Mobile Device Security: Perspectives of Future Healthcare Workers

by Barbara Hewitt, PhD; Diane Dolezel, EdD; and Alexander McLeod, PhD

Abstract

Healthcare data breaches on mobile devices continue to increase, yet the healthcare industry has not adopted mobile device security standards. This increase is disturbing because individuals are often accessing patients' protected health information on personal mobile devices, which could lead to a data breach. This deficiency led the researchers to explore the perceptions of future healthcare workers regarding mobile device security. To determine healthcare students' perspectives on mobile device security, the investigators designed and distributed a survey based on the Technology Threat Avoidance Theory. Three hundred thirty-five students participated in the survey. The data were analyzed to determine participants' perceptions about security threats, effectiveness and costs of safeguards, self-efficacy, susceptibility, severity, and their motivation and actions to secure 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 their knowledge of costs and problems related to the adoption of these measures was mixed. These findings indicate that increasing security awareness of 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] Because more than 48 percent of all healthcare data breaches since 2010 involved laptops, desktops, or mobile devices,[4] it is not surprising that 168 of the 1,419 healthcare data breaches affecting more than 500 individuals involved the theft or loss of vulnerable mobile devices.[5, 6]

Despite the increase in healthcare data breaches involving mobile devices, the healthcare industry has not adopted standards for mobile devices, indicating a need for strong mobile device security policies.[7, 8] The National Institute of Standards and Technology recommends increasing end users' awareness of mobile device security measures, such as encrypting sensitive files, reporting loss or theft of the devices, and following procedures to correctly secure mobile devices or ensure that sensitive information cannot be stored on such devices.[9] 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.[10]

In light of the industry's emphasis on securing these devices, the central issue examined in 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.[11] By exploring the perception of security and vulnerability, this study will help to 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, evidence regarding their perceptions of mobile device security is lacking.[12–15] Specifically, very few studies have 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.[16, 17]

According to the annual breach report of the US Department of Health and Human Services, 710 reported breaches have affected 22.5 million individuals from September 2009 to December 2012.[18] This report noted that 54 percent of all breaches occurring between 2011 and 2012 were hacking/information technology (IT) incidents and unauthorized access/disclosure. 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 more than 44 percent of all individuals affected by a data breach. The types of devices used in 2012 were similar to those used in 2011, with desktop computers (12 percent), laptops (27 percent), and other portable electronic devices (9 percent) accounting for the majority of the breaches.[19]

A 2015 report by the Department of Health and Human Services showed that the number of security breaches is increasing.[20] Table 1 lists the top 10 healthcare data breaches that occurred in 2015. In summary, the data in this report and the federal focus on mobile device security issues signal the necessity of adoption of better healthcare security practices to safeguard patients' protected health information.

A study conducted by the Ponemon Institute[21] showed that more than 88 percent of healthcare organizations allow employees and medical staff to use personal mobile devices, including tablets and smartphones. These organizations have control over whether they will adopt security features, such as anti-malware software, spyware protection, and firewalls, on corporate-owned devices. However, these organizations have less control over whether these mobile device users adopt anti-malware software (23 percent), scan the devices before connecting to sources of confidential data (22 percent), or remove vulnerable mobile applications before accessing the system (14 percent).

Given the large number of healthcare-related mobile data breaches and the lack of regulations governing security, the aim of this 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 the examination of these issues. Liang and Xue's Technology Threat Avoidance Theory (TTAT)[22] explores whether individuals create a mental threat perception when they feel a danger is likely to cause undesirable consequences. This perception is important because undesirable consequences may deter practitioners from adopting security safeguards. TTAT also includes the effectiveness of safeguards and self-efficacy because an individual's perception of these variables influences their motivation to avoid security breaches. This theory is also useful in examining how healthcare professionals are employing avoidance mechanisms to ensure that their mobile devices are safeguarded from security breaches. The TTAT model is shown in Figure 1.

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 that were adapted from general security awareness questions used by Bulgurcu et al.[23]

Research Questions

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

1. How do healthcare professionals perceive the 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 healthcare professionals know how to adopt and use effective mechanisms to reduce security threats on personal mobile devices?

Methods

The purpose of this exploratory survey study was to analyze the perceptions of mobile device security from the viewpoint of future healthcare professionals. 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 used 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 of Susceptibility, Severity, Threat, Effectiveness, Costs, Self-Efficacy, Motivation, Behavior, and Awareness were drawn from Liang and Xue[24] and Bulgurcu et al.[25] See Table 2 for a mapping of research questions to variables.

Instrument

Data were collected from a survey adapted by the researchers from two prior studies. The majority of the questions were taken from a survey that was 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. In addition to the constructs in the TTAT model (see Figure 1), this study aimed to explore whether the individuals were aware of intervention mechanisms for mobile device security, such as anti-malware software, passwords or biometrics, encryption, anti-theft apps, and backing up the mobile device. These questions were adapted from the study completed by Bulgurcu et al.[26]

The survey was distributed in paper form to many of the campus-based students and through a SurveyMonkey web link for the remaining campus-based students and the online students. The survey consisted of 47 questions on a seven-point Likert scale (1 = strongly disagree, 7 = strongly agree) and invited respondents to rate their perceptions of the security of their mobile device, their awareness of security issues, and their behaviors toward protecting their mobile devices from security breaches. Typical questions asked participants to rate the chances of a breach on their mobile device or their awareness of mobile device features such as encryption or passwords. Demographic questions asked

about the 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 capable of installing and using security mechanisms that prevent security breaches (self-efficacy), whether 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 Institutional Review Board (IRB) approval and permission from the department chair to distribute the survey to students in the college. Next, individual department heads were contacted to make them aware of the study and get permission to survey their students. Then one or more instructors in the departments that agreed to participate were contacted to obtain permission to distribute surveys to the students in their classes.

Students enrolled in campus-based classes completed either paper surveys or the online version of the survey. All online students were e-mailed a link to the web-based survey. The first page of the survey included a consent form that all students were required to check before completing the survey. All survey responses were collected anonymously. Data were abstracted manually from the paper surveys and exported from the online survey tool. Data were then analyzed to understand whether respondents agreed or disagreed with the items on the survey.

Data Analysis

Descriptive statistical 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 shows composite percentages for the constructs in the TTAT model to summarize the survey responses for technology threat avoidance.

Results

Demographics

Four hundred forty-three students were invited to participate, and 335 students completed the survey, resulting in a response rate of 76 percent. The majority of the participants were female (75 percent). Ages ranged from 18 to 59 years, and 66 percent of the participants were 20 to 29 years of age. Forty-three percent were white, 38 percent were Hispanic or Latino, 12 percent were black or African American, 4 percent were other, 3 percent were Asian, and less than 1 percent were American Indian, Alaska Native, Native Hawaiian, or Pacific Islander. Table 3 shows the participants' demographic data.

The participants' student classifications included freshman (1 percent), sophomore (37 percent), junior (44 percent), senior (14 percent), master's (3 percent), PhD (1 percent), and other (less than 1 percent). Sixty-seven percent had some previous college, and 17 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 4 shows the participants' educational demographics.

Mobile Device Survey Analysis

This analysis presents the mobile device survey results by research question. First, to explore healthcare professionals' perceptions of susceptibility and severity of security threats on personal mobile devices, data on perceptions about 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 that 71 percent of the respondents indicated that their mobile device could be compromised when threatened by a security breach.

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 do not feel susceptible to a breach. Privacy was important to the participants, with 87 percent conveying that a security breach on their mobile device would invade their privacy. Interestingly, 79 percent felt that it was risky to use their mobile device after a security breach because of 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, the perceptions of safeguard effectiveness were examined. Eighty-two percent of the respondents believed that safeguards are effective, but only 36 percent reported knowing how to obtain security safeguards. Most respondents (67 percent) believed that they were capable of installing safeguards and managing safeguard configurations using help tools. Clearly, these respondents deem safeguards effective and are confident in their ability to use these tools.

Third, the study examined whether respondents were aware of threats, were motivated to prevent them, 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 were currently using security safeguards to protect their devices. This finding is concerning because 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 to awareness. When asked if they were aware that they could back up and recover the information on 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 that they could protect their mobile devices from malware, and 27 percent understood that encryption would improve security. Additionally, 33 percent indicated that they were knowledgeable about anti-theft apps for their mobile device.

Discussion

The results of this work provide 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 to 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 for perceived severity, indicating that the respondents 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 finding raises a 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 back up their device and use passwords or other authentication mechanisms, the costs of safeguards, and the availability of safeguards to reduce threats and security breaches. This awareness included knowing that safeguards could determine whether a breach had occurred, could improve the ability to protect against a security breach, and could enhance effectiveness in preventing future breaches. Being aware of these types of products is important in the mobile device environment because hackers and thieves ply their trade in mobile settings. Fewer individuals were aware of safeguards such as anti-malware software, encryption, and anti-theft apps. Thus, increasing future healthcare professionals' awareness of these safeguards is essential to protect health information.

The third research question asked if respondents were adopting security measures for their personal mobile devices. The respondents reported their willingness to adopt security measures in the future, but few reported that they were already engaging in accepted security behaviors. Respondents reported that they knew how to obtain 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, responses were mixed on the necessity of buying security software, and respondents were 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 behaviors of these future healthcare professionals.

Conclusion

Increasingly, healthcare organizations are turning to mobile devices to improve usability of electronic systems, increase ease of use for practitioners, and untether devices from physical locations. In doing so, healthcare system security is directly affected, and thus health information management professionals shoulder responsibility for protecting against security breaches and preventing access by those that would do harm. Our results indicate that students who are future healthcare professionals realize the severity of security threats but do not feel that 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. Although they are not adopting many mobile security safeguards, they are aware of most mechanisms used to support mobile security. These findings indicate that increasing security awareness among healthcare professionals should be a priority as one pathway to increase the rate of adoption of 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, the study was limited to a single method, and we 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 in hospitals, physicians' offices, pharmacies, and other environments. It would also be interesting to survey a variety of healthcare professionals and examine how their perceptions vary from those noted in this work.

The role of future health professionals in securing mobile devices requires substantial consideration because of 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. The results of this survey clearly demonstrate that much needs to be done to increase the security awareness of health professionals.

Barbara Hewitt, PhD, is an assistant professor in the Department of Health Information Management at Texas State University in San Marcos, TX.

Diane Dolezel, EdD, is an assistant professor in the Department of Health Information Management at Texas State University in San Marcos, TX.

Alexander McLeod Jr., PhD, is an assistant professor in the Department of Health Information Management at Texas State University in San Marcos, TX.

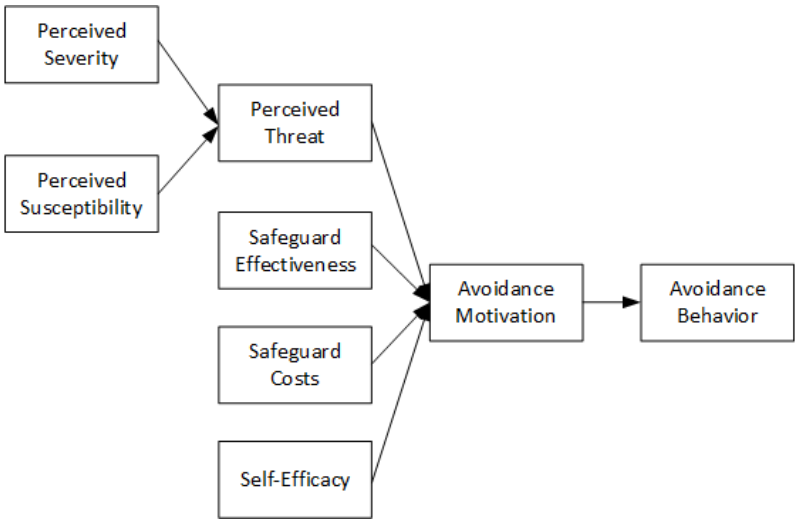
Notes

1. American Health Information Management Association (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): 381–88.
4. Butler, M. "Cracking Encryption: Despite Benefits, Technology Still Not Widely Used to Combat Multi-Million Dollar Breaches."
5. US Department of Health and Human Services. "Breaches Affecting 500 or More Individuals." Available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
6. Oscar, R. "Using Mobile Technology to Improve Health-Plan Utilization and Cut Costs." *Employment Relations Today* 40, no. 2 (2013): 21–27.
7. Thomas, G. "Secure Mobile Device Use in Healthcare Guidance from HIPAA and ISO17799." *Information Systems Management* 24, no. 4 (2007): 333–42.
8. Zeijour, C., and M. Twiggs. "Instituting an Enterprise-wide PHI Disclosure Management Strategy." *Journal of AHIMA* 86, no. 4 (2015): 24–26.
9. Scarfone, K., M. Souppaya, and M. Sexton. *Guide to Storage Encryption Technologies for End User Devices* (National Institute of Standards and Technology [NIST] Special Publication 800-111). Gaithersburg, MD: NIST, 2007.
10. Healthcare Information and Management Systems Society (HIMSS). "Security of Mobile Computing Devices in the Healthcare Environment." 2011. Available at http://www.himss.org/security-mobile-computing-devices-healthcare-environment.
11. Zeijour, C., and M. Twiggs. "Instituting an Enterprise-wide PHI Disclosure Management Strategy."
12. Bowen, R. K. "The Evolving Role of the Privacy and Security Officer." *Journal of AHIMA* 86, no. 6 (2015): 46–47.
13. Crawford, M. "Everyday Ethics." *Journal of AHIMA* 82, no. 4 (2011): 30–33.
14. Flite, C. A., and L. B. Harman. "Code of Ethics: Principles for Ethical Leadership." *Perspectives in Health Information Management* (Winter 2013): 1–11.
15. Zapata, B. C., A. H. Hernández, A. Idri, J. L. Fernández-Alemán, and A. Toval. "Mobile PHRs Compliance with Android and IOS Usability Guidelines." *Journal of Medical Systems* 38 (2014): 81.
16. 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).
17. 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.
18. US Department of Health and Human Services. *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2011 and 2012*. Available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf.
19. Ibid.
20. US Department of Health and Human Services. "Breaches Affecting 500 or More Individuals."
21. Ponemon Institute. *Fourth Annual Benchmark Study on Patient Privacy & Data Security*. 2014. Available at http://www.ponemon.org/library/archives/2014/03.

22. 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.
23. 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): 523–48.
24. Liang, H., and Y. Xue. “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective.”
25. Bulgurcu, B., H. Cavusoglu, and I. Benbasat. “Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness.”
26. Ibid.

Figure 1

Technology Threat Avoidance Model



Note: Adapted from 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. This diagram was generated by the researchers using Visio and was adapted to show only the significant paths identified by Liang and Xue.

Figure 2

Summary of Composite Percentages of Responses Related to Technology Threat Avoidance

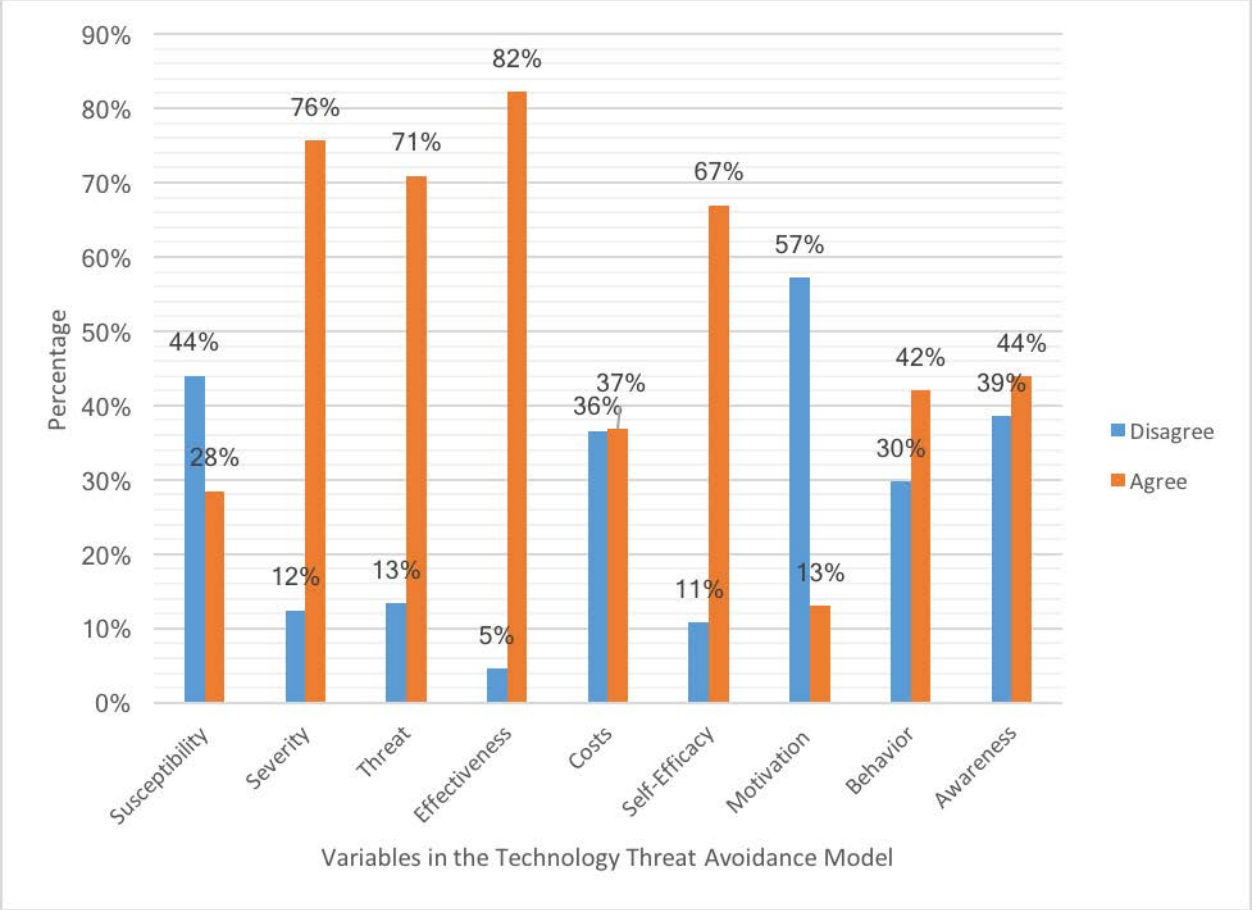


Table 1

Top Ten Healthcare Data Breaches in 2015

Type of Data Breach	**Organization Experiencing Data Breach**	**Number of Records Stolen**
Hacking/information technology incident	Anthem	78,800,000
	Premera Blue Cross	11,000,000
	Excellus Health Plan	10,000,000
	UCLA Health	4,500,000
	Medical Informatics Engineering	3,900,000
	CareFirst BlueCross BlueShield	1,100,000
	Virginia Department of Medical Assistance Services	697,586
	Georgia Department of Community Health	557,779
	Beacon Health System	306,789
Laptop Theft	DJO Global	160,000

Source: US Department of Health and Human Services. "Breaches Affecting 500 or More Individuals." Available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Table 2

Study Variables

Research Question	Variable	Definition
Question 1	Susceptibility	Individuals' perception about whether they are susceptible to security breaches
	Severity	Individuals' perception of how severe the outcome of a breach would be
	Threat	Whether the individuals expected that their device would be compromised
Question 2	Effectiveness	The individuals' perceived effectiveness of a safeguard
	Cost	The cost of implementing a safeguard
	Self-efficacy	Whether individuals believe that they are capable of installing and using security mechanisms that prevent security breaches
Question 3	Motivation	Whether individuals were 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 software, passwords or biometrics, encryption, anti-theft apps, and backing up the mobile device

Table 3

Participants' Demographic Characteristics (*N* = 335)

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

Table 4

Participants' Educational Demographics (*N* = 335)

Characteristic	Number	Percentage
Classification		
Freshman	3	1%
Sophomore	124	37%
Junior	148	44%
Senior	46	14%
Master's	11	3%
PhD	2	1%
Other	1	0%
Educational level		
Some college	228	67%
Associate degree	58	17%
Bachelor's degree	33	10%
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 management	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 program	8	2%
Other	1	0%

[a]"No response" for educational level indicates that this response was left blank on paper surveys.