ISSN: 2473-4901
v11 n6372

Enhancing Healthcare Data Security Through Incentivized Behavioral Cybersecurity

Samuel Tabi
Wiley University
Marshall, Texas, USA
tsbesong@gmail.com

Mary Lind
LSU Shreveport
Mary.lind@lsus.edu
Louisiana State University Shreveport
Shreveport, LA USA

Abstract

Cybercrime has escalated within the healthcare sector, presenting a substantial threat to both operational integrity and patient safety. Notably, 66% of data breaches in healthcare are attributed to providers' failure to identify and address cybersecurity threats. This quantitative correlation study investigated whether factors related to threat avoidance and financial incentives significantly affect healthcare providers' motivation to protect against cyber threats. The study utilized a cross-sectional sample of 107 healthcare practitioners based in the United States. The theoretical framework of the study integrates Carpenter et al.'s refined Technology Threat Avoidance Theory (TTAT) with Jalali et al.'s modified Theory of Planned Behavior (TPB). Employing partial least squares structural equation modeling (PLS-SEM), the study addressed five research questions. The findings indicated that healthcare professionals experienced a heightened sense of control when reliable security technologies were in place. However, variables such as perceived risk, severity, trust in security systems, behavioral control, and financial incentives did not significantly predict motivation for threat avoidance. These results imply that while perceived control is influential, other commonly presumed motivators may not impact cybersecurity behavior as anticipated. Further research should investigate whether factors such as risk propensity, susceptibility, or increased financial incentives can more effectively encourage healthcare providers to adopt robust cybersecurity measures.

Keywords: Cybercrime, healthcare, Technology Threat Avoidance Theory, risk, trust

ISSN: 2473-4901
v11 n6372

Enhancing Healthcare Data Security Through Incentivized Behavioral Cybersecurity

Samuel Tabi and Mary Lind

1. INTRODUCTION

Data security is of paramount importance in the U.S. healthcare sector because of the protected health information (PHI) contained in electronic health records (EHRs) and patient files (Mbonihankuye et al., 2019; Moore & Frye, 2019; Yeng et al., 2021). These data repositories, which house healthcare records, are particularly attractive targets for cybercriminal intent to commit identity theft (Kaddoura et al., 2021). The motivation for cyberattacks on healthcare organizations stems from the fact that healthcare records encompass critical personal information and sensitive data, which hold greater value on the black market than credit card data (Argaw et al., 2020). Breaches in healthcare data pose significant threats to patient safety and disrupt the normal operation of healthcare institutions (Agrawal et al., 2020; Seh et al., 2020). Such breaches compromise the integrity and confidentiality of patient records, thereby eroding patient trust in healthcare providers (Kaddoura et al., 2021; Yaraghi & Gopal, 2018).

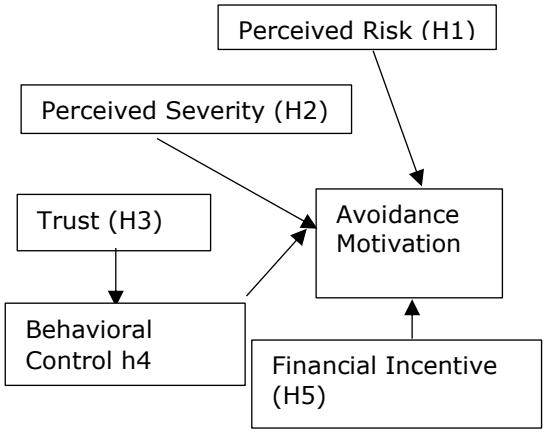
One of the primary causes of data breaches in the healthcare sector is the inability of healthcare providers to detect attacks that target healthcare personnel (Yeng et al., 2021). Information system security professionals within healthcare organizations have employed basic cybersecurity mitigation strategies, such as perimeter fencing, to protect their networks and data (Yeng et al., 2021). Nevertheless, measures such as anti-virus software, intrusion detection and prevention systems, and firewalls have proven ineffective against cyberattacks on healthcare organizations (Yeng et al., 2021). Recent research has indicated that human-related factors, such as inadequate knowledge of healthcare employees or disregard for information security policies, are responsible for the majority of cybersecurity breaches in healthcare organizations (Dong et al., 2021).

Building on the background provided above, this study examines the factors that influence healthcare providers' motivation to protect against cyber threats. The theoretical foundation for this research combines two key frameworks: the Technology Threat Avoidance Theory (TTAT) and an adapted version of the Theory of Planned Behavior (TPB). These theories provide a lens through which to analyze the complex interplay of factors affecting cybersecurity behaviors in healthcare settings. The following section outlines the core components of these theoretical models and their relevance to this study.

2. THEORETICAL BASIS

According to Technology Threat Avoidance Theory (TTAT), when cyber threats are present, users of information systems are inclined to adopt protective measures if they perceive the threat as both probable and potentially severe (Carpenter et al., 2019; Chen & Liang, 2019; Samhan, 2017). If users believe that the threat can be mitigated through specific measures, they are more likely to implement such measures to counteract the threat (Samhan, 2017). In the face of cyber threats, information technology users employ cognitive processes and behaviors to address threats (Chen & Liang, 2019). Users evaluate the severity of the threat and ascertain whether any protective methods are available to counteract it (Chen & Liang, 2019). If a user does not perceive the threat to be sufficiently severe, it may be disregarded (Chen & Liang, 2019). Figure 1 illustrates the TTAT model.

Figure 1 Research Model Based on the TTAT



Trust in Security Technology

The primary element of this study's theoretical framework, as explored in the literature review, is trust in security technology. Trust is an essential aspect of healthcare technology because

of the vast datasets managed by organizations (Moore & Frye, 2019, 2020). The digitization of healthcare information systems, including the adoption of Electronic Health Records (EHR) and the Internet of Medical Things (IoMT) in care delivery, presents potential benefits. However, digitization also renders healthcare organizations vulnerable to cyberattacks (Spanakis et al., 2020). Access to and transmission of patient healthcare data via the Internet are insecure because the Internet, as a public network, lacks comprehensive cybersecurity measures (Lee et al., 2021).

Perceived Behavioral Control

Perceived behavioral control is defined as an individual's evaluation of the ease or difficulty involved in executing a particular behavior (Jalali et al., 2020). It functions as a mediator of the effects of attitudes toward the behavior and the influence of subjective norms associated with the behavior (Bosnjak et al., 2020).

Perceived Risk

Perceived risk is conceptualized as the expected likelihood of a negative event occurring (Jalali et al., 2020). In this study, perceived risk refers to the likelihood that cyberattacks may cause harm in healthcare settings. The existing literature suggests that the risks associated with healthcare data are increasing despite significant investments and efforts by healthcare organizations to improve cybersecurity measures (Rachh, 2021). Consequently, the surge in cybercrimes targeting healthcare institutions has resulted in an increase in healthcare data breaches (Argaw et al., 2020).

Financial Incentives

Stakeholders have significant financial incentives in the realms of cybersecurity and healthcare data management. Cybersecurity breaches involving healthcare data result in substantial financial losses for healthcare organizations (Dong et al., 2021; Meisner, 2018). Researchers have observed a notable increase in cyberattacks targeting hospitals and healthcare organizations, which has exacerbated the considerable financial losses experienced by these entities (Gordon et al., 2019).

Perceived Severity

Perceived severity assesses the magnitude of consequences associated with adverse events (Carpenter et al., 2019). The literature review highlights the substantial impact of cybersecurity breaches. When cybercriminals exploit employees' inadequate cybersecurity practices to commit cybercrimes, the repercussions can be severe for patients (Spanakis et al., 2020). In 2018, data breaches in healthcare organizations negatively impacted over six million patients (Semantha et al., 2020). Furthermore, in 2019, more than 41 million patient records were compromised due to healthcare data breaches (Seh et al., 2020).

3. RESEARCH FINDINGS

This study analyzed survey data collected from 107 healthcare providers in the United States, utilizing partial least squares structural equation modeling (PLS-SEM) techniques to examine the data and address five research questions. The theoretical framework for this study is grounded in the technology threat avoidance theory (TTAT) of Carpenter et al. (2019), augmented by prior research conducted by Samhan (2017) and Jalali et al. (2020) concerning information security risk and trust in technology. The 19 survey questions were derived from three distinct surveys conducted by Carpenter et al. (2019), Jalali et al. (2020), and Samhan (2017). The survey incorporated subscales designed to evaluate perceived information security risk, perceived severity, trust in technology reliability, trust in technology functionality, perceived behavioral control, financial incentives, and threat avoidance motivation. Specifically, the instrument included four subscales previously employed by Jalali et al. (2020), which measured perceived information security risk, trust in security technology reliability, trust in security technology functionality, and perceived behavioral control. Additionally, the instrument featured a subscale adapted from Carpenter et al. (2019) to measure perceived severity and a subscale adapted from both Carpenter et al. and Samhan (2017) to assess avoidance motivation. A single item measuring financial motivation was developed, aligning with the focus of this study. The variables were operationalized using 5-point Likert scales. Among the 107 respondents who completed the online survey, 43 were physicians (40.19%), 33 were physician assistants (30.84%), three were nurses (2.80%), and 28 were nurse practitioners (26.17%). Regarding healthcare-related work experience, 5 participants (4.67%) had 0-1 years, 33 participants (30.84%) had 2-5 years, 32 participants (29.91%) had 6-10 years, 20 participants (18.68%) had 11-15 years, and 17 participants (15.89%) had more than 15 years. All respondents were aged between 25 and 75 years. Specifically, 42 participants (39.25%) were aged 25 to 34, 47 (43.93%) were aged 35 to 44, 11 (10.28%) were aged 45 to 54, 5 (4.67%) were aged 55 to 64, and 2 (1.87%) were aged 65 to 74. The sample was relatively

balanced in terms of sex, with 59 males (55.14%) and 48 females (44.86%). Appendix A contains the survey items used.

The reliability evaluation presented in Table 1 indicates that all constructs demonstrated reliability.

Table 1 Construct Reliability

Construct	Cronbach's α	Composite Reliability
Perceived information security risk	0.925	0.938
Perceived severity	0.941	0.965
Trust in security technology - reliability	0.881	0.926
Trust in security technology - functionality	0.905	0.940
Perceived behavioral control	0.887	0.930
Avoidance motivation	0.880	0.941

Note. All demonstrated high reliability

Variance Inflation Factor (VIF) analysis revealed that the constructs were not multicollinear. Furthermore, by employing the Fornell-Larcker criterion, the constructs exhibited discriminant validity.

The hypotheses were assessed using PLS-SEM, with the findings detailed in Table 2 and Figure 2 in Appendix B. Additionally, Table 3 presents the outcomes of the hypotheses derived from the PLS-SEM analysis.

Table 2 Results of the Path Analysis

Path	β	t	p
PIS -> AM	-0.075	0.331	0.741
PS -> AM	-0.028	0.151	0.880
TTR -> PBC	0.488	3.239	0.001*
TTF -> PBC	0.238	1.603	0.109
PBC -> AM	0.135	1.404	0.160
Fin -> AM	0.102	0.952	0.341

Table 3 Hypothesis Results Summary

H	Variable Relationship	Result
1	Perceived information security risk -> Avoidance motivation	Rejected
2	Perceived severity -> Avoidance motivation	Rejected
3A	Trust in security technology-reliability -> Perceived behavioral control	Supported
3B	Trust in security technology-functionality -> Perceived behavioral control	Rejected
4	Perceived behavioral control -> Avoidance motivation	Rejected
5	Financial incentive -> Avoidance motivation	Rejected

The analysis of the five research questions yielded mixed results regarding the factors influencing healthcare providers' motivation to protect against cyber threats. While perceived behavioral control was significantly predicted by trust in security technology reliability, the data did not support other hypothesized relationships. Specifically, as expected, perceived risk, perceived severity, trust in security technology functionality, and financial incentives did not significantly predict threat avoidance motivation. These findings suggest that the factors influencing cybersecurity behaviors among health care providers may be more complex than initially theorized. The following section explores the implications of these results, discusses potential explanations for the unexpected findings, and proposes directions for future research to examine the drivers of cybersecurity practices in healthcare settings.

4. CONCLUSIONS and IMPLICATIONS

The lack of a significant correlation between perceived risk and healthcare providers' motivation to avoid cyber threats may be attributed to factors such as participants' workload or workplace culture (Seh et al., 2020). Excessive workloads can adversely impact the cognitive capacities of healthcare employees, thereby reducing their ability to implement measures to safeguard healthcare data (Seh et al., 2020). Furthermore, overburdened healthcare employees may become dissatisfied and choose not to adhere to their organizations' security policies (ISSPs; Jalali et al., 2020). Another potential explanation for the absence of

a significant relationship between perceived risk and avoidance motivation is a lack of security awareness. Scholarly literature has linked security awareness to the support of top management (Dong et al., 2021). Consequently, a workplace culture that fails to prioritize cybersecurity may result in employees lacking sufficient understanding of the importance of protecting against cybersecurity threats.

Although perceived severity did not significantly predict healthcare providers' avoidance motivation to protect against cyber threats in the present study, previous research has demonstrated significant findings. For example, Carpenter et al. (2019) identified a statistically significant correlation between employees' perception of the severity of a cyber threat and their avoidance motivation. One possible explanation for the absence of a significant result for Research Question Two is low cybersecurity awareness. Grassegger and Nedbal (2021) emphasized the importance of cybersecurity awareness as a precursor to compliance. If an employee does not perceive a threat as severe, they may disregard it, particularly if compliance is perceived as burdensome or inconvenient. Rostami et al. (2020) observed that Information Security Policies (ISSPs) can create stress and burdens on employees. Consequently, threats may be disregarded as insignificant if they allow employees to avoid onerous cybersecurity measures.

The initial set of hypotheses examined trust as predicated on reliability. The data analysis revealed that trust in technology, grounded in reliability, significantly predicted healthcare providers' perceived behavioral control in safeguarding against cyber threats. Conversely, the association between trust in security technology based on functionality and healthcare providers' perceived behavioral control in mitigating cyber threats was found to be insignificant. Therefore, a healthcare provider's perceived behavioral control in defending against cyber threats is primarily influenced by their trust in security technology's consistent success in providing protection. This finding corroborates with the results reported by Jalali et al. (2020).

Perceived behavioral control pertains to participants' beliefs regarding their ability to influence cybersecurity outcomes through their compliance with Information Systems Security Policies (ISSP). The results pertaining to Research Question Four of this study indicate that perceived behavioral control did not exhibit a significant relationship with healthcare providers' motivation to avoid cyber threats, leading to the retention of the null hypothesis. This outcome does not align with the theoretical framework of this study or previous research findings (Bosnjak et al., 2020; Jalali et al., 2020).

A financial incentive is defined as a monetary bonus offered to healthcare providers with the aim of positively influencing their motivation to avoid cyber threats. However, the statistical analysis did not reveal a significant relationship between financial incentives and the avoidance motivations of healthcare providers. Consequently, financial incentives do not significantly predict healthcare providers' motivation to protect against cyber threats. The literature indicates that the financial costs associated with healthcare data breaches are substantial (Argaw et al., 2020; Dong et al., 2021; Seh et al., 2020). Cyber breaches of healthcare data result in considerable financial losses for healthcare organizations (Dong et al., 2021; Meisner, 2018). These financial costs may include ransoms paid to recover data, fines for HIPAA violations, or revenue losses due to reputational damage (Allen, 2021; Argaw et al., 2020; M. C. Williams et al., 2020). Such financial implications suggest that offering incentives to employees to enhance compliance could be a potentially beneficial strategy.

Future Research

Further research should investigate the differences in risk propensities between healthcare providers and other occupational groups. The healthcare sector is characterized by high levels of stress and demands, making it particularly suitable for individuals with a propensity for risk-taking. Understanding the relationship between risk-taking behavior and cyber threat avoidance could elucidate the factors that influence the decision to implement protective measures for information assets (Carpenter et al., 2019). A comparative research design would enable researchers to assess the risk propensity of various healthcare providers and determine whether specific job roles attract individuals who are more inclined to neglect information security. Furthermore, future research could explore the differences in information security attitudes between the healthcare sector and other industries such as manufacturing, education, retail, and finance. According to TTAT, when a cyber threat is present, the motivation of an information system user to employ a safeguard measure against this threat is contingent upon the user's perception of the threat (Carpenter et al., 2019; Chen & Liang,

2019; Samhan, 2017). The theoretical framework of this study did not significantly predict the motivations and behaviors of healthcare providers regarding cyber threat avoidance. Other factors are likely to influence threat avoidance motivations among healthcare providers. Additionally, workplace overload and insufficient security training may have affected participants' avoidance motivations (Dong et al., 2021; Seh et al., 2020). Employing an alternative theoretical framework that incorporates additional variables such as fear appeals or risk susceptibility would provide further insight into the antecedents of ISSP compliance motivations and behaviors.

Based on this study's findings, financial incentives do not significantly predict a healthcare provider's avoidance motivation to protect against cyber threats. If an incentive for a physician is very small compared to the physician's salary, the incentive will not significantly influence the physician's behavior (Vilendrer et al., 2021). Vilendrer et al. (2021) noted that for an employee to experience enhanced motivation as a result of a financial incentive, the incentive must be substantial, approximately 10% to 20% of the healthcare professional's salary. Additional research should be conducted to determine whether increasing the incentive threshold for healthcare providers would significantly change their threat avoidance motivation.

Yoo et al. (2018) noted that individuals who exhibit psychological ownership of computing devices and the Internet in their homes initiate and display proactive cybersafety behaviors. If an employee of an organization experiences psychological ownership of the organizational resources where they work, they will feel compelled to take measures to safeguard those resources (Verkijika, 2020). Further research should examine health care professionals' psychological ownership of their organizations' health information systems. Healthcare professionals who exhibit psychological ownership of health information systems in their organizations might be more motivated by financial incentives to avoid cyber threats (Verkijika, 2020).

5. REFERENCES

Agrawal, A., Pandey, A., Baz, A., Alhakami, H., Alhakami, W., Kumar, R., & Khan, A. (2020). Evaluating the security impact of healthcare web applications through fuzzy based hybrid approach of multi-criteria decision-making analysis. *IEEE Access, 8*, 135770–135783. https://doi.org/10.1109/ACCESS.2020.3010729

Allen, A. (2021). HIPAA at 25—A work in progress. *The New England Journal of Medicine, 384*(23), 2169–2171. https://doi.org/10.1056/NEJMp2100900

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*, Article 146. https://doi.org/10.1186/s12911-020-01161-7

Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The theory of planned behavior: Selected recent advances and applications. *Europe's Journal of Psychology, 16*(3), 352–356. https://doi.org/10.5964/ejop.v16i3.3107

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*, 380–407. https://doi.org/10.17705/1CAIS.04422

Chen, D., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management, 66*(4), 552–567. https://doi.org/10.1109/TEM.2018.2835461

Dong, K., Ali, F., Dominic, D., & Ali, A. (2021). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability, 13*(5), Article 2800. https://doi.org/10.3390/su13052800

Gordon, J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Network Open,* 2(3), Article e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

ISSN: 2473-4901
v11 n6372

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science, 181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Jalali, M., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research, 22*(1), Article e16775. https://doi.org/10.2196/16775

Kaddoura, S., Haraty, R., Al Kontar, K., & Alfandi, O. (2021). A parallelized database damage assessment approach after cyberattack for healthcare systems. *Future Internet, 13*(4), Article 90. https://doi.org/10.3390/fi13040090

Lee, T.-F., Chang, I.-P., & Kung, T.-S. (2021). Blockchain-based healthcare information preservation using extended chaotic maps for HIPAA privacy/security regulations. *Applied Sciences, 11*(22), Article 10576

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

Mbonihankuye, S., Nkunzimana, A., & Ndagijimana, A. (2019). Healthcare data security technology: HIPAA compliance. *Wireless Communications and Mobile Computing, 2019*, Article 192749

Meisner, M. (2018). Financial consequences of cyber-attacks leading to data breaches in the healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 63–73. https://doi.org/10.12775/CJFA.2017.017

Moore, W., & Frye, S. (2019). Review of HIPAA, part 1: History, protected health information, and privacy and security rules. *Journal of Nuclear Medicine Technology*, *47*(4), 269–272. https://doi.org/10.2967/jnmt.119.227819

Moore, W., & Frye, S. (2020). Review of HIPAA, part 2: Limitations, rights, violations, and role for the imaging technologist. *Journal of Nuclear Medicine Technology, 48*(1), 17–23. https://doi.org/10.2967/jnmt.119.227827

Rachh, A. (2021). A study of future opportunities and challenges in digital healthcare sector: Cyber security vs. crimes in digital healthcare sector. *Asia Pacific Journal of Health Management*, *16*(3), 7–15. https://doi.org/10.24083/apjhm.v16i3.957

Rostami, E., Karlsson, F., & Kolkowska, E. (2020). The hunt for computerized support in information security policy management: A literature review. *Information Management & Computer Security, 28*(2), 215–259. https://doi.org/10.1108/ICS-07-2019-0079

Samhan, B. (2017). Security behaviors of healthcare providers using HIT outside of work: A technology threat avoidance perspective. In *2017 8th International Conference on Information and Communication Systems* (pp. 342–347). IEEE. https://doi.org/10.1109/IACS.2017.7921995

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), Article 133. https://doi.org/10.3390/healthcare8020133

Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A systematic literature review on privacy by design in the healthcare sector. *Electronics, 9*(3), Article 452. http://dx.doi.org/10.3390/electronics9030452

Si, H., Shi, J.-G., Tang, D., Wen, S., Miao, W., & Duan, K. (2019). Application of the theory of planned behavior in environmental science: A comprehensive bibliometric analysis. *International Journal of Environmental Research and Public Health, 16*(15), Article 2788. https://doi.org/10.3390/ijerph16152788

Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., Tanasache, F. D., Palleschi, A., Ciccotelli, C., Sakkalis, V., & Magalini, S. (2020). Cyber-attacks and threats for healthcare: A multi-layer thread analysis. In *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society* (pp. 5705–5708). IEEE. https://doi.org/10.1109/EMBC44109.2020.9

Verkijika, S. (2020). Employees' cybersecurity behaviour in the mobile context: The role of self-efficacy and psychological ownership. In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference* (pp. 1–5). IEEE. https://doi.org/10.1109/IMITEC50163.2020.9334097

Vilendrer, S., Brown-Johnson, C., Kling, S. M. R., Veruttipong, D., Amano, A., Bohman, B., Daines, W. P., Overton, D., Srivastava, R., & Asch, S. M. (2021). Financial incentives for medical assistants: A mixed-methods exploration of bonus structures, motivation, and population health quality measures. *Annals of Family Medicine, 19*(5), 427–436. https://doi.org/10.1370/afm.2719

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research, 22*(9), Article e23692. https://doi.org/10.2196/23692

Yaraghi, N., & Gopal, R. (2018). The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: Insights from an empirical study. *The Milbank Quarterly, 96*(1), 144–166. https://doi.org/10.1111/1468-0009.12314

Yeng, P. K., Szekeres, A., Yang, B., & Snekkenes, E. A. (2021). Mapping the psychosocial, cultural aspects of healthcare professionals' information security practices: Systematic mapping study. *JMIR Human Factors, 8*(2), Article e17604. https://doi.org/10.2196/17604

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107–118. https://doi.org/10.1016/j.dss.2018.02.009

ISSN: 2473-4901
v11 n6372

Appendices and Annexures

Appendix A
Data Collection Instrument

Item	Question	Construct	Scale	Source
1	At my workplace, the risk to my computer and data from Internet security breaches is:	Perceived information security risk	A	Jalali et al. (2020)
2	At my workplace, the likelihood that my computer will be disrupted due to Internet security breaches within the next 12 months is:	Perceived information security risk	A	Jalali et al. (2020)
3	At my workplace, the chance that my computer will fall a victim to an Internet security breach is:	Perceived information security risk	A	Jalali et al. (2020)
4	At my workplace, the vulnerability of my computer and data to Internet security risks is:	Perceived information security risk	A	Jalali et al. (2020)
5	My personal information collected by malware at my place of work could be used to commit crimes against me.	Perceived severity	A	Carpenter et al. (2019)
6	Health records of patients collected by malware at my place of work could be used to commit crimes against patients.	Perceived severity	A	Carpenter et al. (2019)
7	The cybersecurity software at my workplace (e.g., antivirus and firewall) is reliable.	Trust in technology –reliability	B	Jalali et al. (2020)
8	The cybersecurity software at my workplace does not fail me.	Trust in technology –reliability	B	Jalali et al. (2020)
9	The cybersecurity software at my workplace provides accurate service.	Trust in technology –reliability	B	Jalali et al. (2020)
10	The cybersecurity software at my workplace has the functionality I need.	Trust in technology –functionality	B	Jalali et al. (2020)
11	The cybersecurity software at my workplace has the features required for my tasks.	Trust in technology – functionality	B	Jalali et al. (2020)
12	The cybersecurity software at my workplace has the ability to do what I want it to do.	Trust in technology – functionality	B	Jalali et al. (2020)
13	I am able to follow the cybersecurity policies and procedures and technologies (e.g., antivirus, or other products).	Perceived behavior control	B	Jalali et al. (2020)

ISSN: 2473-4901
v11 n6372

14	I have the resources and knowledge to follow the policies and procedures and use the cybersecurity technologies.	Perceived behavior control	B	Jalali et al. (2020)
15	I have adequate training to follow the policies and procedures and use cybersecurity technologies.	Perceived behavior control	B	Jalali et al. (2020)
16	I intend to use anti-spyware software to avoid spyware.	Threat avoidance motivation	B	Carpenter et al. (2019), Samhan, (2017)
17	I predict I would use anti-spyware software to avoid spyware.	Threat avoidance motivation	B	Carpenter et al. (2019), Samhan, (2017)
18	I plan to use anti-spyware software to avoid spyware.	Threat avoidance motivation	B	Carpenter et al. (2019), Samhan, (2017)
19	I would follow the cybersecurity policies and procedures and technologies (e.g., antivirus, or other products) more if there were a financial incentive of about 10% to 20% of my salary.	Financial motivation	B	Developed based on this study's focus

ISSN: 2473-4901
v11 n6372

Appendix B PLS-SEM Model