Mobile Device Security: Perspectives of Future Healthcare Workers

Abstract
Healthcare data breaches on mobile devices continue to increase, yet the healthcare industry has not adopted mobile device security standards. This increase is discerning because these individuals are often accessing patient's protected health information on these personal mobile devices which could lead to a data breach. This deficiency led the researchers to explore the perceptions of future healthcare workers on mobile device security. The investigators designed and distributed a survey to healthcare students to determine the perspectives on mobile device security based on the Technology Threat Avoidance Theory. Three hundred and thirty-five students participated in the survey. Data was analyzed to determine participant's perceptions about security threats, safeguard effectiveness, safeguard costs, self-efficacy, susceptibility, severity and their motivation and behavior toward securing their mobile devices. Awareness of interventions to protect mobile devices was also examined. Results indicate that while future healthcare professionals perceive the severity of threats to their mobile data, they do not feel personally susceptible. Additionally, participants were knowledgeable about security safeguards, but mixed on costs and problems related to adopting these measures. These findings indicate increasing security awareness for healthcare professionals should be a priority.

Keywords: mobile security, healthcare, data breaches, security threat, safeguard effectiveness, safeguard cost, susceptibility, threat severity, technology threat avoidance theory

Introduction

Healthcare professionals are responsible for protecting the privacy, security, and confidentiality of electronic health information[1]. Although the use of mobile devices by healthcare professionals increases connectivity and enables remote logins to electronic health records, it also introduces many significant new security risks[2, 3]. Since over 48 percent of all healthcare data breaches since 2010 involved a laptop, desktop, or mobile devices,[2] it is not surprising that 168 of the 1419 healthcare data breaches affecting over 500 individuals involved the theft or loss of vulnerable mobile devices[4, 5].

Despite the increase in healthcare data breaches involving mobile devices the healthcare industry currently has not adopted standards for mobile devices, indicating a need for strong mobile device security policies[6, 7]. The National Institute of Standards and Technology (NIST) recommends increasing end user's awareness of mobile device security measures, such as encrypting sensitive files, reporting loss or theft of the devices, and procedures for correctly securing mobile devices or ensuring sensitive information cannot be stored on such devices[8]. A report by the Healthcare Information and Management Systems Society (HIMSS) Mobile Security Work Group rates the threat levels for breaches involving access, control, encryption, inappropriate or insecure storage, backups, and mobile device issues as high, and malware threats as moderate[9].

With the industry emphasis placed on securing these devices, the central issue examined by this study is the need to understand the perceptions of future healthcare professionals regarding

mobile device security. This topic is important because data breaches on healthcare mobile devices disrupt access to vital patient care information, and may result in unauthorized disclosure of protected health information[7]. By exploring the perception of security and vulnerability, this paper will help us determine if organizations need to increase security awareness among healthcare professionals through training and other programs.

Background

Although healthcare practitioners face many challenges related to understanding mobile device security, there is a lack of evidence regarding their perceptions of mobile device security[10-13]. Specifically, the researchers found very few studies that examined the perceptions of healthcare students or professionals on the severity of mobile device security threats, or the level of adoption of preventative mobile security measures[14, 15].

According to the DHHS annual breach report, there have been 710 reported breaches affecting 22.5 million individuals from September 2009 to December 2012[16]. In this report, it is noted that 54 percent of all breaches occurring between 2011-2012 were hacking/IT incidents and unauthorized access/disclosure[16]. Subsequently in 2012, healthcare organizations experienced fewer hacking/IT incidents (9 percent) and unauthorized access/disclosure decreased by 18 percent, but these two causes together still accounted for over 44 percent of all individuals affected by a data breach. The types of devices used in 2012 were similar to 2011, with desktop computers (12 percent), laptops (27 percent), and other portable electronic devices (9 percent), accounting for the majority of the breaches.

A 2015 report by the DHHS shows the number of security breaches is increasing. See Table 1 for the Top 10 Data Healthcare Breaches occurring in 2015. In summary, the data in this report and the federal focus on mobile device security issues signals a necessity for adoption of better healthcare security practices to safeguard protected patient's PHI.

In a study conducted by Ponemon[17], over 88 percent of healthcare organizations allow employees and medical staff to use of personal mobile devices including tablets and smart phones. These organizations have control over whether they will adopt security features such as anti-malware software, spyware protection and firewalls on their corporate owned devices. However, these organizations have less control over whether these mobile devices adopt anti-malware (23 percent), scan the devices prior to connection to confidential data (22 percent), or remove vulnerable mobile applications prior to accessing the system (14 percent).

Given the large number of mobile healthcare related data breaches and lack of regulations governing security, the aim of the study is to examine the perceptions of future health professionals concerning security threats, system susceptibility, threat severity, costs of providing safeguards, and the effectiveness of those safeguards in preventing mobile device security breaches in the healthcare environment.

Theoretical Framework

A review of security literature provided a theoretical framework for examining these issues. Liang and Xue's Technology Threat Avoidance Theory (TTAT)[18] explores whether individuals create a mental threat perception when they feel a danger is likely to cause undesirable

consequences. This is important because undesirable consequences may deter practitioners from adopting the security safeguards. TTAT also includes the effectiveness of safeguards and self-efficacy because an individual's perception of these variables impacts their motivation to avoid security breaches. This theory is also useful in examining how healthcare professionals are employing avoidance mechanism to ensure their mobile device is safeguarded from security breaches. Figure 1 shows the Technology Threat Avoidance Theory model.

In addition to TTAT constructs, the researchers wanted to explore if the respondents were aware of various security interventions for ameliorating loss and facilitating recovery from security breaches. Researchers included survey questions about awareness of specific security interventions adapted from general security awareness questions used by Bulgurcu, Cavusoglu and Benbasat[19].

Research Questions

Utilizing validated survey items from these two prior research studies, the authors examined the following research questions:

1. How do healthcare professionals perceive susceptibility and severity of security threats on personal mobile devices?
2. Are healthcare professionals aware of ways to reduce security threats on personal mobile devices?
3. Do they know how to use and adopt effective mechanisms to reduce security threats on personal mobile devices?

Methods

The purpose of this exploratory study was to analyze the perceptions of mobile device security from the viewpoint of future healthcare professionals. The study was conducted using a survey design. The study site was the College of Health Professions at a large state university in the Southern United States. Data were collected using a survey designed by the researchers that contained closed ended questions. Microsoft Excel was utilized to generate descriptive statistics for respondents' survey data.

Participants

The participants chosen for this study were campus-based and online students (n=443) enrolled in a College of Health Professions course. Participants were selected using convenience sampling. The participants are future healthcare professionals and thus potential future mobile device users. Examples of participants' majors include health information management, physical therapy, and communication disorders.

Study Variables

This work used study variables incorporated from previously validated works. Definitions for Susceptibility, Severity, Threat, Effectiveness, Costs, Self-Efficacy, Motivation, Behavior and Awareness were drawn from Liang and Xu[18] and Bulgurcu, Cavusoglu, and Benbasat[19]. See Table 2 for a mapping of research questions to variables.

Instrument

Data was collected from a survey adapted by the researchers from two prior projects. The majority of the questions were taken from the survey used to test the TTAT model which focused on measures of security behaviors used to avoid security breaches. The questions examined whether individual security behaviors were motivated by knowledge of security threats, safeguards, susceptibility, severity and awareness. Using these measures, this study aimed to determine how future healthcare professionals perceived threats to their mobile devices and what interventions they considered when responding to those threats. TTAT is depicted in Figure 1. In addition to those constructs, to explore whether the individuals were aware of intervention mechanisms for mobile devices such as anti-malware, passwords or biometrics, encryption, anti-theft apps, and backing-up the mobile device. These questions were adapted from the study completed by Bulgurcu, Cavusoglu and Benbasat[19].

The survey was distributed in paper form to many of the campus-based students, as well as through a Survey Monkey web link for the remaining campus and online students. The survey consisted of 47 Likert-scale 7-point questions (1=Strongly Disagree, 7= Strongly Agree) inviting respondents to rate their perceptions of the security of their mobile device, awareness of security issues, and behaviors toward protecting their mobile devices from security breaches. Typical questions asked participants to rate chances of breach on their mobile device or awareness of mobile device features like encryption or passwords. There were five demographic questions on participant's classification (e.g., freshman, sophomore), educational level, college major, gender, age and ethnicity.

Specifically, the scale used for this study measured whether individuals felt they were susceptible to security breaches (perceived susceptibility), whether they perceived a threat that their device could be compromised (perceived threat), and how severe the outcome from the breach would be (perceived severity). Safeguard cost and effectiveness are important considerations and the survey asked participants about these aspects (safeguard cost and safeguard effectiveness). The study also measured whether students felt they were capable of installing and using security mechanisms that prevent security breaches (self–efficacy), if they were motivated to secure their mobile device (motivation), and whether they actually secured their mobile device (behavior).

Procedures

During the Fall 2015 semester, the researchers obtained IRB approval and permission to distribute the survey to students in the college from the department chair. Next, individual department heads from the college of health professions were contacted to make them aware of the study and get permission to survey their students. Then one or more instructors in those departments that agreed to participate were contacted to obtain permission to distribute surveys to the students in their classes.

Students enrolled in campus classes either completed paper surveys or the online version of the survey. All online students were emailed a link to the web-based survey. All survey responses were anonymous. Data was abstracted manually from the paper surveys and exported from the online survey tool. Data was analyzed to understand whether respondents agreed or disagreed with the item questions.

Data Analysis

Descriptive statistics analysis was conducted to generate frequencies and percentages to describe the sample population. Similarly, data from the survey's Likert rating scale was consolidated and analyzed. Figure 2 presents a chart that shows composite percentages for the constructs in the TTAT model to summarize survey responses for technology threat avoidance.

Results

Demographics

Four hundred and forty-three students were invited to participate, and there were 335 students who completed the survey, resulting in a response rate of 76 percent. The majority of the participants were female 75 percent. Ages ranges from 18 to 59, sixty-six percent of the participants were 20-29 years of age. Forty-three percent were White, 12 percent were Black, 38 percent were Hispanic or Latino, 3 percent were Asian, and 4 percent were Other, and less than 1 percent were American Indian or Native Hawaiian or Pacific.

Student participants' classifications included freshman (< 1 percent), sophomore (37 percent), junior (44 percent), senior (14 percent), Masters (3 percent), PhD (< 1 percent), and other (<1 percent). Sixty-seven percent had some previous college, and 58 percent had an associate's degree. Thirty-five percent of the participants were physical therapy (35 percent), respiratory care (19 percent), or health information management (16 percent) majors. Table 3 shows participants' demographic data. Table 4 shows the participants' educational demographics results.

Mobile Device Survey Analysis

Mobile device survey analysis is reported by research question. First, to explore how healthcare professionals perceived susceptibility and severity of security threats on personal mobile devices, data on perceptions about users' susceptibility, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, motivation, behavior, and awareness were analyzed. The results indicated that 44 percent of the respondents did not believe that their mobile device would be susceptible to a security breach, however, 76 percent perceived a severe danger to their personal information. Individuals perceived the severity of threats to their mobile devices; thus it was no surprise 71 percent of the respondents indicated that their mobile device could be compromised when threatened by a security breach.

Discerningly, less than half of the participants (48 percent) felt that they were extremely likely to experience a security breach on their mobile device indicating that they don't feel susceptible to a breach. Privacy was important to the students, with 87 percent conveying that a security breach on their mobile device would invade their privacy. Interestingly, 79 percent felt it was risky to use their mobile device after a security breach due to perceived threat. Even though these individuals did not perceive that they were susceptible to a security breach, they recognized the threat that a security breach poses as well as the severity of those threats.

Second, to investigate if healthcare professionals were aware of ways to reduce security threats on personal mobile devices, safeguard effectiveness was examined. Eighty-two percent of the respondents believed that safeguards are effective, but only 36 percent of the students reporting

knowing where to get security safeguards. Most respondents, 67 percent believed they were capable of installing safeguards and managing safeguard configurations using help tools. Clearly these respondents deem safeguards effective and felt confident in their ability to use these tools.

Third, the study also examined if respondents were aware, motivated and behaved in secure ways to protect their mobile devices. Students were motivated to adopt security mechanisms, with 57 percent predicting they would use interventions to reduce security threats in the future. Conversely, only 42 percent reported that they are currently using security safeguards to protect their devices. This is concerning since the best way for individuals to reduce security threats is to apply safeguards to protect their mobile devices against security breaches.

Respondents were asked several questions related awareness. When asked if they were aware they could backup and recover their device, 70 percent recognized that backup mechanisms could prevent loss of information. Although 61 percent were knowledgeable about passwords or biometric access control, only 29 percent knew they could protect their mobile devices from malware and 27 percent understood that encryption would improve security. Additionally, 33 percent indicated they were knowledgeable about anti-theft apps for their mobile device.

Discussion

The results of this work provided interesting insights into the perceptions of mobile device security among future healthcare professionals. This work considered three research questions. First, respondents were asked about their perceived susceptibility and severity of security threats on personal mobile devices? Students did not believe their devices to be susceptible to security breaches, however responses were overwhelmingly affirmative to perceived severity, indicating they perceived severe threats to their personal information in a security breach. These results are not encouraging because perceptions of susceptibility are low while perceptions of severity are high. This begs the question—why?

Second, the study aimed to determine if healthcare professionals were aware of ways to reduce security threats on personal mobile devices. Overall the respondents reported that they were knowledgeable of some safeguards such as the ability to backups their device and use passwords or other authentication mechanism, their costs and availability to reduce threats and security breaches. These included knowing that safeguards could determine if a breach had occurred, could improve their ability to protect against a security breach, and could enhance the effectiveness in preventing future breaches. Being aware of these types of products is important in the mobile device environment as hackers and thieves ply their trade in mobile settings. Fewer individuals were aware of safeguards such as anti-malware, encryption, and theft apps. Thus, increasing future healthcare workers' awareness of these safeguards is essential in order to protect health information.

The third research question asked if respondents were adopting security measures for their personal mobile devices. Future health professionals reported their willingness to adopt security measures in the future, but few reported that they were already participating in accepted security behaviors. Respondents reported that they know where to get security safeguards but expressed concerns that security safeguards can cause problems with other apps or are too much trouble to install. Less than 29 percent reported that they update their devices on a regular basis. In

summary, respondents are mixed on the necessity of buying security software, and concerned about problems that may occur during and after installation of security software. Again, more training on mobile device security could help increase the security awareness and behavior of these future healthcare professionals.

Conclusion

Increasingly healthcare organizations are turning to mobile devices to improve usability, increase practitioner ease of use and untether devices. In doing so, healthcare system security is directly affected and thus healthcare information management professionals shoulder responsibility for protecting against security breaches and those that would do harm. Our results indicate that students as future healthcare professionals realize the severity of security threats but do not feel as though their mobile devices are susceptible. In addition, they feel that they are capable of using safeguards and that those safeguards are effective in preventing security breaches. While they are not adopting many of the mobile security safeguards, they are aware of most mechanisms used to support mobile security. These findings indicate increasing security awareness for healthcare professionals should be a priority as one pathway to increasing the adoption rate for mobile device security mechanisms.

This study is limited in a number of ways. First, respondents from a single institution were surveyed and this group may not be reflective of the population. Second, the items incorporated in the survey were taken from a single theory and publication. While this work shows strong results, other theories may provide implications that are more meaningful. Finally, we were limited to a single method and could not control for common method variance.

Future mobile security research should explore healthcare settings to see if the perceptions found in this work hold true for hospitals, physician's offices, pharmacies, etc. It would also be interesting to examine a variety of healthcare professions and how their perceptions vary from those noted in this work.

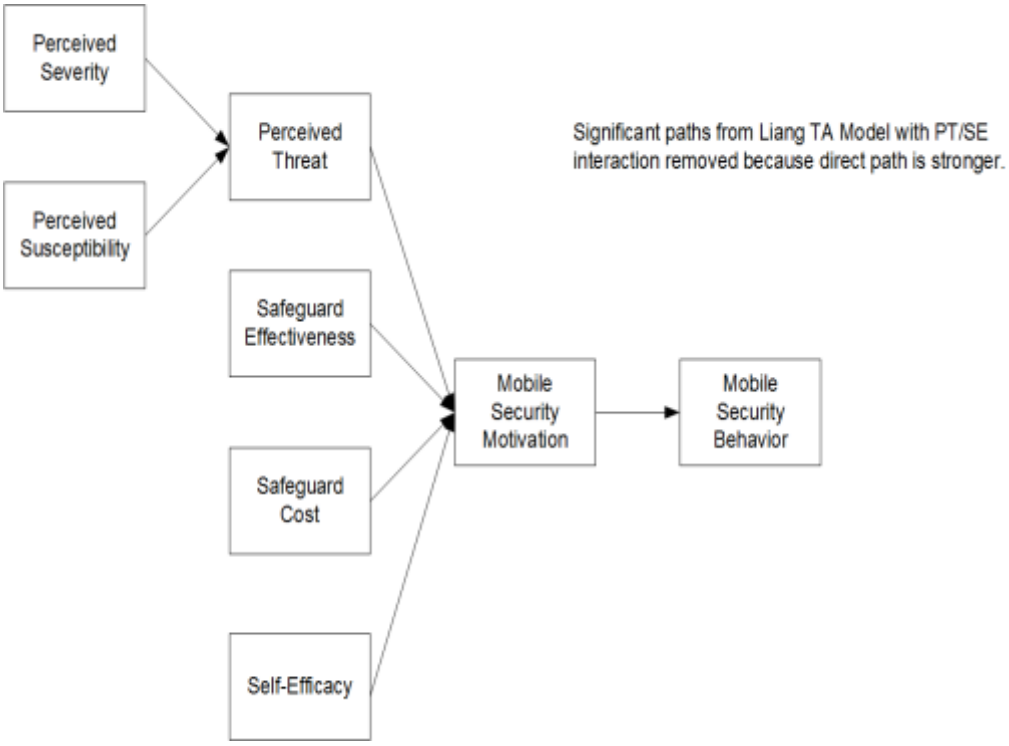
The role of future health professionals in securing mobile devices cannot be understated given the increasing number of data breaches in the healthcare industry. Because they will be responsible for the personal health information of others, it is important to understand their knowledge and perceptions of privacy, security and protective interventions. Examining the results of this survey, it is clear that much needs to be done to increase security awareness for health professionals.

Notes

1. AHIMA. "HIM Functions in Healthcare Quality and Patient Safety." *Journal of AHIMA* 82, no. 8. (2011): 42-54.
2. Butler, M. "Cracking Encryption: Despite Benefits, Technology Still Not Widely Used to Combat Multi-Million Dollar Breaches." *Journal of AHIMA* 86, no. 4. (2015): 18-23.
3. Kim, H.-S., K.-H. Lee, H. Kim and J. H. Kim. "Using Mobile Phones in Healthcare Management for the Elderly." *Maturitas* 79, no. 4. (2014): 381-388.
4. Department of Health & Human Services. "Breaches Affecting 500 or More Individuals". https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
5. Oscar, R. "Using Mobile Technology to Improve Health-Plan Utilization and Cut Costs." *Employment Relations Today* 40, no. 2. (2013): 21-27.
6. Thomas, G. "Secure Mobile Device Use in Healthcare Guidance from Hipaa and Iso17799." *Information Systems Management* 24, no. 4. (2007): 333-342.
7. Zeijour, C. and M. Twiggs. "Instituting an Enterprise-Wide Phi Disclosure Management Strategy." *Journal of AHIMA* 86, no. 4. (2015): 24-26.
8. Scarfone, K., M. Souppaya and M. Sexton. "Guide to Storage Encryption Technologies for End User Devices." *NIST Special Publication* 800, no. (2007):
9. Himss. "Security of Mobile Computing Devices in the Healthcare Environment." 2011.
10. Bowen, R. K. "The Evolving Role of the Privacy and Security Officer." *Journal of AHIMA* 86, no. 6. (2015): 46-47.
11. Crawford, M. "Everyday Ethics." *Journal of AHIMA* 82, no. 4. (2011): 30-33.
12. Flite, C. and L. Harman. "Code of Ethics: Principles for Ethical Leadership." *Perspectives in Health Information Management* no. (2013): 1-11.
13. Zapata, B. C., A. H. Hernández, A. Idri, J. L. Fernández-Alemán and A. Toval. "Mobile Phr's Compliance with Android and IOS Usability Guidelines." *Journal of Medical Systems* 38, no. 8. (2014):
14. Eastin, M. S. and R. LaRose. "Internet Self-Efficacy and the Psychology of the Digital Divide." *Journal of Computer-Mediated Communication* 6, no. 1. (2000): 0-0.
15. Stephens, P. "Validation of the Business Computer Self-Efficacy Scale: Assessment of the Computer Literacy of Incoming Business Students." *Journal of Educational Computing Research* 34, no. 1. (2006): 29-46.
16. Department of Health & Human Services. "Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2011 and 2012". http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf.
17. Ponemon Institute. "Fourth Annual Benchmark Study on Patient Privacy & Data Security". http://www.ponemon.org/library/archives/2014/03.
18. Liang, H. and Y. Xue. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *Journal of the Association for Information Systems* 11, no. 7. (2010): 394-413.
19. Bulgurcu, B., H. Cavusoglu and I. Benbasat. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS quarterly* 34, no. 3. (2010): 523-548.

Figure 1

Technology Threat Avoidance Model



Note: Diagram generate by researchers using Visio.

Table 1

Top Ten Healthcare Data Breaches in 2015 [4]

Type of Data Breach / Organization Experiencing Data Breach	**Numbers of Records**
Hacking/IT Incident	
Anthem	78,800,000
Premera	11,000,000
Excellus	10,000,000
UCLA Health	4,500,000
MIE	3,900,000
CareFirst	1,100,000
DMAS	697,586
Georgia Department of Community	557,779
Laptop Theft	
DJO Global	160,000

Table 2

Study Variables

Research Question	Measure	Definition
Question 1	Susceptibility	Individual's perception about whether he was susceptible to security breaches
	Severity	Individual's perception of how severe the outcome from the breach would be
	Threat	Whether the individual's expected their device would be compromised
Question 2	Effectiveness	The individual's perceived effectiveness of a safeguard
	Cost	The cost of implementing a safeguard
	Self-Efficacy	Whether individuals believe that they were capable of installing and using security mechanisms that prevent security breaches
Question 3	Motivation	Indicated if individual was motivated to secure the mobile device
	Behavior	Whether individuals actually secured their mobile device
	Awareness	Whether the individuals were aware of intervention mechanisms for mobile devices such as anti-malware, passwords or biometrics, encryption, anti-theft apps, and backing-up the mobile device

Figure 2

Summary of Composite Percentages Technology Threat Avoidance Responses

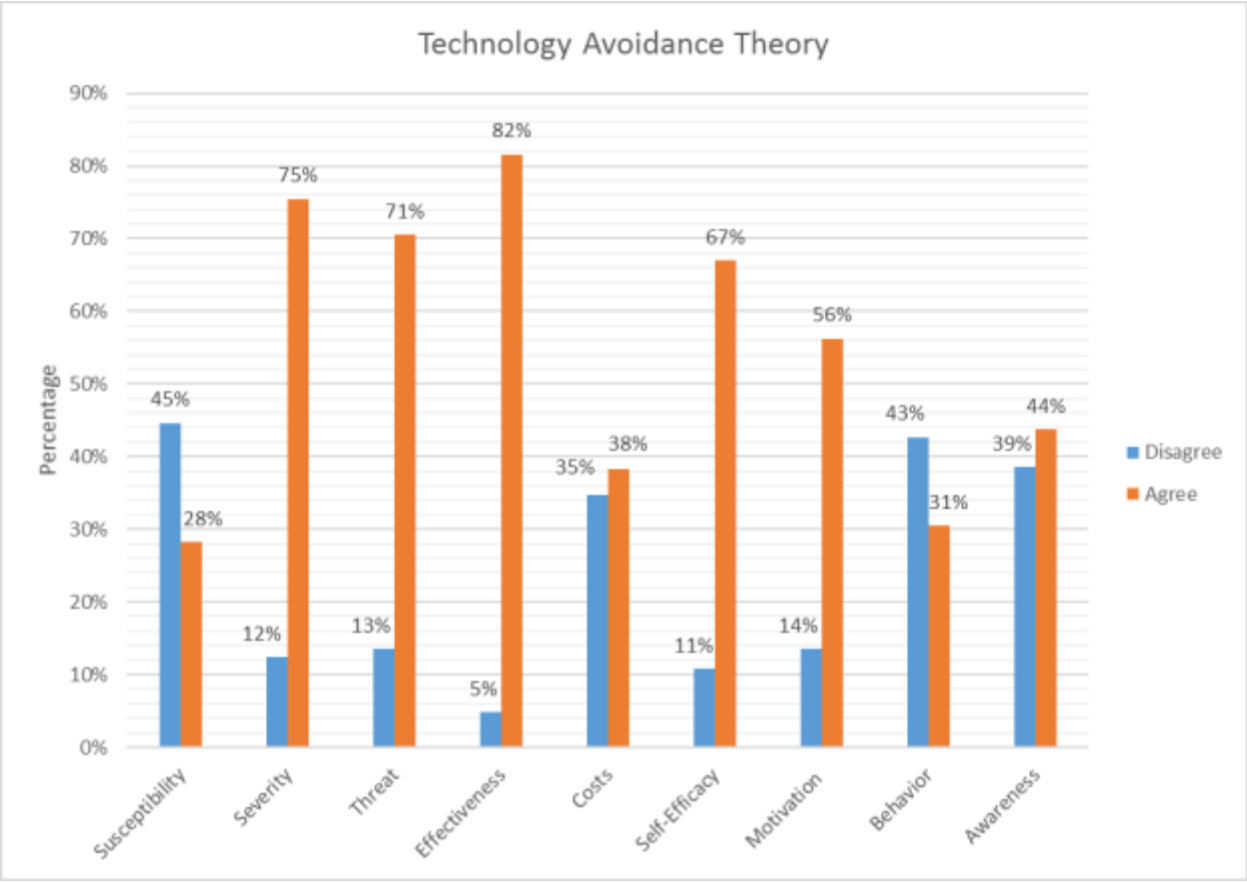


Table 3

Participants' Demographic Characteristics (*N*=335)

Gender	**N**		**%**
Male	84		25%
Female	251		75%
Age			
18 to 19	94		28%
20-29	222		66%
30-39	13		4%
40-49	4		1%
50-59	2		1%
Ethnicity			
American Indian or Alaska	1		0%
Asian	10		3%
Black or African American	39		12%
Hispanic or Latino	127		38%
Native Hawaiian or Pacific	0		0%
White	142		43%
Other	15		4%

Table 4

Participants' Educational Characteristics (N = 335)

Demographics	**N**	**%**
Classification		
Freshman	3	1%
Sophomore	124	37%
Junior	148	44%
Senior	46	14%
Masters	11	3%
Ph.D.	2	1%
Other	1	0%
Educational Level		
Some college	228	67%
Associate Degree	58	17%
Bachelor's Degree	33	13%
Graduate degree or program	1	1%
Other	6	2%
No Response [a]	9	3%
Major		
Clinical Laboratory Science	1	0%
Communication Disorders	28	8%
Health Administration	4	1%
Health information	55	16%
Nursing	12	4%
Physical Therapy	118	35%
Radiation Therapy	0	0%
Respiratory Care	64	19%
Recreational Therapy	19	6%
Biology	8	2%
Psychology	6	2%
Exercise Sports and Science	11	3%
Health and Wellness	8	2%
Other	1	0%

[a] "No Response" for Educational Level indicates this response was left blank on paper surveys.