IT Managers’ and IT Professionals’ Mobile Device Security Strategies

Tanyetta White
University of Phoenix

Teresa Lao
Walden University

The growing use of mobile devices in the workplace for communicating, transferring, and sharing information, presents increasing security risks as technology evolves. The qualitative exploratory case study presented the insights and perspectives of 15 IT managers’ and IT professionals’ mobile device security strategies through interviews. Some of the themes that emerged from the study include the following: security awareness and training programs help improve visibility and user education; secure networks, updates, authentication, and encryption improve mobile device security; and trusted device recognition is critical in mobile device security. The results highlighted the need to increase awareness and education of mobile device security strategies in the workplace to ensure that transmission of information is not breached.

Keywords: mobile security, mobile device security, mobile technologies, security awareness, mobile device management

INTRODUCTION

IT managers and IT leaders are faced with security concerns as they navigate the use of various technologies in professional environments. With the advancement of technologies in mobile devices and increasing demands for usability and communication around the world, the transfer of information can be compromised if organizations do not have the proper measures to protect the medium of communication. Patten and Harris (2013) affirmed that mobile device security is a critical concern around the world as organizations struggle to stay abreast of advancing technologies. Mobile device security consists of various security measures such as applications, policies, standards, and procedures to safeguard against attacks. Organizations use various technologies to conduct their operations. The most common technologies that are used include smartphones, tablets, and other mobile technologies; these are highly preferred over the traditional desktop computers and laptops for personal and business purposes (Chin et al., 2016; Clarke et al., 2016; Friedman & Hoffman, 2008; Olafare et al., 2015; Wibowo & Ali, 2016). The growing interest in mobile devices for communication, transfer, and collaboration could make IT managers and IT leaders wary of adopting new technology procedures due to emerging security concerns (Beyer, 2014; Sujithra & Padmavathi, 2012).

Wibowo and Ali (2016) found that a growing number of hackers and identity thieves are attacking individuals’ security and personal information because individuals are using devices without putting much attention on personal security and protection. Employees are caught unaware of these attacks because they lack the education, training, and awareness to identify and respond to potential threats facing their mobile devices, which justifies the need for IT leaders and IT managers to improve the knowledge transfer of mitigation strategies throughout the organization to secure mobile devices. Several organizations allow employees to use personal devices in the workplace, raising concerns with maintaining confidentiality and privacy of corporate data. The deepening of employees' knowledge and awareness helps prepare organizations with the mindset to execute decisions to prevent attacks on mobile devices (Patten & Harris, 2013).

Because of the issues concerning IT security and cyberattacks in the workplaces today, this study was initiated to deepen our understanding of security strategies used by IT managers and IT professionals in the workplace. The findings of this study are significant because organizations could provide strategic measures to employees, managers, leaders, and researchers so they could become more aware of the seriousness of the IT threat in the workplace. Also, leaders could evaluate their technological preparedness when it comes to technological trends so they could develop readiness measures to ensure mobile devices and computer devices are secure while improving productivity and performance.

Griffin (2017) conducted a qualitative single case study to investigate preventive strategies to minimize and eliminate data breaches in government contractor organizations in the Southeastern region of the United States. Griffin (2017) recommended conducting similar studies using other industries in different regions of the United States or research to identify similarities in security strategies in multiple organizations. The purpose of this exploratory case study was to explore the strategies used by four IT managers and 11 IT professionals to secure mobile devices. The remainder of this research presents the problem with supporting literature, research questions, significance of the problem, research methodology, discussion of results, and conclusions.

BACKGROUND

Organizations today are not fully equipped to handle cybersecurity attacks encountered in the workplace. There are inadequate measures in place that lead to confidential information being compromised and shared with the wrong people. CCSI (2020), for example, indicated that the number one reason that organizations are not prepared to handle cyberattacks is the failure to secure fundamental security measures. Organizational leadership may think that simply downloading anti-virus software is enough to thwart attacks from hackers and identify thieves (CCSI, 2020). This can be a costly assumption that could lead to clients' data being compromised by unscrupulous attackers.

According to the National Conference of State Legislatures (2019), security and privacy are growing concerns as technologies advance to allow more accessibility of personal and corporate information prone to manipulation. The accelerating popularity of mobile devices increases the opportunities for threats on financial, sensitive, and corporate information (Clarke et al., 2016; Gajar et al., 2013; Khan et al., 2015; Sujithra & Padmavathi, 2012). Additionally, researchers contend that security is a vital challenge among IT departments as mobile devices become the most sought-after business tool (Downer & Bhattacharya, 2015; Sujithra & Padmavathi, 2012). Security leaders and managers will benefit from this study by acquiring a deeper understanding of mobile device security strategies shared by other managers and professionals within various organizations. IT leaders and IT managers are concerned with protecting mobile devices in the workplace for productivity and communication (Sujithra & Padmavathi, 2012). Due to the gaps in safeguarding data and the privacy of users' mobile devices, the study revealed IT managers' and IT professionals' recommended strategies.

PROBLEM

Despite the increasing use of mobile devices among organizations, little attention is given to investigate how leaders, managers, employees, and users protect their mobile devices in daily business operations and communication from the rapidly emerging security threats and vulnerabilities (Beyer, 2014; Clarke et al., 2016; Donald et al., 2013; Sharmeen et al., 2018).

To address the problem and purpose of this study, one research question and two sub research questions were developed. The following research questions guided the study:

- **Main research question:** What strategies and processes do IT managers and IT professionals use to protect data and the security of mobile devices?
- **Sub research question 1:** What physical processes are used to secure and protect sensitive data on mobile devices?
- **Sub research question 2:** What software and encryption technologies are used to secure and protect sensitive data on mobile devices?

Research Methodology and Design

The qualitative research study was conducted using semi structured interviews with 11 open-ended questions distributed to participants, which allowed for the content analysis of the responses. Hancock and Algozzine (2006) explained that in the exploratory case study design, the researcher seeks to identify themes or categories. The case study design was used to explore the IT managers' and IT professionals' interview responses to the point of data saturation in data collection and analysis; the results did not render new themes, ideas, concepts, or patterns; fulfilling the trustworthiness and dependability of the data (Elo et al., 2014; Hammarberg et al., 2016; Onwuegbuzie & Collins, 2007). The sequential steps that guided the study are described in the next section.

The 11 semi-structured, open-ended interview questions were field-tested and approved by the Institutional Review Board (IRB) before interviewing participants. Following IRB approval, each participant signed an informed consent form to partake in the interview session. The selection of 15 participants included four IT managers and 11 IT professionals from various organizations throughout the Southeastern region of the United States. These participants needed to have a minimum of two years of mobile device security experience, to the point of data saturation. The time frame allotted for each interview session was approximately one hour.

One-on-one interviews were conducted with each participant in person, via telephone, or through web conference tools such as Zoom, WebEx, or Skype. These interviews were conducted within the target population until the point of data saturation was achieved, which established credible analysis and reporting (Marshall et al., 2013). There was no agreed number of interviews or observations required to be conducted in qualitative research (Lee, 2014; Marshall et al., 2013).

Each interview session was audio-recorded and verbatim transcriptions were sent to participants for credibility and accuracy of responses. Transcription reviews allowed the participants the opportunity to review the researcher's interpretations of the responses and modify responses if necessary. Following the transcription reviews, transcripts were uploaded into NVivo™12 software for coding, categorization, and content analysis. Credibility was established through triangulation, transcription reviews, proper handling of researcher bias, and scrutinizing discrepancies in the data (Creswell, 2003). The next section presents the results of the research.

Results

The results of this study emerged from participants' interview responses. This section presents the five primary themes that emerged during the thematic data analysis of the interviews. Data triangulation was used to analyze the interview responses gathered from the semi structured interview sessions with each participant in conjunction with the literature review. Table 1 includes five themes that emerged from the data analysis to answer the research questions.

TABLE 1
FIVE MAJOR THEMES FROM THEMATIC CONTENT ANALYSIS

Themes
1. Security awareness and training programs help improve visibility and user education.
2. Secure network, updates, authentication, and encryption improve mobile device security.
3. Trusted device recognition is critical in mobile device security.
4. Communication of policies and procedures is necessary to keep individuals knowledgeable and protected.
5. Mobile device management tools help support mobile device security.

The findings reinforced the point that attention and a deeper understanding of individuals' encounters with security threats and mitigation strategies are necessary for improving knowledge and user education of mobile device security. Although some organizations have mobile security strategies, greater emphasis is needed for knowledge transfer to increase awareness of human behavior and reduce absence of actions. According to Chin et al. (2016), information security research largely ignores the role of human operators, which greater emphasizes that mobile security is a new struggle faced by individuals because of expectations to establish and maintain adherence to proper security protocols and strategies.

IT managers and IT professionals who participated in this study emphasized the ever-increasing concern of securing mobile devices with industry progression towards mobility for efficiency and effectiveness of overall productivity and performance. However, the study findings exemplified that some organizations lack awareness on how mobile device security affects the data, the networks, the systems, and the employees. In support of this interpretation, a participant of the study noted:

> From a mobile device security perspective, you can’t secure it if you don’t know about it. Then once we know they exist, the advantage of knowing is the ability at that point to assess risk. It all comes down to the assessment and the mitigation of risks.

For example, one participant further stated:

> Mobile device security is a significant element of where we're going in general. There's a very mobility-focused culture that's evolving and being able to secure mobile devices is a significant strategy as we're trying to drive forward this whole notion of zero trust or trusted access where all of the controls are being pushed to the user devices and then at the applications. We are more focused than ever on mobility security.

All organizations risk the potential for corporate and personal data compromise when they are unaware of the severity of the threats, how to detect them, let alone combat against them. This section addresses the comparisons and contrasts between the five themes identified during data analysis and existing literature.

Security Awareness and Training Programs Help Improve Visibility and User Education

The participants exhibited extensive knowledge of mobile device security, network infrastructure security, information security, and data security. Considering that people and human errors are the largest threats to mobile devices, mobile device security is a primary concern among the security research community (Bitton et al., 2018). The widespread vulnerabilities and attacks yield human errors, intentional and unintentional lack of awareness of security measures (Alsaleh et al., 2017; Bitton et al., 2018). Liang et al. (2019) shared the lack of awareness, neglect for preparation, disregard of security efforts, and user consciousness contribute to the growing vulnerabilities and attacks. Users attested that their worries are due to the lack of clearly formulated and communicated security awareness practices for managing mobile data (Tairov, 2019). Individuals including but not limited to users, enterprises, manufacturers, managers, and developers must become more cognizant of detecting risks and ways to mitigate those risks (Orman, 2013).

Mobile users' carelessness, lack of education, and awareness have contributed to the increase of security threats faced and encountered (Bitton et al., 2018; Harris et al., 2013; Liang et al., 2019; Markelj & Bernik, 2013; Shonola & Joy, 2015). Chen and Li (2017) affirmed that individuals and IT users are highly susceptible to target from threats due to the lack of systemic security training to detect, prevent, or cope with privacy threats. The researchers explicated that maintaining awareness of security practices allows employees, managers, and organizations to stay ahead of intended harm (Kleiner & Disterer, 2015; Wibowo & Ali, 2016). Therefore, researchers recommended that organizations seek ways to enhance and ensure mobile device security awareness and training initiatives (Harris et al., 2013; Kleiner & Disterer, 2015; Saleem & Hammoudeh, 2017).

Many individuals do not consider the privacy of mobile devices by storing passwords and codes in their email accounts, which increases the vulnerabilities to breach, compromise, corruption, and theft of data (Curran et al., 2015). By improving user education through training and security awareness programs, organizations could empower employees to employ prevention methods and reduce the risk of attacks. Training and security awareness will increase visibility and reduce the costs of addressing attacks after the occurrence. Organizations and individuals prevent attacks on mobile devices by employing mobile security awareness (Bitton et al., 2018). Malware prevention practices are gaining attention with the increased interest and support for mobile devices for conveniently and expeditiously exchanging data (Wibowo & Ali, 2016).

The participants stated that expanding individuals' awareness and knowledge of mobile device security through frequency will help organizations to improve the actions to address security risks and threats. Participants shared some of their experiences and their general knowledge of encounters with malware attacks, security threats, and securing mobile devices accordingly. The convergence of the conceptual framework included the social engineering defensive framework (SEDF), ensuring security training and awareness of the technology and security policies was a leading factor for enhancing the mobile device security issues that organizations are faced with as technology exponentially advances.

According to Ludwig von Bertalanffy (1968), general systems theory focuses on mobile device security in entirety instead of a component used to support managers and leaders in the decision making of information technology adoption. Security awareness and training is not an independent strategy to enforce device security but a component of the whole mobile device strategy. Wibowo and Ali (2016) attested that one individual or deficiency can cause the entire network to succumb to infections or data leakages. Systems theory increases individuals' understandings of the security strategies that managers used to protect mobile devices in the work environment.

Secure Network, Updates, Authentication, and Encryption Improve Mobile Device Security

Lima et al. (2017) asserted that authentication and encryption standards help managers and employees to enforce locks to increase the level of security with passwords and PINs before performing operations on mobile devices. Theme two is pertinent to theme one in that individuals must possess the knowledge and education to detect threats and secure mobile devices, which also contributes to acquiring knowledge of encryption and authentication protocols. The encryption to protect corporate data as a prevention strategy when mobile devices are lost or stolen, led in a mandate by some organizations (Millman, 2017). Many participants echoed that individuals cannot even begin to protect data and mobile devices unless visibility exists. Some participants emphasized the need for employees and managers to apply zero trust, not completely trusting the security of any mobile devices. One participant stated:

> In the mobile device space, it all begins with visibility. So from a mobile device security perspective, it's all about you can't secure it if you don't know about it.
>
> You can't even understand it as much as mitigate it if you don't know what it is.
>
> So our mobile security begins with visibility. Then, you know, the biggest advantage we would have there is the ability to understand risk.

Curran et al. (2015) indicated data is never 100% secure. The study participants determined that ensuring data is protected with regular updates and supporting the mobile devices is key to stopping the potential growth of security threats. Wibowo and Ali (2016) further emphasized that a significant precaution for individuals is to keep up to date with any information regarding mobile malware and regular security updates. Security concerns remain present among organizations regarding data protection in today's global technology (Curran et al., 2015). Kleiner and Disterer (2015) posited that continuous updates of applications, operating systems, and anti-virus software are necessary to secure data and mobile devices. The best that users can do is stay up to date and regularly check for software updates to ensure the security of the mobile devices (Wibowo & Ali, 2016) and maintain regular updates of applications, operating systems, and firmware (Kleiner & Disterer, 2015).

While vigilantly staying abreast of security practices does not eliminate the security threats, it helps to minimize and control the consequences of those threats on corporate data and mobile devices. In tandem with employees and users working to ensure that software updates occur, attentiveness is necessary to ensure that the downloaded and installed applications originate from trusted sources (Wibowo & Ali, 2016). If individuals neglect the software updates, the potential for vulnerabilities and attacks increases.

Data protection is pertinent to organizations because it relates to the entire network, which connects to mobile devices. Therefore, organizations need to carefully assess security policies and infrastructure to ensure that data protection with various components including, but not limited to the secure networks, regular updates, passwords, PINs, encryption, and multi-factor authentication. Lima et al. (2017) indicated that authentication and encryption schemes provide management with the opportunity to lock the system using passwords and PINs before acting.

Lima et al. (2017) affirmed that the increased risk of lost or stolen mobile devices subject hackers to avenues to implode attacks and intrusions to data, causing security assurance challenges. Wibowo and Ali (2016) affirmed that choosing to fully encrypt mobile devices strengthens the security and minimizes the risks of intrusion and compromise of data. Individuals also must create strong and complex passwords to increase the security of mobile devices (Wibowo & Ali, 2016). Five participants expressed that organizations must protect their data by ensuring visibility and communication. Additionally, the participants expressed satisfaction with their current strategies to protect the data with a primary emphasis on training their people.

Five participants shared similarities in their opinions about data protection, specifically regarding standardization for securing lost, stolen, or misplaced devices. One participant indicated that the organization currently does not have a standard strategy to manage the security of temporarily lost devices, later recovered. However, another participant expressed that data protection varies with the organization's level of security. Mobile device security strategies to ensure data protection such as phishing programs, testing, regular updates, and selection of supported corporate-liable devices were suggestions used in some organizations, but mobile device security remains a work in progress with the faster advancement of technology.

Trusted Device Recognition Is Critical in Mobile Device Security

According to Lima et al. (2017), trusted device management relies on the verification of trusted certificates, keys, and signatures to manage the interaction of systems and applications to install. Millman (2017) highlighted the importance of trust in the mobile device community and organizations need to ensure that the devices used to comply with the defined security standards and policies. Theme three corresponds with securing mobile devices through networks to ensure updates, password authentication, and encryption strategies expressed in theme two. Additionally, theme three also relates to theme one, as providing employees with security awareness and training programs to improve overall visibility and tactics to register trusted devices on the organization's secure network. Four participants discussed the importance of device registration and achieving the root of trust, having a point of control encompassing minimum requirements that mobile devices must contain to be considered "trusted."

The root of trust and zero trust in the security of mobile devices were emphasized by four of the 15 participants. The registration of mobile devices on the organization's network helps to control unwanted entry. Organizations may manage the security of trusted devices by providing mobile devices to employees rather than allowing them to use personal devices (Wibowo & Ali, 2016). One key benefit of the organization providing the devices to employees is complete control of the apps, interactions, and uses allowed (Wibowo & Ali, 2016). Having awareness of protocols allows individuals to circumvent the potential for data leakage and compromise on the mobile device through the organization's network.

The significance of recognizing mobile devices as a trusted device can be supported by risk management. In support of risk management, Wibowo and Ali (2016) indicated the common approach adopted by many organizations is the implementation of bans or blacklisting devices and applications from download or access on the network. Some mobile devices are more susceptible to negative impacts from malware attacks, which intensifies the need to ban vulnerable devices to minimize the exposure to risks of data corruption or data theft (Wibowo & Ali, 2016). Risk management increases as the organizations advance the trusted device recognition practices with the assessment of harmful applications.

Communication of Policies and Procedures Is Necessary

According to Sahd and Rudman (2016), organizations encounter consequences from the lacked governance of policies and procedures for securing mobile devices, posing a lack of understanding of the implemented technologies and the speed of technology advancements. The policies and procedures which direct employees' behaviors and conduct to meet the organization's objectives make up the corporate governance (Sahd & Rudman, 2016). Evolving mobile security policies and procedures aid organizations in keeping pace with the changes and risks. Sahd and Rudman (2016) recommended that managers and leaders consider the effects that mobile device advancements may pose for meeting the objectives of the policies and procedures. Theme four is related to theme one concerning security awareness and training programs as a means of communicating security knowledge to employees and users. Sahd and Rudman (2016) stated that the successful deployment of mobile device security policies and procedures should include training, including training the application developers in platform-specific coding and IT staff receiving regular refresher training on new software and security risks.

Several participants emphasized the importance of employing individuals who are knowledgeable and skilled to support the security of data and mobile devices in organizations. Employees must be familiar with the organization's mobile device security strategies and the appropriate procedures to execute when threats are detected or encountered. Five participants expressed the importance of security policies and procedures being communicated and kept current to support safeguarding data and mobile devices. The depth of the organization's policies varies based on the level of security and the devices supported by the organizations. Mobile devices that do not comply with the security policies outlined by the organization should be restricted from accessing corporate data or networks (Wibowo & Ali, 2016). Two of the participants indicated that the lack of training and employee resistance to comply with these security measures impacts security policies and procedures.

Mobile Device Management Tools Help Support Mobile Device Security

Kleiner and Disterer (2015) and Tairov (2019) indicated that mobile device management (MDM) is the application of technological measures, software, services, processes, and policies required to help employees and managers successfully establish centralized control of the mobile devices and data access. Millman (2017) reinforced that MDM tools allow users the opportunity to enroll their mobile devices and identify devices as trusted and access to the network and applications. To ensure registered network access of the devices and the applications, Disterer and Kleiner (2013) indicated that organizations should be using MDM tools. MDM tools also aid in the configuration of mobile devices and the deployment of applications, including upgrades (Sahd & Rudman, 2016; Tairov, 2019). Tairov (2019) posited that MDM enables industries to permit employees to use mobile devices that are approved by the organization to support day-to-day business communication and activities.

Theme five relates to theme four. MDM tools may be used as solutions to enforce mobile device security policies, software updates, backing up and installing applications (Sahd & Rudman, 2016). Wibowo and Ali (2016) suggested that organizations should enforce mobile device security policies by using MDM tools. While MDM tools are useful solutions to protecting mobile devices in the organization, limitations may exist on the enforcement capabilities of some operating systems. Theme five aligns with theme two, in which the software updates include ensuring that the MDM tools used are continuously updated. One participant referred to MDM as an asset management tool rather than a security management tool. However, 10 out of 15 participants recommended MDM tools to assist in securing mobile devices. The decision to employ MDM tools to aid in mobile device security also depends on the security level and the organization's financial position.

Limitations

The limitations of this study included: 1) time allotted for each interview; 2) truthfulness of interviews; 3) use of the exploratory case study; 4) sample population; and 5) scope of the case. The first limitation was the time allotted to complete the interview session with each participant. The time frame designated for each participant interview was approximately 60 minutes. However, due to the varying knowledge and experience, some interviews lasted 25 to 45 minutes, while other interviews exceeded 60 minutes. Other participants had distractions during the interview session, which shortened the time frame. Rescheduling of some interviews occurred due to unforeseen circumstances or oversight. The study settings and the interview times were selected and scheduled per each participant's request.

A second limitation was researcher bias, minimized by maintaining a reflexive journal and field notes of personal opinions, beliefs, and values experienced during data collection and analysis to establish meaning and interpretations. Transcription reviews also helped the researcher to ensure the credibility of the research.

The purposeful selection of the participants in the study occurred from the eligibility criteria defined by the researcher. Purposive sampling is the deliberate selection of participants of a population to satisfy the research purpose and obtain rich descriptions to deepen the readers’ understandings of the mobile device security phenomenon (Gentles et al., 2015). The researcher solely solicited participation from individuals who were IT managers and IT professionals with a minimum of two years of knowledge and experience in mobile device security.

Recommendation

Organizations can control and monitor the ongoing activities of employees. With proper measures in place that focus on the prevention of current and future cyber threats, organizations could continue to transmit information with various stakeholders without the fear of having their data compromised. The following recommendations could extend the body of research concerning mobile devices and other technology used in the workplace. Researchers who are interested in pursuing studies about mobile and other technology devices could focus their attention on the recommendations listed below.

The first recommendation is for scholars to extend the exploration to the mobile device security framework in different organizations and see how to accomplish security awareness training. A second recommendation is to conduct a multiple case study to determine how IT managers' and IT professionals' mobile device security strategies in the Southeast region of the United States compare with others. Third, researchers could conduct a quantitative study to compare strategies, processes, and programs in the industries between other United States regions. Lastly, quantitative research might include using the findings of this study to test a hypothesis about the effectiveness of security awareness training programs.

CONCLUSION

This study fulfilled the gap in the existing literature by providing strategies for improving security in the workplace. Also, organizational leaders can gain insight from the responses of IT managers and IT professionals on the need to be more educated in terms of mobile device security usage and protection. The responses from the IT managers and professionals indicated that the rapid demand and use of mobile devices in the workplace necessitates more awareness to organizations about the urgency to be more prepared to face the challenges that cybersecurity brings.

Organizations are struggling to stay abreast with mobile device security as threats are surfacing at a faster rate and not easily detectable. Hackers and identity thieves are very adept at what they do. We cannot underestimate the expertise of these criminals in wreaking havoc when it comes to personal information and data breach. Thus, organizational leaders must be one or two steps ahead in ensuring appropriate safety measures are in place to protect any breach in data.

Participants' responses implied that employees might resist compliance of policies on unsupportable devices on the networks because of individuals' suspicions about company-mandated software or MDM installation and refusal to complete training awareness programs. Participants explicated that all attacks are not preventable; however, safety measures can help prepare for such attacks. Employees need to remain connected to various channels and regularly communicate any concerns to the organization could reduce these cyber threats.

Although organizations in the study presented strategies that proved to be effective, there is still room for improvement and increased protection from the advanced vulnerabilities that continue to emerge as technologies develop. Based on the emerging themes from data analysis, IT managers and IT professionals should ensure that they train their people on the security risks, policies that protect mobile devices, and measures to combat the threats and breaches encountered. Human error from intentional and unintentional negligence, lack of knowledge, training, and awareness, including neglect in mobile device security, are the major catalysts for the increased emphasis on expanding security awareness training programs in organizations.

REFERENCES

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*, *12*(3), 1–35. doi:10.1371/journal.pone.0173284

Beyer, C. (2014). Mobile security: A literature review. *International Journal of Computer Applications*, *97*(8), 9–11. doi:10.5120/17025-7315

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. *Computers & Security*, *73*, 266–293. doi:10.1016/j.cose.2017.10.015

CCSI. (2020). *10 common IT security risks in the workplace*. Retrieved from https://www.ccsinet.com/blog/common-security-risks-workplace/

Chen, H., & Li, W. (2017). Mobile device users’ privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security*, *25*(3), 330–344. doi:10.1108/ICS-04-2016-0027

Chin, A.G., Etudo, U., & Harris, M.A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235–252. doi:10.15388/infedu.2016.12

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016). Awareness of mobile device security: A survey of user's attitudes. *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, *7*(1), 15–31. doi:10.4018/IJMCMC.2016010102

Creswell, J.W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage

Curran, K., Maynes, V., & Harkin, D. (2015). Mobile device security. *International Journal of Information and Computer Security*, *7*(1), 1–13. doi:10.1504/IJICS.2015.069205

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology*, *9*, 43–53. doi:10.1016/j.protcy.2013.12.005

Donald, A.C., Oli, S.A., & Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. *International Journal of Engineering and Innovative Technology (IJEIT)*, *3*(1), 30–35. Retrieved from semanticscholar.org

Downer, K., & Bhattacharya, M. (2015). BYOD security: A new business challenge*. IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, pp. 1128–1133. doi:10.1109/SmartCity.2015.221

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, pp. 1–10. doi:10.1177/2158244014522633

Friedman, J., & Hoffman, D.V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, *7*(1/2), 159–180. Retrieved from https://ebscohost.com

Gajar, P.K., Ghosh, A., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating. *Journal of Global Research in Computer Science*, *4*, 62–70. Retrieved from rroij.com

Gentles, S.J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, *20*(11), 1772–1789. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss11/5

Griffin, T. (2017). *Strategies to prevent security breaches caused by mobile devices (Order No. 10688514)*. Available from ProQuest Dissertations & Theses Global. (2014068551). Retrieved from https://proquest-com

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction (Oxford, England)*, *31*, 498–501. doi:10.1093/humrep/dev334

Hancock, D.R., & Algozzine, R. (2006). *Doing case study research: A practical guide for beginning researchers*. New York: Teachers College Press.

Harris, M.A., Patten, K., & Regan, E. (2013). The need for BYOD mobile device security awareness and training. *Proceedings of Nineteenth Americas Conference on Information Systems (AMCIS)*, *5*, 3441–3451. Retrieved from https://www.semanticscholar.org

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science*, *56*, 376–383. doi:10.1016/j.procs.2015.07.223

Kleiner, C., & Disterer, G. (2015). Ensuring mobile device security and compliance at the workplace. *Procedia Computer* Science, *64*, 274–281. doi:10.1016/j.procs.2015.08.490

Lee, Y.A. (2014). Insight for writing a qualitative research paper. *Family & Consumer Sciences Research Journal*, *43*(1), 94–97. SocINDEX with Full Text, EBSCOhost. Retrieved November 30, 2016.

Liang, H., Fleming, C., & Man, K.L. (2019). Personal mobile devices at work: Factors affecting the adoption of security mechanisms. *Multimedia Tools and Applications*, pp. 1–14. doi:10.1007/s11042-019-7349-2

Lima, A., Sousa, B., Cruz, T., & Simões, P. (2017). Security for mobile device assets: A survey. *Proceedings of the International Conference on Cyber Warfare & Security*, pp. 227–236. Retrieved from https://www.ebscohost.com

Markelj, B., & Bernik, I. (2013). Mobile devices and effective information security. *Innovative Issues and Approaches in Social Sciences*, *6*(2), 40–52. doi:10.12959/issn.1855-0541.IIASS-2013-no2-art03

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in is research. *The Journal of Computer Information Systems*, *54*, 11–22. doi:10.1080/08874417.2013.11645667

Millman, R. (2017). Maximise productivity and minimise risk with mobile management. *Computer Weekly*, *25*. Retrieved from https://www.proquest.com

National Conference of State Legislatures. (2019). Retrieved from www.ncsl.org

Olafare, O., Parhizkar, H., & Vem, S. (2015). A new secure mobile cloud architecture. *International Journal of Computer Science Issues (IJCSI)*, *12*(2), 161–175. Retrieved from https://arxiv.org

Onwuegbuzie, A.J., & Collins, K.M. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report*, *12*(2), 281–316. Retrieved from https://nsuworks.nova.edu/tqr/vol12/iss2/9

Orman, H. (2013). Did you want privacy with that?: Personal data protection in mobile devices. *IEEE Internet Computing*, *17*(3), 83–86. doi:10.1109/MIC.2013.48

Patten, K.P., & Harris, M.A. (2013). The need to address mobile device security in the higher education IT curriculum. *Journal of Information Systems Education*, *24*(1), 41–52. Retrieved from www.jise.org

Sahd, L.M., & Rudman, R. (2016). Mobile technology risk management. *Journal of Applied Business Research*, *32*(4), 1079–1096. doi:10.19030/jabr.v32i4.9723

Saleem, J., & Hammoudeh, M. (2017). Defense methods against social engineering attacks. *Computer and Network Security Essentials*, pp. 603–618. doi:10.1007/978-3-319-58424-9_35

Sharmeen, S., Huda, S., Abawajy, J.H., Ismail, W.N., & Hassan, M.M. (2018). Malware threats and detection for industrial mobile-IoT networks. *IEEE Access*, *6*, 15941–15957. doi:10.1109/ACCESS.2018.2815660

Shonola, S.A., & Joy, M.S. (2015). Security of m-learning system: A collective responsibility. *International Journal of Interactive Mobile Technologies (iJIM)*, *9*(3), 64–70. doi:10.3991/ijim.v9i3.4475

Sujithra, M., & Padmavathi, G. (2012). Mobile device security: A survey on mobile device threats, vulnerabilities, and their defensive mechanism. *International Journal of Computer Applications*, *56*(14), 1–6. doi:10.5120/8960-3163

Tairov, I.L. (2019). Mobile device management as a component of corporate IT infrastructure. *Business Management/Biznes Upravlenie*, (3), 60–71. Retrieved from https://www.ebscohost.com

von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Revised ed.). New York, NY: George Braziller.

Wibowo, K., & Ali, A. (2016). Mobile security: Suggested security practices for malware threats. *Competition Forum*, *14*(1), 119–125. Retrieved from https://www.questia.com