulting data indicated perceived usefulness and attitude significantly influenced actual usage, while perceived ease of use was not significant (Hu et al., 1999).

As technologies moved to an online environment, it became increasingly important for emerging research to factor in the concept of threat when attempting to explain acceptance of those technologies. Lu, Hsu, and Hsue (2005) used an extension of TAM as a framework for examining the determinants for adopting online technologies, introducing perceived risk as an additional construct. Their study surveyed users to determine the influence of perceived risk on adopting anti-virus technologies in an online environment. One group of users implemented the application on a trial basis, while a second group continued to use the application beyond the trial period. For both groups, the results indicated perceived risk and perceived usefulness were significant indicators of the resulting attitude to use online applications (Lu et al., 2005).

Additional studies implemented various extensions of TAM to describe user attitudes in different online environments, including social media, online investment technology, and implementation of security software by employees (Jones, McCarthy, Halawi, & Mujtaba, 2010; Rauniar, Rawski, Yang, & Johnson, 2014; Roca, García, & de la Vega, 2009). Notably, Roca et al. (2009) added perceived trust as a mediating construct for perceived usefulness and perceived ease of use in predicting behavioral intentions to use online investment systems. Perceived security and perceived privacy were included as antecedents to perceived trust. Perceived privacy as a predictor of perceived trust was not supported. Also, the relationship between perceived ease of use and behavioral intention was not supported. All other relationships were significant in determining investors’ intentions to use online trading websites (Roca et al., 2009).

Summarizing, the research streams of TRA, TPB, and TAM provide a solid foundation for perceptions of motivation and behavior.

## Protection Motivation Theory

Originally proposed by Rogers (1975), Protection Motivation Theory (PMT) sought to identify how individuals develop appropriate responses to threats.  Prior to reacting to threats, individuals navigate a thought process that ultimately determines their response.  Initially, PMT suggested individuals assign a level of severity to the threat, while simultaneously gauging the likelihood that the threat will affect them personally. Individuals also examine possible responses to the threat and the ability of the responses to protect them.  As a result, the appraised severity, expectancy of exposure, and belief in efficacy of coping response interact to motivate individuals to implement a protective mechanism and ultimately respond as intended (Rogers, 1975).  Figure 4 shows the relationships examined in PMT.

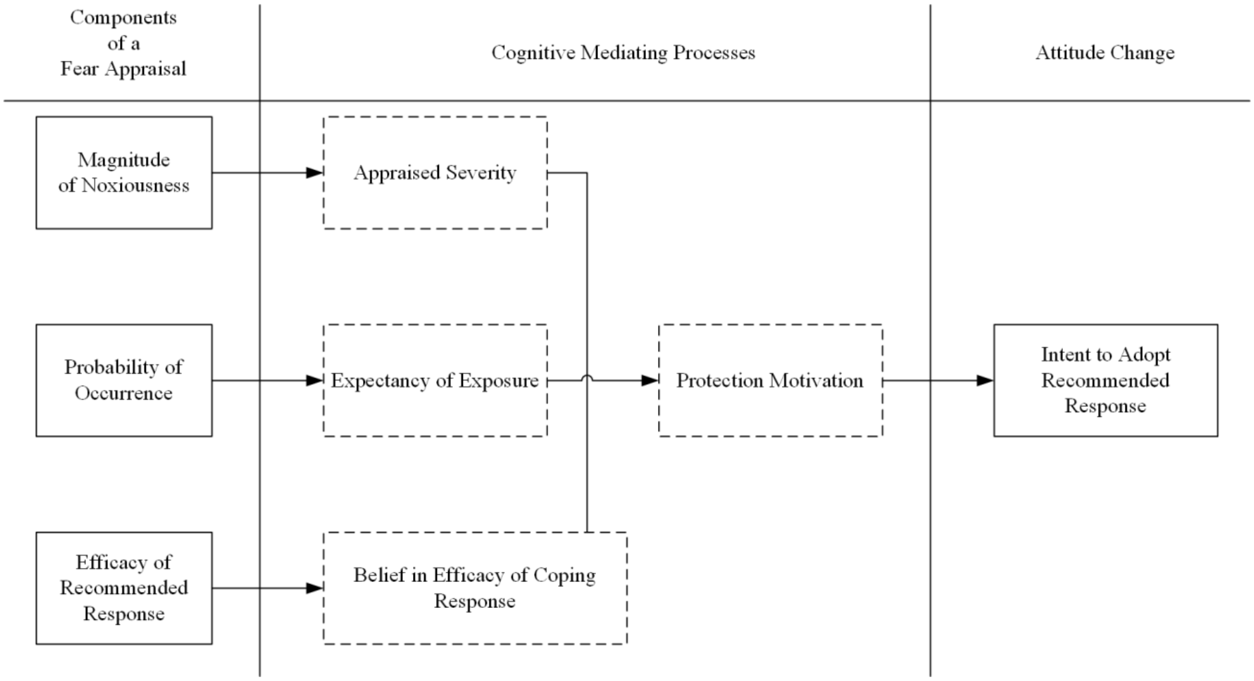

Components of a Fear Appraisal
Cognitive Mediating Processes
Attitude Change
Magnitude of Noxiousness
Appraised Severity
Probability of Occurrence
Expectancy of Exposure
Protection Motivation
Intent to Adopt Recommended Response
Efficacy of Recommended Response
Belief in Efficacy of Coping Response

Figure 4 - Protection Motivation Theory (Rogers, 1975)

In 1983, Maddux and Rogers extended PMT to include self-efficacy as an integral construct for forming protection motivations. They proposed that individuals must believe the response mechanism will effectively protect them from a threat, but must also believe in their ability to implement the mechanism. Maddux and Rogers' studies including self-efficacy in the PMT model confirmed self-efficacy as an additional construct for predicting intentions to implement protective responses (Maddux & Rogers, 1983).

Many studies have analyzed protection motivation in the context of various technologies. While studies based on TRA and TPB emphasized the adoption of technologies, studies with PMT as the foundational theory incorporated the concept of protecting oneself from threats associated with those technologies. Specifically, PMT was the basis for studies in the context of wireless security systems, information security compliance, and usage of the Internet, anti-virus software, and mobile devices (Chenoweth, Minch, & Gattiker, 2009; Chou & Chou, 2016; Dang-Pham & Pittayachawan, 2015; Herath & Rao, 2009; Johnston & Warkentin, 2010; Lee, Larose, & Rifon, 2008; Tsai et al., 2016; Vance, Siponen, & Pahnila, 2012; Woon, Tan, & Low, 2005).

While PMT is widely used to determine user protection motivations, mixed results indicate it is not the best fit for explaining why users implement behaviors to avoid technological threats. In 2005, Woon et al. sought to determine the factors that cause homeowners to implement protective behaviors when using a wireless security system. They tested the full PMT model and added response cost as a construct. Their findings confirmed the significance of perceived severity, response efficacy, self-efficacy, and response cost. However, they found that perceived susceptibility was not significant in determining protective behaviors (Woon et al., 2005). Likewise, other studies identified that perceived susceptibility was not significant in predicting protective motivations. The context of these studies included internet usage and compliance with information security policies in the work environment (Herath & Rao, 2009; Johnston & Warkentin, 2010; Tsai et al., 2016; Vance et al., 2012; Yoon, Hwang, & Kim, 2012). Dang-Pham and Pittayachawan (2015) studied students' protection motivations when using personal devices at the university and at home. They found perceived susceptibility was a predictor of protective motivations in the university setting, but not at home (Dang-Pham & Pittayachawan, 2015). Conversely, perceived susceptibility was significant in the context of internet usage and compliance with information security policies in other studies (Chenoweth et al., 2009; Ifinedo, 2012; Lee et al., 2008). Although these studies had similar contexts, they found mixed results regarding the influence of perceived susceptibility on protection motivation.

PMT studies have also returned mixed results regarding perceived severity, self-efficacy, cost, and safeguard effectiveness. Perceived severity had no significance in the context of online behaviors and information security policy compliance (Ifinedo, 2012; Lee et al., 2008). Ifinedo (2012) also found that cost was not significant in determining compliance with information security policies. Self-efficacy failed to predict protective motivations for college students in an online environment (Chenoweth et al., 2009), and response efficacy was not significant in the context of teachers' motivation to avoid technological threats (Chou & Chou, 2016). The prevalence of mixed results among studies based on the PMT model highlights the need for a model that is better suited for determining the process by which individuals develop intentions and behaviors for avoiding technological threats.

## Technology Threat Avoidance Theory

Technology Threat Avoidance Theory (TTAT) as proposed by Liang and Xue (2009) is similar to Protection Motivation Theory (PMT), but better suited for use in IT-related disciplines. The theory proposes that users are motivated to employ safeguards when they perceive threats, and suggests that user motivation to invoke a safeguarding mechanism is influenced by threat perceptions. Liang and Xue (2010) examined the associations in the model, which included the relationships between susceptibility, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, and avoidance behavior.

Liang and Xue (2010) drew from PMT to incorporate a threat appraisal into the TTAT model. They posited that perceived severity and perceived susceptibility were antecedents to perceived threat. Perceived severity was defined as the level of harm malicious threats to IT would cause the user. Perceived susceptibility was defined as the likelihood that malware would bring negative consequences to the user. Additionally, perceived severity and perceived susceptibility were expected to interact with one another to increase threat perceptions (Liang & Xue, 2010). These two constructs were expected to explain the level of the user's threat perceptions.

The TTAT model also incorporated a coping appraisal process similar to PMT, which included the self-efficacy, safeguard effectiveness, and safeguard cost constructs. Self-efficacy was the user's perception of their ability to implement the safeguarding measure. Safeguard effectiveness was defined as the user's perception that the safeguarding measure would actually protect them from malware. Safeguard cost was defined as the impact implementing the safeguarding measure would have on the user, including the monetary and time implications. Liang and Xue (2010) proposed these constructs would increase avoidance motivation. Additionally, they anticipated an interaction between safeguard effectiveness and perceived threat would negatively affect avoidance motivation (Liang & Xue, 2010).

Additional constructs in the TTAT model were derived from TAM, and these included avoidance motivation and avoidance behavior. Avoidance motivation was defined as the user's level of motivation to avoid technology threats by implementing protective actions. Avoidance behaviors were the actual actions taken to avoid the threats from malware (Liang & Xue, 2010). Figure 5 shows the constructs proposed in the original Technology Threat Avoidance Theory.

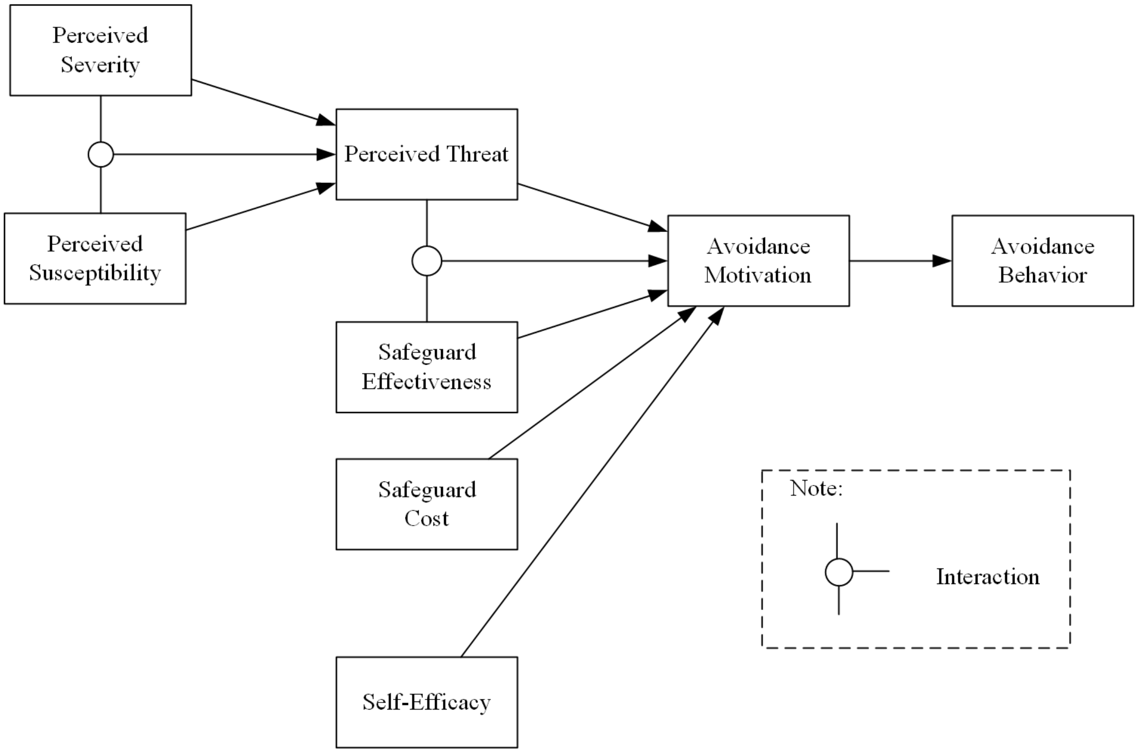


Figure 5 - Technology Threat Avoidance Theory (Liang & Xue, 2010)

A review of the TTAT literature confirms the theory's use in many different IT contexts and flexibility in explaining threat avoidance behavior. Prior studies revealed inconsistencies regarding the significance of severity, susceptibility, and the interaction between the two constructs. The lack of consistent results suggested a need to review the placement of susceptibility in the threat calculus. The original test by Liang and Xue (2010) found both severity and susceptibility to be significant in determining threat perceptions. However, the test indicated the interaction between severity and susceptibility was not significant in the threat appraisal process (Liang & Xue, 2010).

Subsequent studies of the TTAT model continued to return mixed results regarding the relationships between susceptibility, severity, and threat, calling into question how these constructs influence threat perceptions. In the context of game-based phishing attacks, Arachchilage and Love (2013) found susceptibility, severity, and the interaction between the two to be significant in determining threat perceptions. Other studies in the contexts of avoiding online threats and compliance with password security guidelines found susceptibility and severity to be significant, but did not test the interaction between the two (Chen & Zahedi, 2016; Mwagwabi, 2015).

Young, Carpenter, and McLeod (2016) replicated the full TTAT model in the context of avoiding malware. The results indicated a significant association between severity and threat. However, the results did not support a relationship between susceptibility and threat, nor the interaction between susceptibility and severity (Young et al., 2016). Manzano (2012) tested the full TTAT model in the context of users' avoidance of IT threats at home. The study surveyed two groups for comparison. Group 1 was comprised of individuals who worked in a non-IT setting. Group 2 was made up of

IT experts. Both were asked questions to assess their IT practices at home. The study returned mixed results for the threat appraisal process. Specifically, the relationship between susceptibility and threat was supported for Group 1, but not for Group 2. Both groups indicated a significant relationship between severity and threat, while neither group supported the interaction between susceptibility and severity (Manzano, 2012). Das and Khan (2016) incorporated susceptibility, severity, and the interaction between severity and susceptibility into an expectancy-based model to analyze the steps smartphone users take to avoid malicious threats via their devices. Das and Khan conducted their study on three groups, including iPhone users, Blackberry users, and Android users. Susceptibility and severity were only significant for Blackberry users. The interaction between susceptibility and severity was not supported (Das & Khan, 2016).

Other studies that tested a partial TTAT model also returned mixed results. Vance, Anderson, Kirwan, and Eargle (2014) tested severity and susceptibility in the context of determining risk-taking behaviors by measuring responses to security warnings. Vance et al. tested participants prior to experiencing a malware incident and again after experiencing a malware incident. The results were mixed between the pre-test and post-test regarding the significance of susceptibility and severity in predicting risk-taking behaviors (Vance et al., 2014).

In the context of detecting and avoiding fake websites, Zahedi, Abbasi, and Chen (2015) included severity and susceptibility in the threat appraisal of their model. They surveyed two groups, including participants who used online banking websites and participants who used online pharmacies. Susceptibility was not supported for either group, while severity was supported for participants who used online banking sites (Zahedi et al., 2015).

The number of studies that use TTAT in part or in whole to analyze threat appraisals and the resulting avoidance behaviors provide support for the applicability of TTAT in information security research. However, the lack of consistent results regarding the significance of susceptibility and severity in the threat appraisal process suggests revisions to the TTAT model would be beneficial in explaining the development of threat perceptions. Table 1 provides an overview of these studies detailing the mixed results of susceptibility, severity, and threat as seen in Young, Carpenter, and McLeod (2017).

Table 1 - Severity, Susceptibility, and Threat Perceptions (Young et al., 2017)

| **Author** | **Title** | **Notes** | **Susceptibility** | **Sus X Sev** | **Severity** | **Threat** |
|---|---|---|---|---|---|---|
| Liang & Xue (2010) | Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective | Original TTAT Theoretical Test | sig. | n.s. | sig. | sig. |
| Manzano (2012) | The Cybercitizen Dimension: A Quantitative Study Using a Threat Avoidance Perspective | Voluntary working participants with an experimental group and control group of IT professionals | mixed between two groups | n.s. | mixed between two groups | mixed between two groups |
| Arachchilagea & Love (2013) | A Game Design Framework for Avoiding Phishing Attacks | Changed context to a game-based phishing attack | sig. | sig. | sig. | sig. |
| Young, Carpenter, & McLeod (2016) | Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Theory Replication | Replication of TTAT theoretical test; broadened to the context of malware | n.s. | n.s. | sig. | sig. |

Table 1 Continued

| **Author** | **Title** | **Notes** | **Susceptibility** | **Sus X Sev** | **Severity** | **Threat** |
|---|---|---|---|---|---|---|
| Chen & Zahedi (2016) | Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China | Context is avoiding online threats comparing Western vs. Eastern cultures | sig | 0 | sig. | sig. |
| Mwagwabi (2015) | A Protection Motivation Theory Approach to Improving Compliance with Password Guidelines | Extends TTAT to include exposure to hacking as a predictor of vulnerability | sig. | 0 | sig. | sig. |
| Vance et al. (2014) | Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG) | Uses partial TTAT model examining users' perceptions of risk, severity, susceptibility, and threat | n.s. | 0 | n.s. | 0 |
| Zahedi et al. (2015) | Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance | Only uses severity and susceptibility as part of a threat appraisal | mixed | 0 | mixed | 0 |
| Xue et al. (2015) | Investigating the Resistance of Telemedicine in Ethiopia | Uses TAM intention and behavior. Not really TTAT | sig. | 0 | 0 | 0 |

Note: sig. = significant, n.s. = not significant, 0 = not tested

## Privacy

The increase in data collected by mobile devices and wearable technologies suggests the need for theoretical frameworks to incorporate privacy concerns as a key construct in determining users' avoidance behaviors. Matt and Peckelsen (2016) added privacy concerns and previous privacy experience as control variables to predict users' intentions to use privacy-enhancing technologies. The privacy concerns construct for their study was adapted from Dinev and Hart (2006), who described privacy concerns as perceptions individuals developed in response to organizations sharing their personal data for economic gain.  Matt and Peckelsen operationalized previous past experiences as participants' prior exposure to privacy violations.  Their results indicate both privacy concerns and previous privacy experience have a strong influence on users' intentions to implement privacy-enhancing technologies (Matt & Peckelsen, 2016).

Some studies emphasized the need to understand how individuals develop their privacy concerns, therefore seeking to identify the antecedents to privacy concerns (Junglas, Johnson, & Spitzmüller, 2008; Xu, Dinev, Smith, & Hart, 2011).  Junglas et al. (2008) explored the importance of personality traits in predicting concern for privacy in the context of using location-based services.  They confirmed the personality traits agreeableness, conscientiousness, and openness to experience significantly influenced concern for privacy (Junglas et al., 2008).  Xu et al. (2011) attempted to identify the factors that influence privacy concerns in the context of organizational information practices.  Their research confirmed disposition to value privacy, privacy risk, and privacy control had a strong effect on privacy concerns (Xu et al., 2011).

Other research analyzed users' privacy perceptions in the context of online privacy (Berendt, Günther, & Spiekermann, 2005; Clemons & Wilson, 2015; Dinev & Hart, 2006).  Clemons and Wilson (2015)  surveyed families and teenagers in eight countries to measure their privacy concerns.  The context of the study was data mining students' text messages and school-issued email accounts so external organizations could conduct targeted ad campaigns.  Although the level of concern varied among countries and between parents and their students, all groups surveyed were significantly concerned with the invasion of privacy and the potential consequences (Clemons & Wilson, 2015). In the context of online shopping, Dinev and Hart (2006) incorporated an extension of the privacy calculus in their model to analyze an apparent paradox between consumers' stated privacy concerns and their online shopping behaviors. They suggested that an increased perception regarding Internet privacy positively affected Internet privacy concerns. As a result, increased Internet privacy concerns negatively affected the willingness to provide personal information to transact on the Internet. All associations in their proposed model were found to be significant (Dinev & Hart, 2006).

In summary, many studies have included a privacy construct in the research model, especially in the context of online activities and organizational usage of personal data. The proliferation of data electronically available increases the need to understand these interactions. Therefore, it is important to consider and understand the impact of privacy concerns on individuals' behaviors and account for that in health information research.

# 3. RESEARCH QUESTIONS

This study explores how people judge threats, perceive privacy, and are motivated to avoid harm. Inconsistent results in prior works bring into question the relationships associated with threat determination, privacy, and user motivation. Based on the literature and results from previous studies, the following research questions were developed.

Research question one examines the relationship between perceived susceptibility and severity of threats when developing threat perceptions. Prior research returned mixed results regarding the occurrence or timing of susceptibility when determining its impact on threat perceptions. This study attempted to identify if users must first feel susceptible to a threat in order to form a perception regarding the severity of the threat.

RQ1: How do users perceive susceptibility to a threat when evaluating the severity of the threat?

Research question two analyzes the influence of perceived severity of a threat and the resulting threat perceptions. This study attempts to understand if perceived susceptibility as an antecedent to perceived severity, removing the interaction with perceived susceptibility, causes users to have stronger threat perceptions. Once users feel susceptible to a threat and therefore feel the threat would have a severe impact on them, it would follow that the user would perceive the threat more strongly.

RQ2: What is the relationship between perceived severity and the formation of threat perceptions?

Research question three introduces privacy as a new construct to the TTAT model. Privacy has limited exploration with technology threat avoidance (Herath et al., 2014). This research question sought to understand if privacy concerns influenced motivation to avoid perceived threats.

RQ3: How do privacy perceptions affect user motivation to implement technology safeguards?

The following research questions were derived from previous TTAT studies with consistent results. The constructs for these questions were identical in placement to the original TTAT model (Liang & Xue, 2010). Although these questions returned consistent results in prior studies, revisions to the threat calculus and the introduction of privacy concerns required a determination of reliability and validity, and therefore an analysis of the complete model and the corresponding research questions.

RQ4: What is the relationship between threat perceptions and user motivation to adopt technology safeguards?

RQ5: How does self-efficacy influence user motivation to adopt technology safeguards?

RQ6: Does safeguard cost impact user motivation to adopt the safeguard?

RQ7: Do perceptions about safeguard effectiveness impact motivation to adopt the safeguard?

RQ8: What is the relationship between user motivation and actual adoption of technology safeguards?

# 4. RESEARCH MODEL AND HYPOTHESES

The research model in this study extended and refined the full TTAT model. Due to inconsistent prior results, this model considered perceived susceptibility as an antecedent to perceived severity, refining the existing threat calculus. This change in the model provided a test for determining if users must first feel susceptible to a threat in order to develop a perception of the threat severity, strengthening the influence of the two constructs on threat perception. In addition, Liang and Xue (2010) did not consider privacy concerns. In this model, privacy concerns are believed to affect user motivation, so the privacy construct is inserted as an antecedent to avoidance motivation. Due to the sensitive nature of data collected by fitness technologies, this model attempted to determine if privacy concerns increased avoidance motivation. Figure 6 shows the inner model utilized in this work.

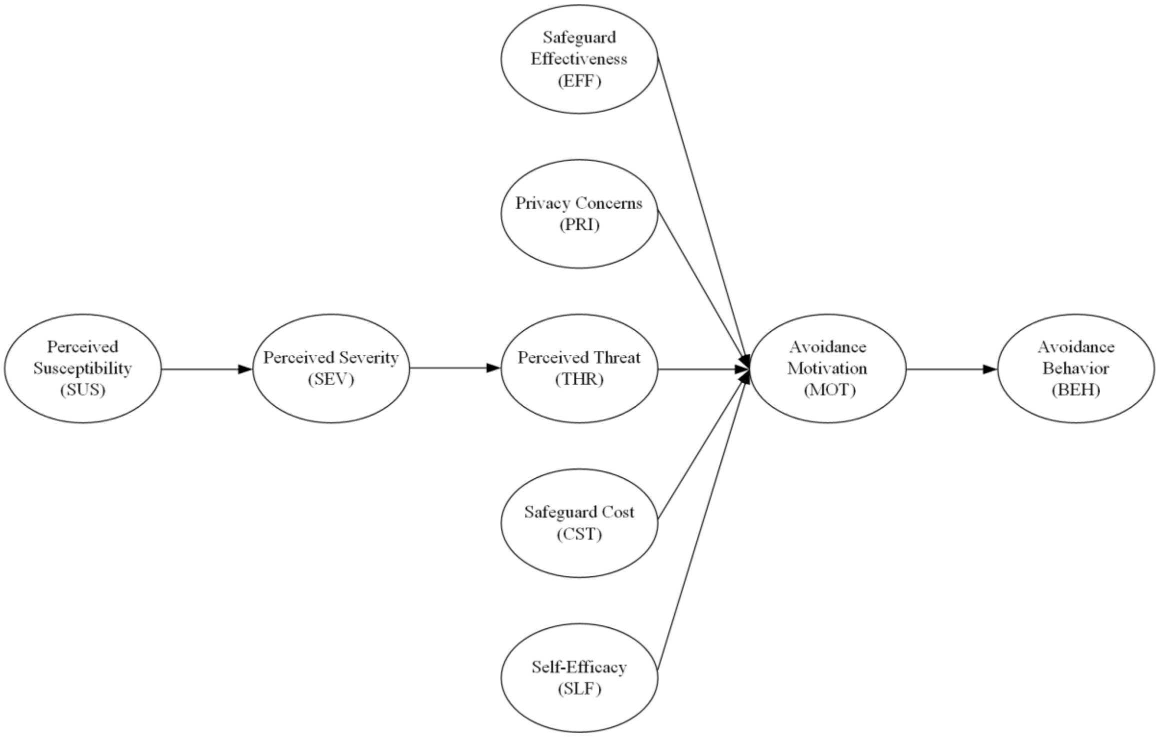


Figure 6 - Revised Technology Threat Avoidance Model

Following the research model, hypotheses were developed to examine the full TTAT model as refined and detailed. In response to these prior works and to explore the modified relationships between these constructs, this study positioned perceived susceptibility as an antecedent to perceived severity in the threat calculus. Given these modifications to the TTAT model, this study hypothesized that:

H1a Perceived susceptibility positively influences perceived severity.

H1b Perceived severity positively influences threat perceptions.

H1c Perceived threat positively influences avoidance motivation.

Previous research has focused on the impact of privacy concerns on technology acceptance. However, research incorporating privacy concerns in the context of threat avoidance is limited (Herath et al., 2014). This study sought to examine the impact of privacy concerns on threat avoidance and hypothesized that:

H2 Privacy concerns positively influence avoidance motivation.

In order to evaluate their motivation to avoid malicious threats to IT, users must first assess their ability to do so. Self-efficacy refers to the certainty that users place on their ability to implement protective measures. Users who believe in their abilities are typically more likely to enact a safeguard (Liang & Xue, 2010). Therefore, this study hypothesized that:

H3 Self-efficacy positively influences avoidance motivation.

Safeguarding measures require financial and intellectual commitments from users, causing users to evaluate the safeguard cost. Users must determine if the financial burden or intellectual impact will impede their productivity. Users may be less likely to adopt safeguarding measures that require an undue amount of time, hassle, or money

(Liang & Xue, 2010). This study hypothesized that:

H4 Safeguard cost negatively influences avoidance motivation.

While safeguard cost and self-efficacy are important for determining avoidance motivation, user perceptions about safeguard effectiveness are equally important. Unless users perceive the safeguard to be an effective tool for avoiding malware, they are unlikely to implement it (Liang & Xue, 2010). Therefore, this study hypothesized that:

H5 Safeguard effectiveness positively influences avoidance motivation.

Prior research has demonstrated a strong relationship between motivation and behavior (Arachchilage & Love, 2013; Liang & Xue, 2010; Young et al., 2016). Once users develop avoidance motivation, they are likely to implement the safeguarding measure (Liang & Xue, 2010). In keeping with consistent results from prior studies, this study hypothesized that:

H6 Avoidance motivation positively influences avoidance behavior.

Figure 7 shows the relationships between the constructs and their related hypotheses.

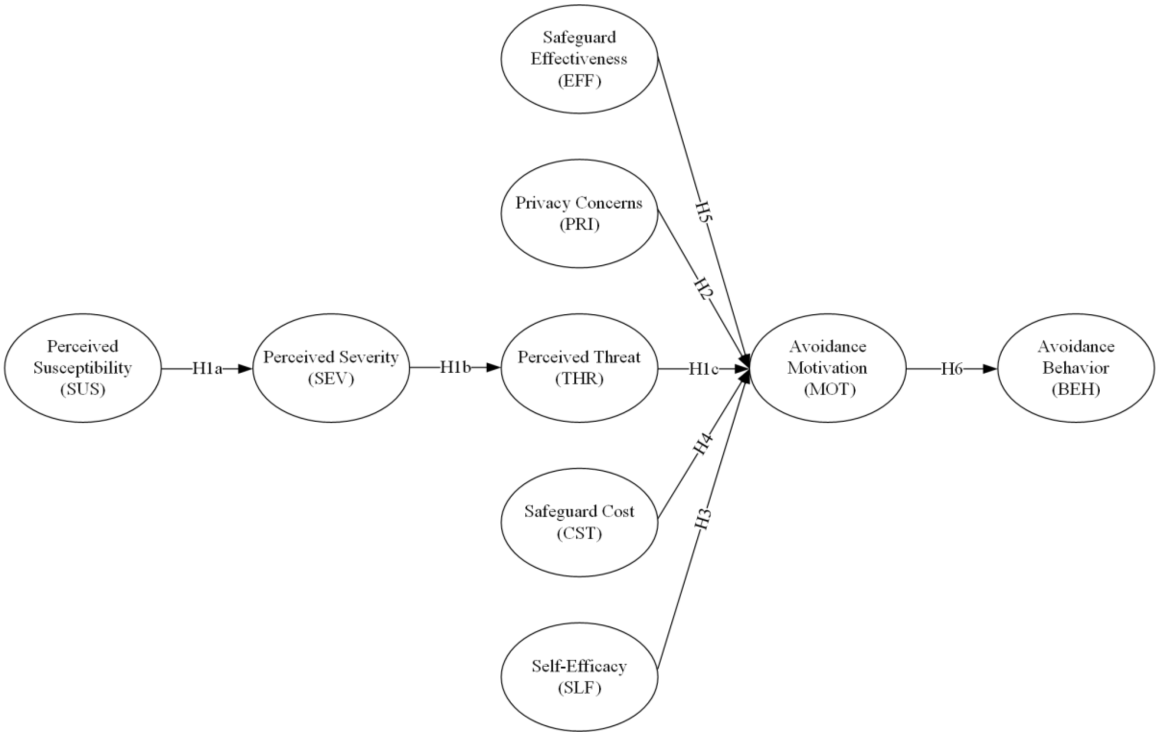


Figure 7 - Hypotheses

# 5. METHODOLOGY

## Method

This research employed a survey instrument to examine the revised TTAT model and resulting hypotheses. Respondents were surveyed to ascertain their perceptions of susceptibility to and severity of threats while using wearable activity trackers connected to the Fitbit system. Because the wearable activity tracker was connected via Bluetooth to the user's phone and then subsequently to the Fitbit website, user threat perceptions were important. The data collection methods involved completing a survey instrument as outlined in the measures section below.

## The Fitbit System

For the purposes of this study, the Fitbit system was defined as all of the interconnected components through which the Fitbit activity tracker collects, stores, and transmits personal fitness data. These components included the user, Fitbit activity tracker, mobile device application, desktop application, and website - www.fitbit.com. Captured personal fitness data were received by the Fitbit system using a variety of access points including Bluetooth, wireless Internet, accessing the Fitbit website, and connecting to a device using the dongle provided with the tracker. Personal fitness data included the number of steps taken, number of floors climbed, heart rate, distance traveled, calories burned, height, weight, age, minutes active, minutes asleep, minutes sedentary, minutes awake, and demographic information associated with the user's profile.

## Measures

The majority of the items used in the survey instrument were adapted from the measures used by Liang and Xue (2010). The questions used to assess privacy concerns were adapted from Matt and Peckelsen (2016). All adapted TTAT measures were previously validated; however, a revalidation was performed due to minor wording changes based on a review of the literature. For example, "malware" was more encompassing than "spyware," so the terminology was updated (Manzano, 2012; Young et al., 2016, 2017). Some items were modified to fit the context of this study, the Fitbit system. The original TTAT items used mixed scales drawn from both semantic differential and Likert based questions. Some items ranged from strongly disagree to strongly agree, while others covered "not at all confident" to "totally confident," and still others from "innocuous" to "extremely devastating" (Liang & Xue, 2010). The scale for this study was standardized to provide consistent wording for each measure and used a typical seven-point Likert scale construction.

The instrument contained 42 items, which were grouped by construct. The questions anchored at strongly disagree, disagree, somewhat disagree, neither agree nor disagree, somewhat agree, agree, and strongly agree. Items adapted from Liang and Xue's (2010) original test of the TTAT model included five questions measuring perceived severity, four for perceived susceptibility, three for perceived threat, three for safeguard cost, six for safeguard effectiveness, six for self-efficacy, three for avoidance motivation, and two for avoidance behavior. Four items measuring privacy concerns were adapted from Matt and Peckelsen (2016).

Due to the different context of this study and issues with Liang and Xue's (2010) items, some of the original TTAT measurements were not applicable. Measurements that were omitted included one item for perceived susceptibility, five for perceived severity, one for perceived threat, and four for self-efficacy. Additional items were added to measure perceived severity, susceptibility, and threat. Along with the adapted items, the new measurements were evaluated for reliability and validity.

## Data Collection

The participants for this study were freshman college students who had not previously used a Fitbit activity tracker. An email was sent to 3,300 randomly selected freshmen inviting them to respond to a preliminary questionnaire regarding previous Fitbit usage. A total of seven hundred forty-seven students responded to the preliminary questionnaire. The first one hundred respondents who had not previously used a Fitbit were selected to participate. Participants were invited to attend an intake session in an on-campus computer lab to receive and activate a Fitbit activity tracker. Ninety-eight students participated in a presentation explaining the Fitbit system and describing how the system functioned. The presentation also outlined the types of data collected via the Fitbit system. This collection of data was defined as personal fitness data for the purposes of this study. Upon conclusion of the presentation, participants were asked to respond to the electronic survey.

# 6. ANALYSIS

A total of ninety-two survey responses were collected from ninety-eight participants, yielding a response rate of 94%. The study was designed to examine the activities and perceptions of incoming freshmen who were 18 or 19 years old; therefore, it was no surprise that all respondents selected the 18-24 age bracket. With regard to gender, 30.4% of the participants were male, and the remaining 69.6% selected female. The sample was comprised of 40% Hispanic, 39% White, 13% African American, 7% Asian, and 2% other ethnicity. Due to the design, the highest level of educational attainment was constrained, with 44% reporting a high school degree, 52% attending some college, 2% acquiring an Associate's degree, and 1% a Bachelor's degree.

The items on the survey were organized according to the corresponding latent variables, and the data were analyzed using SmartPLS (Ringle, Wende, & Will, 2005). This statistical tool is useful for evaluating both large and small sample sizes (Chin, 1998), and is effective with interval or ratio responses. Because it utilizes bootstrap resampling, the underlying distribution is not critical (Vinzi, Trinchera, & Amato, 2010).

In this work, all items were modeled as reflective indicators of latent variables. A two-step approach to analysis was followed by first considering the reliability and validity of the measurement model and then assessing the structural model (Anderson & Gerbing, 1988). Reliability demonstrates that the items provide a consistent reflection of the underlying latent variable, whereas validity ensures the instrument measures the intended relationships contained in the model (DeVellis, 2003; Tavakol & Dennick, 2011). Individual item consistency was first evaluated using Cronbach's Alpha. Table 2 provides the Cronbach's Alpha value for each construct. All items scored higher than

0.70, demonstrating adequate reliability.  Perceived threat scored the lowest at 0.85.

Table 2 - Construct Reliability as Measured by Cronbach's Alpha

| | Cronbach's Alpha |
|---|---:|
| Avoidance Behavior | 0.93 |
| Avoidance Motivation | 0.98 |
| Safeguard Effectiveness | 0.98 |
| Perceived Severity | 0.93 |
| Perceived Susceptibility | 0.94 |
| Perceived Threat | 0.85 |
| Privacy Concerns | 0.98 |
| Safeguard Cost | 0.86 |
| Self-Efficacy | 0.94 |

After establishing construct reliability, construct validity was assessed by testing both convergent and discriminant validity.  Convergent validity confirms the items measured the intended constructs, while discriminant validity establishes a clear difference between constructs (Trochim, 2006).  As suggested by Gefen, Rigdon, and Straub (2011), an examination of convergent validity of individual items was evaluated via a factor analysis.  Factor loadings for individual items were organized by construct, and each was analyzed to determine if on-factor loadings were greater than 0.70 (See Appendix A).  On-factor loadings refer to the items that load together for a particular construct.  The lowest on-factor loading was 0.75, and all constructs demonstrated adequate convergent validity.

After assessing the convergent validity of the measurement model, factor analysis was also used to evaluate discriminant validity.  While on-factor loadings are an indication of convergent validity, off-factor loadings are used to consider discriminant validity.  No off-factor loadings were within 0.26 of their corresponding on-factor loading, demonstrating acceptable discriminant validity.  All factor loadings are available in Appendix A.

An additional step in substantiating discriminant validity is to calculate the square root of the average variance extracted (AVE).  AVE measures the amount of shared variance between the latent variables in the model, as opposed to the amount of variance that is due to error (Fornell & Larcker, 1981).  A value of 0.70 indicates a large amount of variance can be attributed to a specific variable, although a value of 0.50 is viewed as adequate (Alarcón & Sánchez, 2015).  Table 3 details the average variance extracted for all constructs.

Table 3 - Average Variance Extracted

| | AVE |
|---|---:|
| Avoidance Behavior | 0.93 |
| Avoidance Motivation | 0.97 |
| Safeguard Effectiveness | 0.89 |
| Perceived Severity | 0.77 |
| Perceived Susceptibility | 0.77 |
| Perceived Threat | 0.68 |
| Privacy Concerns | 0.93 |
| Safeguard Cost | 0.75 |
| Self-Efficacy | 0.78 |

The AVE value is then compared to the correlation with the other constructs.  The goal is to ensure the AVE is higher than the correlation with each construct, supporting discriminant validity.  In Table 4, the average variance extracted is listed in bold on the diagonals, and the correlation values with the other constructs are listed vertically.  The correlation value indicates the strength of the relationship between two variables

(Statsoft, 2013).

Table 4 - AVE and Construct Correlations

| AVE Correlations | Avoidance Behavior | Avoidance Motivation | Safeguard Effectiveness | Perceived Severity | Perceived Susceptibility | Perceived Threat | Privacy Concerns | Safeguard Cost | Self-Efficacy |
|---|---|---|---|---|---|---|---|---|---|
| Avoidance Behavior | **.93** | | | | | | | | |
| Avoidance Motivation | .46 | **.97** | | | | | | | |
| Safeguard Effectiveness | .28 | .46 | **.89** | | | | | | |
| Perceived Severity | .01 | .27 | .30 | **.77** | | | | | |
| Perceived Susceptibility | .08 | .08 | .09 | .40 | **.77** | | | | |
| Perceived Threat | .13 | .43 | .32 | .51 | .27 | **.68** | | | |
| Privacy Concerns | .08 | .18 | .17 | .32 | .51 | .33 | **.93** | | |
| Safeguard Cost | .00 | .14 | .35 | .27 | .19 | .31 | .24 | **.75** | |
| Self-Efficacy | .35 | .45 | .44 | .20 | .01 | .35 | .10 | .40 | **.78** |

The AVE value was greater than any correlational value by construct, and the factor loadings were greater on-factor than off-factor; therefore, the measurement model demonstrated satisfactory discriminant validity. In summary, the reliability and validity assessment provided insight into the suitability of the research model.

## 7. RESULTS

After evaluating the outer measurement model, the proposed inner model was assessed using SmartPLS. First, the path coefficients and variance extracted, or $R^2$ values, were calculated for the construct relationships. Path coefficients provided insight into the relationship between constructs by measuring the size and direction of the effect (Webley & Lea, 1997). $R^2$ values indicated the percentage of variance in each dependent variable that can be explained by the independent variables (Caldwell, 2013). Table 5 provides the path values for the relationships in the model.

Table 5 - Path Coefficients

| | Avoidance Behavior | Avoidance Motivation | Perceived Severity | Perceived Threat |
|---|---|---|---|---|
| Avoidance Motivation | 0.46 | | | |
| Safeguard Effectiveness | | 0.29 | | |
| Perceived Severity | | | | 0.51 |
| Perceived Susceptibility | | | 0.40 | |
| Perceived Threat | | 0.24 | | |
| Privacy Concerns | | 0.13 | | |
| Safeguard Cost | | -0.20 | | |
| Self-Efficacy | | 0.33 | | |

The path values represent the effect of one construct on another. Interestingly, all path values were positive except for safeguard cost to avoidance motivation. This was consistent with Liang and Xue (2010). The values were the strongest in the susceptibility to severity to threat calculus, with perceived susceptibility to perceived severity at 0.40

and perceived severity to perceived threat at 0.51. Privacy concerns to avoidance motivation was the lowest at 0.13. Figure 8 details the path values between constructs for the complete model.

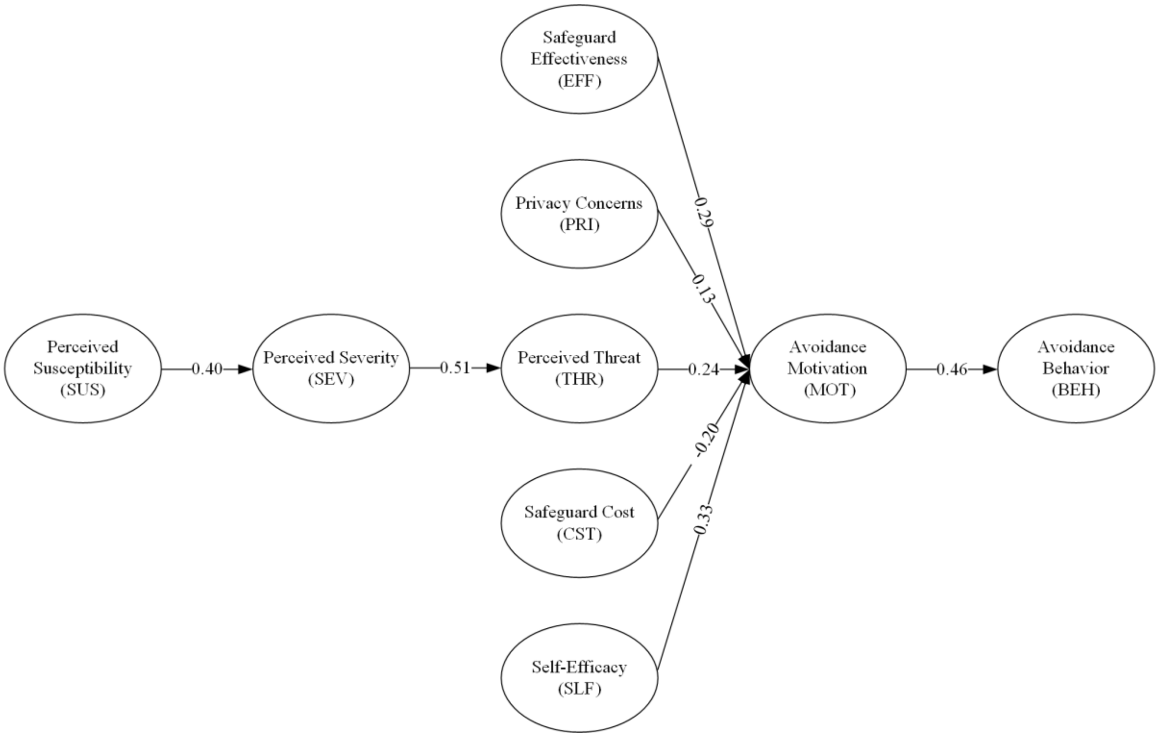


Figure 8 - Path Coefficients

The $R^2$ values or variance extracted was calculated for all dependent variables. The model accounted for a significant portion of variance of avoidance behavior, avoidance motivation, perceived threat, and perceived severity. Table 6 shows the variance extracted by construct.

Table 6 - $R^2$ of Dependent Variables

| | R Square |
|---|---:|
| Avoidance Behavior | 0.22 |
| Avoidance Motivation | 0.38 |
| Perceived Severity | 0.16 |
| Perceived Threat | 0.26 |

The percentage of variation in the dependent variables explained by the independent variables is detailed in Figure 9. Avoidance motivation explains 22% of avoidance behavior. Safeguard effectiveness, privacy concerns, perceived threat, safeguard costs, and self-efficacy account for 38% of avoidance motivation. Perceived severity accounts for 26% of perceived threat, and perceived susceptibility explains 16% of perceived severity.

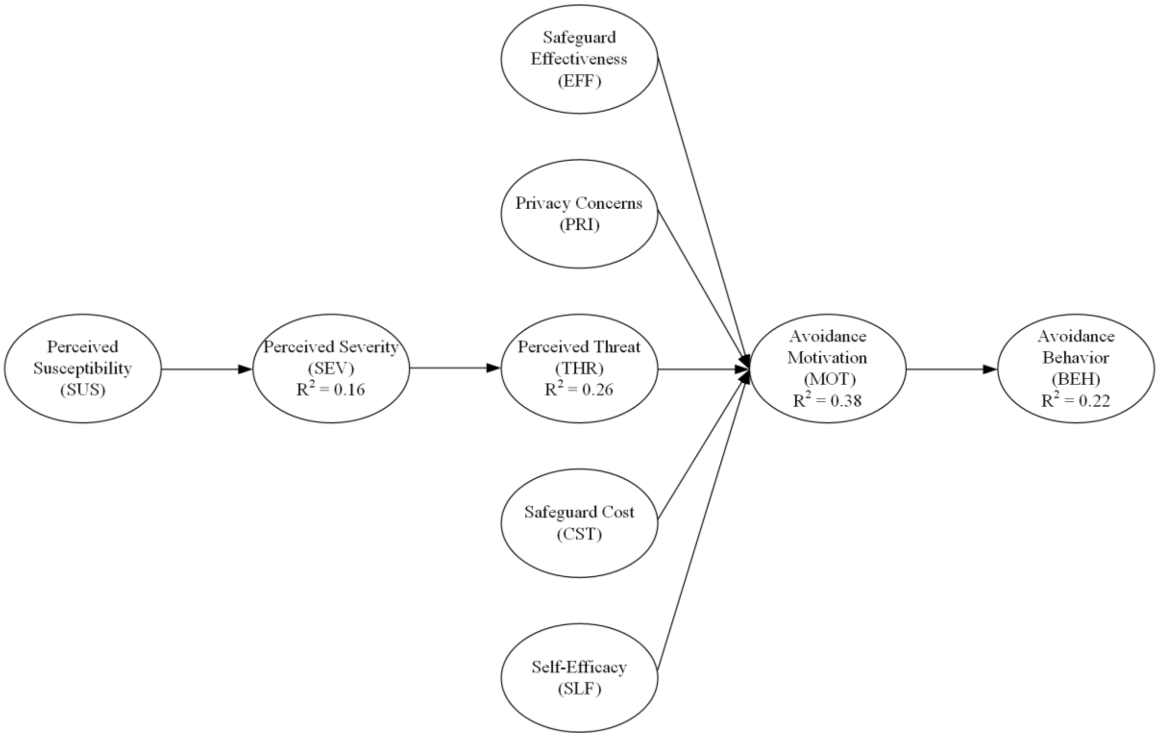

Safeguard Effectiveness (EFF)
Privacy Concerns (PRI)
Perceived Susceptibility (SUS)
Perceived Severity (SEV) $R^2 = 0.16$
Perceived Threat (THR) $R^2 = 0.26$
Avoidance Motivation (MOT) $R^2 = 0.38$
Avoidance Behavior (BEH) $R^2 = 0.22$
Safeguard Cost (CST)
Self-Efficacy (SLF)

Figure 9 - $R^2$ Values

After determining the path coefficients and variance values, a test of significance was performed for each path. Table 7 reports the sample mean, standard deviation, t-statistic, and corresponding p value for each relationship specified in the model.

Table 7 - Results

| | Sample Mean | Standard Deviation | T-Statistics | P Value |
|---|---|---|---|---|
| Avoidance Motivation→Avoidance Behavior | 0.46 | 0.09 | 5.20 | 0.01 |
| Safeguard Effectiveness→Avoidance Motivation | 0.29 | 0.08 | 3.62 | 0.01 |
| Perceived Threat→Avoidance Motivation | 0.24 | 0.12 | 2.07 | 0.04 |
| Privacy Concerns→Avoidance Motivation | 0.13 | 0.10 | 1.30 | 0.20 |
| Safeguard Cost→Avoidance Motivation | -0.20 | 0.11 | 1.93 | 0.06 |
| Self-Efficacy→Avoidance Motivation | 0.33 | 0.11 | 3.11 | 0.01 |
| Perceived Severity→Perceived Threat | 0.51 | 0.08 | 6.31 | 0.01 |
| Perceived Susceptibility→Perceived Severity | 0.40 | 0.09 | 4.33 | 0.01 |

Significant relationships included avoidance motivation→avoidance behavior, safeguard effectiveness→avoidance motivation, perceived threat→avoidance motivation, self-efficacy→avoidance motivation, perceived severity→perceived threat, and perceived susceptibility→perceived severity. Privacy concerns→avoidance motivation and safeguard cost→avoidance motivation were not significant, having p values greater than .05.

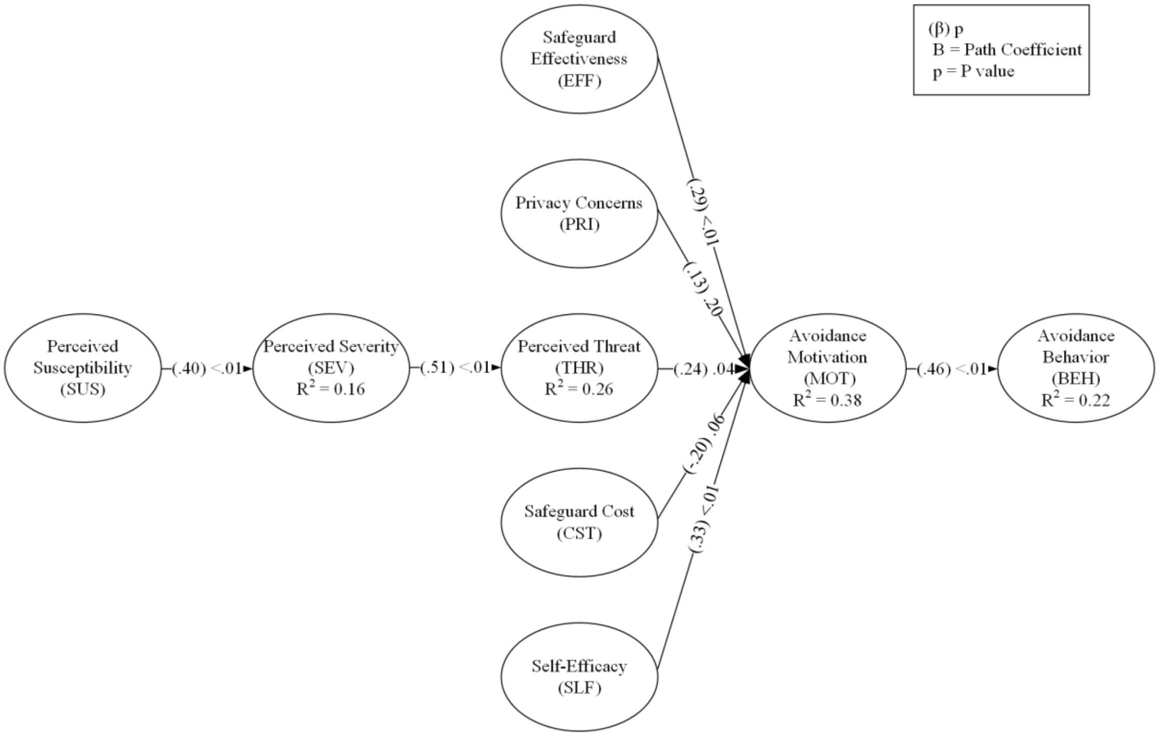

(β) p
B = Path Coefficient
p = P value
Safeguard Effectiveness (EFF)
Privacy Concerns (PRI)
Perceived Susceptibility (SUS)
Perceived Severity (SEV) R$^2$ = 0.16
Perceived Threat (THR) R$^2$ = 0.26
Avoidance Motivation (MOT) R$^2$ = 0.38
Avoidance Behavior (BEH) R$^2$ = 0.22
Safeguard Cost (CST)
Self-Efficacy (SLF)
(.40) <.01
(.51) <.01
(.24) .04
(.46) <.01
(.29) <.01
(.13) .20
(-.20) .06
(.33) <.01

Figure 10 - Results indicating path coefficients, p values, and R$^2$ values

With the exception of safeguard cost and privacy concerns, the model's beta coefficients indicated significant support for the hypothesized relationships. With regard to the threat calculus, perceived susceptibility showed a positive and significant effect on perceived severity ($\beta$ = .40, $\rho$ < 0.01, R$^2$ = .16). Perceived severity was significant and positive in its relationship with perceived threat ($\beta$ = .51, $\rho$ < 0.01, R$^2$ = .26). Perceived threat was positively and significantly associated with avoidance motivation ($\beta$ = .24, $\rho$ = 0.04), as was safeguard effectiveness ($\beta$ = .29, $\rho$ < 0.01). Safeguard cost ($\beta$ = -.20, $\rho$ = 0.06) was negatively related to avoidance motivation but only marginally significant. The relationship between self-efficacy ($\beta$ = .33, $\rho$ < 0.01) and avoidance motivation proved significant and positively correlated. Figure 10 shows the results, including path coefficients, p values, and R$^2$ values.

Results provided support for H1a, H1b, and H1c, supporting the modified threat calculus. H2 was not supported, indicating privacy concerns did not have a significant effect on avoidance motivation. In addition, H4 was not significant at p=.06, so safeguard costs were not supported. However, H3, H5, and H6 were supported, suggesting self-efficacy and safeguard effectiveness were both significant in predicting avoidance motivations, and avoidance motivations have a significant effect on avoidance behaviors. Table 8 provides a summary of the hypothesis results.

Table 8 - Hypothesis Results

| Hypothesis | Description | Results |
|---|---|---|
| H1a | Perceived susceptibility positively influences perceived severity. | Supported |
| H1b | Perceived severity positively influences threat perceptions. | Supported |
| H1c | Perceived threat positively influences avoidance motivation. | Supported |
| H2 | Privacy concerns positively influence avoidance motivation. | Not supported |
| H3 | Self-efficacy positively influences avoidance motivation. | Supported |
| H4 | Safeguard cost negatively influences avoidance motivation. | Not supported |
| H5 | Safeguard effectiveness positively influences avoidance motivation. | Supported |
| H6 | Avoidance motivation positively influences avoidance behavior. | Supported |

# 8. DISCUSSION

This study sought to determine user motivations for implementing safeguarding measures against potential threats to IT.  The TTAT model was revised to measure user perceptions and motivations in the context of wearable activity trackers.  Due to the sensitive nature of data collected by activity trackers, the model was extended to include a privacy construct to determine if privacy concerns increase avoidance motivation. Additionally, perceived susceptibility was proposed as an antecedent to perceived severity in the threat calculus.  When compared to the original TTAT test and other studies based on the TTAT model, this study further confirmed the suitability of the model for evaluating avoidance motivations and behaviors, and improves understanding of the threat calculus involving perceived susceptibility, perceived severity, and perceived threat.

A comparison of the results analyzing the significance of each construct in this and prior studies is provided in Table 9.  As illustrated, avoidance motivation was a significant predictor of avoidance behavior in each study.  Perceived threat and safeguard effectiveness both had a significant and positive influence on avoidance motivation. Likewise, perceived severity had a significant and strong effect on perceived threat. Safeguard cost had a significant but negative influence on avoidance motivation in most studies, indicating that as safeguard costs increase, users are less motivated to implement the safeguarding measure.  However, for this study safeguard cost was not significant. Self-efficacy generally indicated a significant effect on avoidance motivation, although one study found it was not significant.  Additionally, perceived susceptibility was significant in three of the four studies that had a direct path to perceived threat

(Arachchilage & Love, 2013; Liang & Xue, 2010; Young et al., 2016, 2017)

Table 9 - Comparison of TTAT Results

| | Liang & Xue (2010) | Arachchilage & Love (2013) | Young, Carpenter, & McLeod (2016) | Young, Carpenter, & McLeod (2017) | Boysen (2018) |
|---|---|---|---|---|---|
| Perceived Severity (SEV→THR) | (.27) .01 | (.50) .01 | (.59) .01 | (.57) .01 | (.51) .01 |
| Perceived Susceptibility (SUS→THR) | (.41) .01 | (.36) .01 | (.05) .24 | (.18) .01 | |
| Perceived Susceptibility (SUS→SEV→THR) | | | | (.37) .01 | (.40) .01 |
| Perceived Severity X Perceived Susceptibility | (.10) n.s. | (.59) .01 | (-.02) .71 | | |
| Perceived Threat | (.26) .01 | (.39) .01 | (.10) .06 | (.12) .01 | (.24) .04 |
| Avoidance Motivation | (.43) .01 | (.39) .01 | (.75) .01 | (.82) .01 | (.46) .01 |
| Distrust Propensity | | | | (.10) .01 | |
| Impulsivity | | | | (.06) .05 | |
| Privacy Concerns | | | | | (.13) .20 |
| Risk Propensity | | | | (-.16) .01 | |
| Safeguard Cost | (-.14) .05 | (-.11) .05 | (-.30) .01 | (-.32) .01 | (-.20) .06 |
| Safeguard Effectiveness | (.33) .01 | (.39) .01 | (.33) .01 | (.42) .01 | (.29) .01 |
| Self-Efficacy | (.19) .05 | (.16) .01 | (.10) .01 | (.03) .28 | (.33) .01 |
| Threat X Safeguard Effectiveness | (-.18) .05 | (.45) .01 | (-.02) .67 | | |

Note: (B) p = path value and p value

The modifications to the TTAT model for this study returned interesting results. For instance, positioning perceived susceptibility as an antecedent to perceived severity in the threat calculus resulted in a strong and significant effect. This suggests that users might first evaluate the likelihood of falling victim to malware before they determine the severity of such a threat. This relationship was repeated and also found to be significant in a larger study by Young, Carpenter, and McLeod (Young et al., 2017), indicating a revision to the threat calculus might provide more consistent results than previous tests of the TTAT model. Future studies measuring the modified threat calculus would help determine if the revisions are applicable in various contexts.

Surprisingly, privacy concerns were not significant in determining avoidance motivation.  Wearable fitness devices collect sensitive data that are closely related to protected health information.  However, user responses suggested a lack of concern for the privacy of those data.  This may be due in part to the limited age range of the study respondents.  Also, participants in this age group may be less likely to have experienced data breaches and privacy violations.

The results of this study provide insight into users' motivations to avoid malicious threats to IT.  Prior research confirming the original TTAT model's suitability for evaluating technology threat avoidance verifies the stability of the foundational constructs.  However, the lack of consistency in the variables associated with the threat calculus indicates the need to consider other factors.  Additional variables such as risk propensity and distrust propensity may provide a more reliable measurement of the threat appraisal process (Young et al., 2017).  As the need to better understand users' threat avoidance motivations and behaviors increases, a modified and improved TTAT model might benefit researchers.

# 9. CONCLUSION

This research attempted to understand and refine the threat calculus in Technology Threat Avoidance Theory (TTAT) in order to provide a more representative model for analyzing user motivations to employ safeguarding measures. In addition to the revised threat calculus contained in the model for this study, a privacy construct was introduced to further extend and analyze user motivations. While privacy concerns were not significant in the study, the revised threat calculus was fully supported. However, the variance in perceived threat and avoidance motivation was lower in this study than in the original TTAT test by Liang & Xue (2010), indicating other variables may be affecting threat perceptions and avoidance motivation. To further explain the variance in threat perceptions, researchers might consider possible antecedents to privacy concerns. Just as users must evaluate susceptibility and severity to determine threat perceptions, they might also consider various factors when analyzing their privacy concerns. The amount of personal health information stored within complex systems, such as the Fitbit system, calls for further consideration of users' privacy concerns. Constructs related to negative experiences with data breaches and privacy violations could provide further insight into the development of privacy concerns and the resulting avoidance motivations. Additionally, as Young et al. (2017) proposed, additional constructs could help explain more of the variance in avoidance motivation.

## Limitations

While this research made progress towards a model more suited for analyzing technology threat avoidance, the study design introduced some limitations. Because participation was limited to college freshmen, respondents were all in the same age group. Future work should employ a more heterogeneous sample in order to improve generalizability.

Another concern is related to the items used to measure self-efficacy. As noted by Young et al. (2017), the measures for self-efficacy might need to be redesigned to be more conducive in the context of technology threat avoidance behaviors. The items used by Liang and Xue (2010) were slightly modified for this study and might not provide a true indication of users' confidence in implementing a safeguarding measure. While self-efficacy was found to be significant with this study group, prior inconsistencies suggest modifications to the self-efficacy measure might be beneficial.

## Contributions and Implications for Future Research

The results provide several contributions for researchers and organizations. By continuing to refine and evaluate the TTAT model in various contexts, researchers have access to a modified model that might better assess and determine user motivations and behaviors. The model for this study introduced the privacy construct to TTAT. Although it was not found to be significant with this study group, it deserves further evaluation. Theoretically considering it as an antecedent in the model might provide an understanding of the role privacy plays in user motivations. This study was restricted to freshman college students in the 18-24 age group, suggesting individuals in that age group might have different perspectives on privacy of personal fitness data. Also, due to their age, the participants in this study may have limited exposure to data and privacy breaches, minimizing their concerns about privacy. A larger study with a more heterogeneous group of participants might yield different responses regarding privacy concerns.

Organizations can benefit from these results, because the model provides a framework for understanding how users develop threat perceptions.  Previous studies returned mixed results for the threat calculus.  Considering perceived susceptibility as an antecedent to perceived severity indicated a significant effect on threat perceptions.  As such, organizations should consider addressing users' perceptions about susceptibility when determining the best method for motivating users to comply with security policies. Because this is the initial study relocating perceived susceptibility in the threat calculus, future research in different contexts would assist in determining if this modification returns consistently significant results.

# APPENDIX SECTION

## Appendix A—Factor Loadings

| | BEH | CST | EFF | MOT | PRI | SEV | SLF | SUS | THR |
|---|---|---|---|---|---|---|---|---|---|
| BEH1 | **0.97** | 0.00 | 0.30 | 0.47 | 0.12 | 0.05 | 0.32 | -0.06 | 0.15 |
| BEH2 | **0.96** | -0.01 | 0.25 | 0.43 | 0.02 | -0.04 | 0.36 | -0.09 | 0.10 |
| CST1 | -0.08 | **0.93** | 0.30 | 0.14 | 0.29 | 0.29 | 0.33 | 0.24 | 0.36 |
| CST4 | 0.08 | **0.90** | 0.36 | 0.12 | 0.14 | 0.20 | 0.41 | 0.08 | 0.19 |
| CST5 | 0.11 | **0.75** | 0.28 | 0.01 | 0.22 | 0.20 | 0.29 | 0.15 | 0.11 |
| EFF1 | 0.25 | 0.30 | **0.91** | 0.42 | 0.21 | 0.26 | 0.38 | 0.10 | 0.35 |
| EFF2 | 0.28 | 0.33 | **0.94** | 0.43 | 0.28 | 0.29 | 0.36 | 0.11 | 0.36 |
| EFF3 | 0.27 | 0.33 | **0.95** | 0.44 | 0.14 | 0.32 | 0.41 | 0.12 | 0.28 |
| EFF4 | 0.28 | 0.37 | **0.97** | 0.45 | 0.13 | 0.30 | 0.44 | 0.06 | 0.30 |
| EFF5 | 0.26 | 0.36 | **0.95** | 0.41 | 0.15 | 0.30 | 0.42 | 0.09 | 0.27 |
| EFF6 | 0.28 | 0.32 | **0.95** | 0.47 | 0.10 | 0.26 | 0.48 | 0.04 | 0.26 |
| MOT1 | 0.47 | 0.18 | 0.46 | **0.98** | 0.20 | 0.30 | 0.46 | 0.07 | 0.45 |
| MOT2 | 0.47 | 0.15 | 0.45 | **0.99** | 0.19 | 0.25 | 0.42 | 0.10 | 0.43 |
| MOT3 | 0.44 | 0.07 | 0.45 | **0.98** | 0.13 | 0.24 | 0.45 | 0.06 | 0.40 |
| PRI1 | 0.12 | 0.22 | 0.14 | 0.21 | **0.96** | 0.31 | -0.09 | 0.44 | 0.28 |
| PRI2 | 0.06 | 0.26 | 0.19 | 0.15 | **0.94** | 0.32 | -0.06 | 0.54 | 0.30 |
| PRI3 | 0.05 | 0.21 | 0.18 | 0.17 | **0.98** | 0.30 | -0.12 | 0.50 | 0.34 |
| PRI4 | 0.05 | 0.25 | 0.16 | 0.12 | **0.98** | 0.30 | -0.11 | 0.49 | 0.35 |
| SEV2 | -0.08 | 0.17 | 0.22 | 0.09 | 0.27 | **0.80** | 0.02 | 0.33 | 0.25 |
| SEV3 | 0.03 | 0.27 | 0.31 | 0.32 | 0.38 | **0.92** | 0.19 | 0.39 | 0.53 |
| SEV4 | 0.07 | 0.27 | 0.24 | 0.32 | 0.23 | **0.89** | 0.28 | 0.33 | 0.51 |
| SEV5 | -0.03 | 0.23 | 0.31 | 0.12 | 0.22 | **0.90** | 0.13 | 0.31 | 0.37 |
| SEV6 | 0.01 | 0.24 | 0.26 | 0.24 | 0.28 | **0.89** | 0.21 | 0.41 | 0.50 |
| SLF1 | 0.25 | 0.38 | 0.50 | 0.39 | -0.06 | 0.22 | **0.85** | 0.01 | 0.28 |
| SLF2 | 0.31 | 0.30 | 0.40 | 0.39 | -0.14 | 0.17 | **0.91** | 0.04 | 0.26 |
| SLF3 | 0.36 | 0.45 | 0.38 | 0.44 | -0.06 | 0.20 | **0.91** | 0.05 | 0.38 |
| SLF4 | 0.26 | 0.29 | 0.28 | 0.31 | -0.08 | 0.12 | **0.83** | 0.00 | 0.32 |
| SLF5 | 0.26 | 0.42 | 0.36 | 0.34 | -0.11 | 0.23 | **0.92** | 0.02 | 0.35 |
| SLF6 | 0.37 | 0.30 | 0.39 | 0.47 | -0.08 | 0.13 | **0.87** | -0.05 | 0.29 |
| SUS1 | -0.07 | 0.08 | 0.07 | 0.07 | 0.37 | 0.36 | -0.14 | **0.78** | 0.09 |
| SUS2 | -0.08 | 0.15 | 0.01 | 0.04 | 0.51 | 0.32 | -0.02 | **0.87** | 0.26 |
| SUS3 | -0.12 | 0.14 | 0.05 | -0.03 | 0.43 | 0.27 | -0.06 | **0.92** | 0.12 |
| SUS4 | -0.09 | 0.18 | 0.06 | 0.06 | 0.40 | 0.34 | 0.10 | **0.93** | 0.22 |
| SUS5 | 0.00 | 0.23 | 0.16 | 0.20 | 0.49 | 0.42 | 0.05 | **0.91** | 0.34 |
| SUS6 | -0.07 | 0.19 | 0.09 | 0.01 | 0.44 | 0.37 | 0.09 | **0.85** | 0.32 |
| THR1 | 0.18 | 0.18 | 0.14 | 0.31 | 0.44 | 0.53 | 0.22 | 0.37 | **0.83** |
| THR2 | 0.05 | 0.20 | 0.32 | 0.35 | 0.32 | 0.49 | 0.30 | 0.34 | **0.86** |
| THR3 | 0.14 | 0.35 | 0.31 | 0.38 | 0.11 | 0.33 | 0.37 | 0.02 | **0.79** |
| THR4 | 0.07 | 0.32 | 0.30 | 0.39 | 0.16 | 0.28 | 0.29 | 0.09 | **0.83** |

## Appendix B—Survey Instrument

| Construct | Indicator | Indicator Text |
|---|---|---|
| Perceived Susceptibility | SUS1 | It is extremely likely that the Fitbit system will contain malware in the future. |
| | SUS2 | The chances of getting malware on the Fitbit system are great. |
| | SUS3 | There is a good possibility that the Fitbit system will contain malware at some point. |
| | SUS4 | There is a good chance that there will be malware on the Fitbit system at some point in the future. |
| | SUS5 | The Fitbit system is at risk of becoming a victim of malware. |
| | SUS6 | It is possible that the Fitbit system will experience a malware incident. |
| Perceived Severity | SEV1 | The consequences of losing my fitness data from the Fitbit system could be severe. |
| | SEV2 | Malware could steal my fitness data from the Fitbit system without my knowledge. |
| | SEV3 | My fitness data collected by malware could be misused by cyber criminals. |
| | SEV4 | Malware could invade my privacy through the Fitbit system. |
| | SEV5 | My fitness data collected by malware could be subjected to unauthorized secondary use. |
| | SEV6 | Fitness data collected by malware could be used to commit crimes against me. |

| Construct | Indicator | Indicator Text |
|---|---|---|
| Perceived Threat | THR1 | The consequences of getting malware on the Fitbit system threatens me. |
| | THR2 | Malware is a danger to the Fitbit system. |
| | THR3 | It would be awful if the Fitbit system was infected by malware. |
| | THR4 | It would be risky to use the Fitbit system if it had malware. |
| | THR5 | I am worried that using the Fitbit system will negatively affect me. |
| | THR6 | I am scared that the Fitbit system will have harmful consequences for me. |
| Privacy Concerns | PRI1 | I am concerned that the information I submit to the Fitbit system could be misused. |
| | PRI2 | I am concerned that a person can find private information about me on the Fitbit system. |
| | PRI3 | I am concerned about submitting information on the Fitbit system, because of what others might do with it. |
| | PRI4 | I am concerned about submitting information on the Fitbit system, because it could be used in a way I did not foresee. |
| Self-Efficacy | SLF1 | I could successfully install and use security software if…I had seen someone else do it before trying myself. |
| | SLF2 | I could successfully install and use security software if…I could call someone for help if I got stuck. |
| | SLF3 | I could successfully install and use security software if…someone helped me get started. |
| | SLF4 | I could successfully install and use security software if…I had a lot of time to complete the task. |
| | SLF5 | I could successfully install and use security software if…someone showed me how to do it first. |
| | SLF6 | I could successfully install and use security software if…I had used a similar package before. |

| Construct | Indicator | Indicator Text |
|---|---|---|
| Safeguard Cost | CST1 | I don't have security software on the Fitbit system because I don't know how to get it. |
| | CST2 | I don’t have security software on the Fitbit system because it may cause problems with other programs. |
| | CST3 | I don’t have security software on the Fitbit system because installing it is too much trouble. |
| | CST4 | I don't have security software on the Fitbit system because I'm not aware such software exists. |
| | CST5 | I don't have security software on the Fitbit system because I don't think such software is worth the cost. |
| Safeguard Effectiveness | EFF1 | Security software would be useful for detecting and removing malware from the Fitbit system. |
| | EFF2 | Security software would increase my ability to protect the Fitbit system from malware. |
| | EFF3 | Security software would enable me to search for and remove malware from the Fitbit system faster. |
| | EFF4 | Security software would enhance my effectiveness in finding and removing malware on the Fitbit system. |
| | EFF5 | Security software would make it easier to search for and remove malware on the Fitbit system. |
| | EFF6 | Security software would increase my productivity in searching for and removing malware on the Fitbit system. |
| Avoidance Motivation | MOT1 | I intend to use security software to avoid malware breaches. |
| | MOT2 | I will use security software to avoid malware breaches. |
| | MOT3 | I plan to use security software to avoid malware breaches. |
| Avoidance Behavior | BEH1 | I run security software regularly to remove malware. |
| | BEH2 | I update my security software regularly. |

# REFERENCES

Ajzen, I. (1985). From intentions to actions: A Theory of Planned Behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11-39). Berlin, Germany: Springer.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Alarcón, D., & Sánchez, J. A. (2015). Assessing convergent and discriminant validity in the ADHD-R IV rating scale: User-written commands for Average Variance Extracted (AVE), Composite Reliability (CR), and Heterotrait-Monotrait ratio of correlations (HTMT). *Spanish STATA Meeting.* Seville, Spain: Universidad Pablo de Olavide.

Albarracin, D., Johnson, B. T., Fishbein, M., & Muellerleile, P. A. (2001). Theories of Reasoned Action and Planned Behavior as models of condom use: A meta-analysis. *Psychological Bulletin 127*(1), 142-161.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423. doi:10.1037/0033-2909.103.3.411

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*(3), 706-714. doi:10.1016/j.chb.2012.12.018

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior, 45*, 93-98. doi:10.1016/j.chb.2014.11.075

Bagozzi, R. P., Wong, N., Abe, S., & Bergami, M. (2000). Cultural and situational contingencies and the Theory of Reasoned Action: Application to fast food restaurant consumption. *Journal of Consumer Psychology, 9*(2), 97-106. doi:10.1207/S15327663JCP0902_4

Barcena, M. B., Wueest, C., & Lau, H. (2014). How safe is your quantified self? *Security Response*. Mountainview, CA: Symantec.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM, 48*(4), 101-106. doi:10.1145/1053291.1053295

Caldwell, S. (2013). *Statistics unplugged* (4th ed.). Belmont, CA: Wadsworth Cengage Learning.

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222. doi:10.25300/misq/2016/40.1.09

Chenoweth, T., Minch, R., & Gattiker, T. (2009). *Application of Protection Motivation Theory to adoption of protective technologies.* Paper presented at the 42nd Hawaii International Conference on System Sciences, Waikoloa, HI.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.

Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*, 334-345. doi:10.1016/j.chb.2016.08.034

Clemons, E. K., & Wilson, J. S. (2015). Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications. *Journal of Management Information Systems, 32*(2), 40-70. doi:10.1080/07421222.2015.1063277

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security, 48*, 281-297. doi:10.1016/j.cose.2014.11.002

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security, 24*(1), 116-134. doi:10.1108/ICS-04-2015-0018

Davis, F. D., Jr. (1986). *A Technology Acceptance Model for empirically testing new end-user information systems: Theory and results.* (Doctoral dissertation, Massachusetts Institute of Technology). Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/15192/14927137-MIT.pdf?sequence=2

DeVellis, R. F. (2003). *Scale development: Theory and applications* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. doi:10.1287/isre.1060.0080

Fishbein, M. (1979). A Theory of Reasoned Action: Some applications and implications. *Nebraska Symposium on Motivation, 27*, 65-116.

Fisher, W. A., Fisher, J. D., & Rye, B. J. (1995). Understanding and promoting AIDS-preventive behavior: Insights from the Theory of Reasoned Action. *Health Psychology, 14*(3), 255-264. doi:10.1037/0278-6133.14.3.255

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. doi:10.2307/3151312

Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii-A7. doi:10.2307/23044042

George, J. F. (2004). The Theory of Planned Behavior and Internet purchasing. *Internet Research, 14*(3), 198-212. doi:10.1108/10662240410542634

Godin, G., Valois, P., & Lepage, L. (1993). The pattern of influence of perceived behavioral control upon exercising behavior: An application of Ajzen's Theory of Planned Behavior. *Journal of Behavioral Medicine, 16*(1), 81-102. doi:10.1007/BF00844756

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61-84. doi:10.1111/j.1365-2575.2012.00420.x

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

Hu, P. J., Chau, P. Y., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the Technology Acceptance Model using physician acceptance of telemedicine technology. *Journal of Management Information Systems, 16*(2), 91-112. doi:10.1080/07421222.1999.11518247

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566. doi:10.2307/25750691

Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba, B. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Issues in Information Systems, 11*(1), 9-16.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402. doi:10.1057/ejis.2008.29

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS quarterly*, 183-213. doi:10.2307/249751

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454. doi:10.1080/01449290600879344

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90. doi:10.2307/20650279

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.

Lu, H.-P., Hsu, C.-L., & Hsu, H.-Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security, 13*(2), 106-120. doi:10.1108/09685220510589299

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi:10.1016/0022-1031(83)90023-9

Manstead, A. S. R., Proffitt, C., & Smart, J. L. (1983). Predicting and understanding mothers' infant-feeding intentions and behavior: Testing the Theory of Reasoned Action. *Journal of Personality and Social Psychology, 44*(4), 657-671. doi:10.1037/0022-3514.44.4.657

Manzano, D. L. (2012). *The cybercitizen dimension: A quantitative study using a threat avoidance perspective.* (Doctoral dissertation, Capella University). Available from ProQuest Dissertations and Theses database. (UMI No. 3513688)

Matt, C., & Peckelsen, P. (2016). *Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior.* Paper presented at the 49th Hawaii International Conference on System Sciences, Koloa, Hawaii.

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of Reasoned Action application for green information technology acceptance. *Computers in Human Behavior, 36*, 29-40.

Moar, J. (2016). Fitness wearables: Time to step up [White paper]. Basingstoke, England: Juniper Research.

Mwagwabi, F. (2015). *A Protection Motivation Theory approach to improving compliance with password guidelines.* (Doctoral dissertation, Murdoch University). Retrieved from http://researchrepository.murdoch.edu.au/id/eprint/27070

Norman, P., & Conner, M. (2005). The Theory of Planned Behavior and exercise: Evidence for the mediating and moderating roles of planning on intention-behavior relationships. *Journal of Sport and Exercise Psychology, 27*(4), 488-504. doi:10.1123/jsep.27.4.488

Orbeil, S., Hodgkins, S., & Sheeran, P. (1997). Implementation intentions and the Theory of Planned Behavior. *Personality and Social Psychology Bulletin, 23*(9), 945-954.

Ouyang, X. (2016). Why hackers love health apps: Most health apps don't have good privacy or security safeguards. *PC World*. Retrieved from http://www.pcworld.com/article/3099004/software/why-hackers-love-health-apps.html

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the Theory of Planned Behavior. *MIS Quarterly, 30*(1), 115-143. doi:10.2307/25148720

Ramayah, T., Rouibah, K., Gopi, M., & Rangel, G. J. (2009). A decomposed Theory of Reasoned Action to explain intention to use Internet stock trading among Malaysian investors. *Computers in Human Behavior, 25*(6), 1222-1230. doi:10.1016/j.chb.2009.06.007

Rauniar, R., Rawski, G., Yang, J., & Johnson, B. (2014). Technology Acceptance Model (TAM) and social media usage: An empirical study on Facebook. *Journal of Enterprise Information Management, 27*(1), 6-30. doi:10.1108/JEIM-04-2012-0011

Rehman, T., McKemey, K., Yates, C., Cooke, R., Garforth, C., Tranter, R., . . . Dorward, P. (2007). Identifying and understanding factors influencing the uptake of new technologies on dairy farms in SW England using the Theory of Reasoned Action. *Agricultural Systems, 94*(2), 281-293. doi:10.1016/j.agsy.2006.09.006

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0 (beta). Retrieved from www.smartpls.com

Roca, J. C., García, J. J., & de la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113. doi:10.1108/09685220910963983

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

Schifter, D. E., & Ajzen, I. (1985). Intention, perceived control, and weight loss: An application of the Theory of Planned Behavior. *Journal of Personality and Social Psychology, 49*(3), 843-851. doi:10.1037/0022-3514.49.3.843

Shimp, T. A., & Kavas, A. (1984). The Theory of Reasoned Action applied to coupon usage. *Journal of Consumer Research, 11*(3), 795-809. doi:10.1086/209015

Statsoft, I. (2013). *Electronic statistics textbook.* Retrieved from http://www.statsoft.com/Textbook

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53-55. doi:10.5116/ijme.4dfb.8dfd

Trochim, W. M. K. (2006). *The research methods knowledge base.* Retrieved from http://www.socialresearchmethods.net/kb/

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A Protection Motivation Theory perspective. *Computers & Security, 59*, 138-150. doi:10.1016/j.cose.2016.02.009

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679-722.

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

Venkatesh, V., Morris, M. G., & Ackerman, P. L. (2000). A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. *Organizational Behavior and Human Decision Processes, 83*(1), 33-60. doi:10.1006/obhd.2000.2896

Vinzi, V. E., Trinchera, L., & Amato, S. (2010). *PLS path modeling: from foundations to recent developments and open issues for model assessment and improvement*: Springer.

Webley, P., & Lea, S. (1997). PSY6003 Advanced statistics: Multivariate analysis II: Manifest variables analyses Retrieved from http://people.exeter.ac.uk/SEGLea/multvar2/pathanal.html

Widup, S., Bassett, G., Hylender, D., Rudis, B., & Spitler, M. (2015). *2015 protected health information data breach report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_2015-protected-health-information-data-breach-report_en_xg.pdf

Woon, I., Tan, G.-W., & Low, R. (2005). *A Protection Motivation Theory approach to home wireless security*. Paper presented at the 26th International Conference on Information Systems, Las Vegas, NV.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824.

Xue, Y., Liang, H., Mbarika, V., Hauser, R., Schwager, P., & Getahun, M. K. (2015). Investigating the resistance to telemedicine in Ethiopia. *International Journal of Medical Informatics, 84*(8), 537-547. doi:10.1016/j.ijmedinf.2015.04.005

Yaraghi, N. (2016). *Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches*. Retrieved from https://www.brookings.edu/research/hackers-phishers-and-disappearing-thumb-drives-lessons-learned-from-major-health-care-data-breaches/

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407-415.

Young, D., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A Technology Threat Avoidance replication. *AIS Transactions on Replication Research, 2*(1), 1-17. doi:10.17705/1atrr.00015

Young, D., Carpenter, D., & McLeod, A. (2017). *Refining Technology Threat Avoidance Theory*. Manuscript submitted for publication.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448-484.