FACTORS AFFECTING INFORMATION SECURITY AND THE WIDEST IMPLEMENTATIONS OF BRING YOUR OWN DEVICE (BYOD) PROGRAMS

Dr. Abdessamed El Gbouri abdessamad.elgbouri@gmail.com
Authors' affiliation addresses: University of Fairfax

Dr. Scott Mensch smensch@iup.edu
Authors' affiliation addresses: Indiana University of Pennsylvania

Abstract

Mobile Internet use has increased and recently surpassed desktop usage. The United States government is no different in the use of mobile connectivity. The challenges of mobile device use have been accentuated since the government is considered a critical infrastructure. With the increase in information security concerns, many government stakeholders have enacted laws to establish comprehensive information security frameworks. This research effort was designed to review user's acceptance in adopting a Bring Your Own Device (BYOD) strategy. A qualitative study has been proposed using the Unified Theory of Acceptance and Use of Technology (UTAUT) as the basis for aligning interview questions. The intention of this study is to produce several themes, namely: convenience, data and personal security, privacy, and trust in the organization as the most concerning issues that could impact the decision to participate in such a program.

Key words: BYOD, Security, Cybersecurity, Information Security, Mobile Device Security

Introduction

Information Security (IS) policy effectiveness is only as good as the ability to impose its requirements as explained by Barman (2002). Barman also explained that the policy documents must be "living documents" that change as the organization grows and the technology advances. Although organizations tend to put in place the latest technical solutions to increase productivity and proficiency of their operations, relevant and updated IS policies must be properly implemented, as recommended by Vacca (2009): "The policy is almost always a work in progress. It must evolve with technology, especially those technologies aimed at surreptitiously getting into your system. The threats will continue to evolve, as will the systems designed to hold them at bay."

The National Institute of Standards and Technology (NIST), in collaboration with the National Vulnerability Database (NVD), published the special publication 800-53 (revision 4) (n. d.) outlining the security controls and assessment procedures for federal information systems and organizations, Souppaya and Scarfone (2016a) outlined the BYOD controls out of the NIST Special Publication 800-53 (Rev. 4) in their Appendix A of the NIST SP 800-46 (Rev. 2), and specified the main concerns as Access Controls (AC controls), Security Assessment and Authorization (CA controls), Contingency Planning (CP controls), Identification and Authentication (IA controls), Risk Assessment (RA controls), System, and Communication Protection (SC controls).

The collection of controls mentioned above outlines a total of 12 controls out of a plethora of controls presented by the NIST SP 800-53 (r.4). This group of 12 controls indicates that the security policies that will be drafted will generally be related to these controls, where in

fact the latest BYOD capabilities and their related policies should include the majority of the control families outlined by the general NIST SP 800-53 (r. 4), including Audit and Accountability (AU), Awareness and Training (AT), Configuration Management (CM), Incident Response (IR), Media Protection (MP), and specifically all high impact outlined controls.

Background

The defense critical infrastructure program (United State Department of Defense, n. d.), which is part of the Office of the Assistant Secretary of Defense (Homeland Defense and America Security Affairs), defines critical infrastructure as:

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. (para. 3)

The above characterization indicates that the United States Department of Defense (USDOD) infrastructures, including the military, are, by definition, critical infrastructures since they are integral participants in the overall protection of the country's interests and assets. Although the Presidential Policy Directive PPD 21 (2013) cites the Department of Defense as one of the 16 sectors identified as critical infrastructures, it also cites communications and information technology as two other critical infrastructure sectors. Assets must be protected at rest or in transit by developing the proper technical systems for sensitive information sharing as reported by the Deputy Secretary of Defense in 2011 when Lynn explained that the USDOD's strategy is based on five categories:

1. Treating cyberspace as an operational domain like land or sea,
2. Introducing improved defenses and new operating concepts for USDOD networks,
3. Working with DHS (U.S Department of Homeland Security) and the private sector to secure critical infrastructure,
4. Working with the international community, and
5. Building a stronger cyber workforce and investing in cybersecurity research and development (U.S. Department of Defense, 2011).

Vorakulpipat, Polprasert, and Siwamogsatham (2014) provided an overview of research and practice issues in mobile device security focusing on critical infrastructure. In the overview of the study, the authors stated the most concerning trends that included access controls, next-generation firewalls, BYOD control mechanisms, management, and policy.

The present study will address a crucial concern related to BYOD policies. The research will relate the behavioral elements that prevent end-users from adopting and accepting the requirements and the responsibilities that come with enrolling into a BYOD program. It will attempt to answer the questions regarding the appealing factors of the BYOD solution from the end-user perspective and the incentives that could make the most sense for users to adopt the BYOD capabilities, all while considering presently implemented BYOD policies.

Problem Statement

The full implementation of the BYOD programs will be of paramount importance since well-thought out security policies will increase employee satisfaction, improve productivity, and lead to cost-effective operations, and finally offer the flexibility employees so often desire, as reported by DeShield (2017). The study could reveal the acceptance rates of the BYOD program and the barriers to such implementations, with the hope of drafting a generalized BYOD policy framework specific to critical infrastructures. D'Arcy, Herath, and Shoss, (2014) surveyed 539 employees to understand the relationship between "Security-Related Stress" (or SRS) and deliberate information security policy (ISP) violations, and indicated that SRS, "engenders an emotion-focused coping response in the form of moral disengagement from ISP violations, which in turn increases one's susceptibility to this behavior" (p. 285). The objective of the study was to relate the policy elements that will limit SRS and promote adherence to the ISP, as well as identifying the policies that could be preventing end-users from enrolling into the BYOD programs.

The problem to be studied in the present research relates to the impact of the available BYOD policies to maintain IS operations on the proper adoption and enrollment levels needed into a BYOD program. The current study will benefit both business and governmental communities as each has been impacted by the increasing trend in mobile technology. Investigating the impact of the policies on the success of the program will provide insights into the major policy elements that affect the widest implementation of the program, giving a wider insight on a new BYOD policy framework for critical infrastructures.

Introductory Method and Research Design Descriptions

The planned method in this study is a qualitative approach. The purpose is to identify the main topics that affect the proper implementation of a BYOD program and the main barriers to the reserve members' acceptance to enroll in the BYOD program. Detailed interviews of 45 minutes to 1 hour long will be conducted with 15 to 20 Reservists, with the objective to extract the effects of policies on the acceptance of the BYOD program. This level of acceptance will reveal the effect of policies on the implementation of the BYOD program. The research will orient the questions without bias, intervention, or preconceived notions towards information security matters. The interview questions will be open-ended to avoid introducing the researcher biases even involuntarily. With unbiased rigor and impartiality, the respondents will be able to relate how they see the problem from their perspectives, and what could be the possible solutions to allow the use of their private devices to access government web platforms without compromising their privacy or government confidentiality, integrity, and availability of information.

During the interviews, the purpose of the study will be introduced with a short explanation regarding the organization's BYOD program and then will utilize a series of open-ended questions gauging understanding of the program and its objectives. The demographic questions will be the only type that will be direct and specific. The focus of the interviews will be the collection of data about the understanding of the respondents regarding main information security behaviors when using their private devices, as well as on the policy elements that cause

the most resistance to BYOD enrollments by end users. Other data that could possibly be collected through these interviews could be the utilized platforms and devices. Any follow-on questions could indicate additional relevant information, especially on the factors and device usages and capabilities that end-users would not want to sacrifice to be able to use the BYOD program. The objective is to accumulate comprehensive data that could be used immediately by the leadership in making enhanced decisions related to policies, while ensuring successful implementations of programs.

Purpose of the Study

The research method for the present study will be qualitative in nature. Specifically, this study will utilize the exploratory, phenomenological method, a non-positivism approach. The use of a quantitative study would mean that the relevant factors affecting the end-user's acceptance of a BYOD policy program would have already been identified; however, this cannot be accurately done without having the perspective of the end-users themselves. Qualitative phenomenology is often described as a study of experience or consciousness (Husserl, 1970). One overarching concept is to accurately describe a phenomenon as captured through understanding the experiences of one that has lived the reality (Groenewald, 2004). Merriam (2009) suggested any qualitative study provides a "richly descriptive" (p. 16) outcome, often given the term emerging themes. A qualitative study could provide the main elements the respondents see as the prevalent factors toward a decision of program acceptance.

Research Method Appropriateness to the Study

The purpose of the study is to investigate the end-user's behaviors towards accepting or denying a new IT solution. The second perspective is investigating the complexity and conformity of the drafted policies to support and manage the new bring your own device solutions. This study may reveal the main factors preventing the widest implementation of the BYOD program into the organization component, and especially the general policy elements that could be considered as a security risk from both the end-user's, and the organization's perspectives, with the ultimate goal of providing a BYOD policy framework for any critical infrastructure.

Several strategies could be used to identify what the respondents know about these security risks. Some explanations could be provided on the widely known cyber-attacks, but the objective will answer all questions by relying on the cumulative data obtained from the interviews.

Specific Population Group

The general group for this study is the entire population of approximately 100,000 reserve servicemen spread over 160 reserve training centers located throughout 47 of the United States. However, the study will utilize a sample of that population which is a unit of 200 reserve servicemen. Due to national security concerns, the primary author has received permission to use this sample population and he had decided to withhold any additional identifying information to maintain operational security.

Significance of the Study

The Significance of the Study to the Academic

The problem in the present research study is identifying the reasons behind the successful implementation of BYOD policies when technology advances and policies become outdated. The considered challenges are specifically from the end-user's perspective, and what could drive them to not enroll in a BYOD program. This study will also develop and explain what the benefits of the BYOD solution are for the employees' productivity and what limitations and restrictions it puts on the use of their devices, especially because the personnel are part of critical infrastructure. The main objective is to identify a valid BYOD policy framework that could be extended to any critical infrastructure.

Nature of the Study

Existing literature in the BYOD technology and IS focuses mainly on the importance of BYOD as an information technology solution and the IS risks and recommendations to remediate them (DeShield, 2017). The present research design is focused on looking primarily at the effect of the policy itself and some of its characteristics that may hinder the achievement of IS in any organization when implementing BYOD. The policy can be complex or unrealistic, can be too hard to implement, or too costly to accept by either the leadership for its dollar amount risks or the end-user due to loss of security and privacy.

Research Question

The overarching omnibus question for this study is: How can the concerns and issues that have impaired acceptance of using personal mobile policies at a unit level by reserve service members in a Military reserve unit be addressed? The study will utilize a phenomenological, qualitative approach to studying the experience of service members in acceptance of policies related to using personal BYOD devices for work related to reserve duties.

The present study is not about the technical feasibility of the BYOD program and solutions, but it is rather about the factors that affect the adoption of a company-wide BYOD implementation. The benefits of this study are to identify: why is BYOD not widely used? What are the shortfalls that are affecting its appeal to end-users? Are there any recommendations to improve the program appeal in reaching, convincing, or even incentivizing use by the reservists? Are there any better ways to explain the program helpfulness, its importance, and more notably, its value to the individual serviceman and to the organization? Finally, what is the BYOD policy framework that should be implemented and followed to ensure the strongest information security posture for critical infrastructures?

Assumptions

The main assumption of this study is that it is feasible to have a government-approved mobile application (MC-BYOD Mobile App) that can be linked to mobile device management or an MDM framework to allow proper control not only over the mobile application but also over

the device itself, including operability. This also assumes that the device is entered in the encrypted mode using an inserted CAC and has location identification, as well as access control management, based on the network accessed and the location of the device. This MDM program will also allow the organization to have provision and update the MC-BYOD application.

For the sake of this study, it will be assumed that this BYOD program will be implemented on privately owned devices and not on devices provided by the USDOD. Although it is feasible to implement this costly solution at a wider scale, it is only implemented for key personnel; however, it is more realistic to assume that the organization would want to cut cost by implementing a mobile app and a client, as well as an equally advanced MDM platform, rather than entering in the cost-benefit analysis of providing mobile devices to the entire organization's reserves.

Literature Analysis

Studying information security includes a wide range of topics to consider. Schou and Hernandez (2015) outlined several concerns that pointed to viewing information security from a holistic perspective. Effective computer security will focus on risk management strategies, information assurance governance processes, planning processes, risk mitigation processes, threat detection, and recovery processes. Most importantly, Schou and Hernandez related the application of information security in select industries, which will be most relevant to the present study as the federal government is a very large user of the latest cybersecurity solutions.

Veiga and Eloff (2007) explained the aspects that relate to information security governance, offering a new framework on the governance of information systems management. Veiga and Eloff explained the main objectives for information security programs, including protecting, safeguarding information, and ensuring the CIA triad: confidentiality, integrity, availability.

Soukup (2015) explained how the smartphone is a device that combines telephone services with computer capabilities. He also demonstrated how such phone operability depends on not only manufacturers of the hardware but also telecommunication services and other privately-owned companies. Enge (2018) completed a 2018 study on mobile versus desktop usage. According to Enge, mobile usage was taking the lead over desktop usage by volume of activity between the years of 2016 and 2017. The results showed that in only one year many activities by mobile users had increased by over 10%. As indicated by the C4/CIO report (2013), this organization was no different in its challenges in managing its mobile strategy. The use of mobile technologies had become an integral information security concern for all government entities. According to the report, steps have been taken to manage these important IT solutions and the Bring Your Own Device technology was only one of them.

The USDOD has mandated organizational regulations for use of technology all over the globe. Many of its employees, civilians, and uniformed servicemen rely on European telecommunication services making them subject to international information related laws, including the GDPR (Intersoft Consulting, Art. 3, para. 5, n. d.). In article 50 of the GDPR, four pillars have been enumerated to ensure international cooperation for the protection of personal

data all based on developing collaboration mechanisms in legislation and regulations enforcement processes. Some regulations have global impact, such as stopping the flow of data to a country as a reprimand for a non-compliant organization (Intersoft Consulting, Art 58, para. 2).

DeShields (2017) completed a study on the challenges of BYOD technology and stated that employee satisfaction was one of the factors that made the adoption of the BYOD solutions more appealing for businesses, reporting that 11% of employees over age 45 and 13% of employees under age 35 appreciated the freedom of independence and choice of technology. The same was supported by Abubaker, Murray, and Armarego (2017) suggesting that BYOD effectively improves mobility, flexibility, and the freedom of technology of choice.

Other than the benefits BYOD has for the employee, the employer has the most to gain from its implementation, since it maintains remote visibility over the accessing devices and the considerable reductions in costs (Wani, Mendoza, & Gray, 2019). In addition, the organization has a lot to gain from increased mobility and productivity (Amoud & Roudies, 2017). The use of BYOD technology and its capabilities increase employee's satisfaction (Deshield, 2017). Generally satisfied employees are happy (Franca, Sharp, & Da Silva, 2014) therefore more efficient in their work environment.

Risk Management

As indicated by Schou and Hernandez (2015), risk management is an integral domain in managing information security. Hopkin (2014) outlined the fundamentals of risk management to include understanding, evaluating, and implementing effective strategies to manage risk. The recommended options are either to reduce risk, accept the risk, mitigate the risk, or transfer risk by purchasing insurance against the threat possibilities. In the case of BYOD technology, Peredo (2017) reports that in the health care industry, in many instances "mobile devices were the entry point that malicious actors used to compromise the system" (p. 32). Peredo also reports that in 2015 alone, more than 111 million individuals had data lost because of cyberattacks in the United States.

Other solutions in mitigating risks of BYOD technologies are the advancement of comprehensive policy frameworks, root-based solutions (applications running alongside and with the same permissions as the operating system of the smartphone), secure containers (virtualization solutions where multiple virtual phones can be running on the same physical phone), and hardware-backed solutions, which is the reliance on a separate environment that can run security dedicated functionality, parallel to the Operating System (OS) and separated from it by a hardware barrier. These solutions were explained by Kanonov and Wool (2016) in an attempt to understand secure containers in the Android operating system.

Privacy Concerns and Feasibility

According to Gajar, Ghosh, and Rai (2013), successful deployment of a BYOD program depends on the effective management of security and privacy-related matters. Garba et al. (2017) provided a systematic approach to the management of BYOD security and privacy. The authors

outlined the lack of research on BYOD policy management and the importance of a dynamic approach to BYOD security, privacy controls, and policy drafting, taking into consideration the nature of the organization, the internal IT security being used, the privacy budget, and the level of risk tolerance acceptable to the organization.

A Study conducted by Hao Chen, H., Li, Chen, L., and Yin (2020) when 235 employees of Chinese entreprises were surveyed to understand employees' adoption of the BYOD: and they specifically looked into the roles of information security-related conflict and fatigue. Chen et al. (2020) found that there is a correlation between information security–related conflict and information security fatigue among employees. This study started with a number of hypothesies. This strategy is different from the current study since it is limiting and not inclusive, the present study conducts a qualitative study that asks open questions and let the respondents provide the themes of concern, many themes will be revealed based on the proer coding and analysys of the results, the conflict management measures and emotion management strategies explained in the study by Chen et al. (2020) are expected to be only one aspect of the themes that will be revealed by the present study.

Other studies investigated which types of employees adopt BYOD and how they benefit from it, such as Meske, Stieglitz, Brockmann, and Ross, (2017). The present study didn't categorize the types of users, mainly because the population interviewed was very diverse, and the implementation of the BYOD program should not consider the particularities of the end users.

Governance and Policies

Gajar et al. (2013) conducted a study to identify BYOD risks and mitigating strategies and concluded that governance of BYOD "would start right from the requirements of the organization which would attract all the legal, statutory, and compliance issues along with the policies of the organization" (p. 69). Barman (2012) provided a detailed approach to drafting information security policies. The author explained the policy drafting processes, how to write policy documents, and how to maintain policies by continuously checking on their relevance, value, and alignment with the organization's business vision, goals, and plans. Planning and enforcing compliance with approved policies was one of the primary activities in the policy management process, in addition to implementing effective review processes (Greene, 2014). To consider the main topics of information security, Greene outlined security program policies, principles, and practices, including information security frameworks, governance and risk management, asset management, human resources security, physical and environmental security, communications and operations security, and access control management. In every information security domain, the first milestone is to draft a proper policy. BYOD use is no different, as explained by Kadam (2007). Kadam also outlined detailed strategies to develop and implement the most effective information security policies and, most importantly, the proper ways to measure the success of the information security program.

The particularity of the present study is its value to the United States government and any other critical infrastructure. These critical sectors include energy, water, food supply, healthcare, information communication technology, transport, banking, finance, and major research

institutes (United State Department of Defense, 2017; Vorakulpipat et al., 2014). The objective of this study is to build on the existing literature on BYOD policy frameworks and draft a more comprehensive framework that will take into consideration the extremely high risks of mobile technologies on critical infrastructure, since their "impact is not only at the organizational level but also at the national level" (Vorakulpipat et al., 2014, para. 6).

As the Unified Theory of Acceptance and Use of Technology (UTAUT) suggests, employees' acceptance or denial of any new technology is based on several factors, including performance expectancy, effort expectancy, social influence, and the facilitating conditions (DeShield, 2017; Lescevica et al., 2013). Similarly, but based on Protection Motivation theory, Hovav and Putri (2014) conducted a study where they investigated the employees' intent to comply with organizational BYOD policy. The authors found that:

The independent variables of perceived threat appraisal, perceived response efficacy and perceived digital mutualism justice significantly and positively affected employees' intent to comply with an organizational BYOD policy. On the other hand, perceived freedom threat negatively affects intention to comply with BYOD policy (p. 9).

After acceptance of the technology, employees have to comply with the information security policies governing enrollment, use, and performance via the BYOD solutions. Györy, Cleven, Uebernickel, and Brenner, (2012) reported that employees' non-compliance with security policies was the largest information security threat in the user-driven IT environment.

The Need for BYOD Policy Frameworks

To ensure the nation's information security, especially regarding its critical infrastructure, the United States White House released Executive Order 13636 "Improving critical infrastructure cybersecurity" (Executive Order 3636, 2013). This order directed the National Institute of Standards and Technology to draft a cybersecurity framework (NIST Cybersecurity Framework Background, n. d.). The Cybersecurity Enhancement Act of 2014 further reinforced NIST's E.O. 13636 role.

The review of the literature revealed a gap in research related to the use of the BYOD technology in the government and specifically in the organization reserve community. The current study will provide an insight into the importance of BYOD policy updates and the effects on the information security of the organization. The qualitative aspect of this research will provide a unique analysis of BYOD policy challenges revealed through open interviews with end-users.

The literature outlined above relates a large number of research studies conducted to understand more about BYOD technology and its challenges, specifically its policies. These studies advanced the body of knowledge on BYOD (DeShield, 2017). BYOD has morphed and new techniques have emerged. It is only a matter of time before we see new ways of using mobile devices for much more than just accessing work, mainly because of the extensive usage of mobile devices compared to desktop computers (Enge, 2018; Federal Resources, 2018). It is

expected that the way of doing business itself will morph to benefit from the capabilities of mobile devices.

To ensure these users have all the information needed for making an informed decision to enroll or not in this type of program, it is necessary to evaluate the possible barriers to their decisions. The present study will explore the policies of a BYOD program and how these policies could affect the decision toward enrollment. This study will also provide an insight into the effects of inappropriate policies related to information security that are imposed by the organization. The particularity of this study is its relation to critical infrastructure. Executive Order 13636 (2013) ordered the government to utilize as much of the input of the private sector as possible to increase the information security of the nation, including critical infrastructure.

Research studies in these domains do not always receive the widest academic publicity and support due to the sensitivity of government issues and the potential appeal for those who desire harm. However, academia has to refocus information assurance, including the main researched subfields such as forensics, information security, and intrusion and penetration testing to more defensible approaches, as explained by Kallberg and Thuraisingham (2012):

The future of cybersecurity is both defensive information assurance measures and active defense driven information operations that jointly and coordinately are launched, in the pursuit of a cohesive and decisive execution of the national cyber defense strategy. The cohesive cyber defense requires universities to optimize their campus-wide resources to fuse knowledge, intellectual capacity, and practical skills in an unprecedented way in cybersecurity. The future will require cyber defense research teams to address not only computer science, electrical engineering, software, and hardware security, but also political theory, institutional theory, behavioral science, deterrence theory, ethics, international law, international relations, and additional social science. (p.1)

The research method for the present study will be qualitative in nature. The use of a quantitative study would mean that the relevant factors affecting the end-user's acceptance of the program would have already been identified. This could not be accurately done without having the perspective of the end-users themselves. The qualitative study approach relates the policy elements causing the most resistance to BYOD enrollments, as seen through the experiences of the respondents. The expectation is that the emerging factors would reveal concerns in adoption and would go into more depth than with a quantitative study. A qualitative approach revealed further insight into the challenges on the risks of outdated policies on IT solutions on information security (Landoll, 2016).

For this study, respondents will be given an overview of the BYOD technology and its benefits to the user, to increase trust and inclusion. The participants will also be given the value of the program to the organization. The information provided will be necessary to help the participants understand their role in the decision to adopt or reject using a personal device for military activities. The reasons behind the interview will be explained, such as the guarantee of confidentiality, how confidentiality and privacy are maintained, and the process of data collection and analysis.

The open-ended questions used during the participant interviews sessions will be selected as a starting point for conversation, to gauge the participant's understanding of the question, and ultimately excite the participant's thinking and insight. The four constructs of UTAUT are as follows:

1. Performance Expectancy: During the interviews, the users will be asked about their expectations when desiring to use their mobile devices to access corporate platforms based on some variation of a BYOD program. The desire is that they would reveal insights into limitations and challenges, based on experience, hindering their desired expectations.
2. Effort Expectancy: The participants will be asked about the expected needed effort they would make in using the new technology solution, including the ease of initial device and software set up, ease of initiating secure connections via their mobile devices, their physical efforts, time to use, and cost of using their online connectivity.
3. Social Influence: Being the age of mobile connectivity and its benefits to users and organizations, the participants will be asked to answer a question related to the extent of social influence in their decision to rely on a certain technology. Two sources will be considered in the probing phases of the interviews: society and marketing. When considering the societal influence, the participants will be asked to answer questions on the effect of social networking, on word of mouth reviews about the considered technology, peer reviews, and online reviews. The marketing considerations will address to what extent the participant shaped opinion from the advertisements on social media feeds, email campaigns and targeted advertisements based on web browsing histories, and views of online content such as views articles, podcasts, and videos.
4. Facilitating Conditions: The participants will be asked what they believed the conditions were that the organization put in place to make it easy for them to accept the technology in question, including but not limited to the ease of use, cost, if any, repercussions of non-compliance with government policies, risks to the member's information or the organization's data, and the balance between risks and the value of communication to the immediate mission.

Implications and Conclusions

The analysis of the collected data will be conducted after all interviews are transcribed and emerging themes are identified, the results presented will aim at drafting a more inclusive BYOD Policy framework. Businesses usually have less control over influencing user acceptance; however, the proposed study hopes to reveal the potential for government and business to understand and control some aspects of the acceptance levels of users. This possibility for understanding the elements that help an end user to decide to accept or reject a BYOD solution is important. For this study, the concern is heightened by the subject of the research, a segment of the nation's critical infrastructure.

So often organizations implement solutions based on cost/benefit margins, but rarely based on expectations on criteria that the organization has little to no control over (Landau, 2018), namely the end-user behavioral expectations. The purpose of the study is to introduce potential recommendations by adding a layer to current framework models for programmatic implementations. The level of acceptance of a new technology solution can be influenced by expanding preparation efforts to include training related to the forthcoming startup of the solution. Although the proposed study will focus on a government entity, the recommendations

from the end-user community could be important in any organizational structure. The present study intends to demonstrate how valuable themes in the end-user decision-making process toward acceptance of a BYOD program can be.

References

Abubakar, G. B., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security, 25*(4), 475-492. doi:10.1108/ICS-03-2016-0025

Amoud, M., & Roudies, O. (2017). Experiences in secure integration of BYOD. *Proceedings of the 7th International Conference on Information Communication and Management (ICICM 2017)*. ACM, New York, NY, USA. (pp. 127-132). doi:10.1145/3134383.3134394

Barman, S. (2012). *Writing information security policies*. Indianapolis, IN: New Riders Publishing

Chen, H., Li, Y., Chen, L.,Yin, J. (2020). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security–related conflict and fatigue. Journal of Enterprise Information Management, ISSN: 1741-0398. doi: 10.1108/jeim-10-2019-0318

D'Arcy, J., Herath, T., & Shoss, M. (2014) Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318, doi:10.2753/MIS0742-1222310210

DeShield, L. (2017). *The challenges of implementing bring your own device*. Retrieved from https://pdfs.semanticscholar.org/72ad/2e8689233676c065819204b88d34515fd3a2.pdf

Enge, E. (2018). Mobile vs Desktop Usage in 2018: Mobile takes the lead. Retrieved from https://www.stonetemple.com/mobile-vs-desktop-usage-study/

Kanonov, U., & Wool, A. (2016). Secure containers in Android: The Samsung KNOX case study. *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices* (SPSM '16). ACM, New York, NY, USA, 3-12. doi:10.1145/2994459.2994470

Landoll, D. (2016). *Information security policies, procedures, and standards: A practitioner's references*. Boca Raton, FL: CRC Press.

Meske, C., Stieglitz, S., Brockmann, T. and Ross, B. (2017), "Impact of mobile IT consumerization on organizations- an empirical study on the adoption of BYOD practices", in Nah, F.F.-H. and Tan, C.-H. (Eds), HCIBGO: Lecture Notes in Computer Science, pp. 349-363. doi: 10.1007/978-3-319-58484-3_27

National Institute of Standards and Technology. (n. d.). *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*. NIST special publication 800-53 (rev. 4). Retrieved from https://nvd.nist.gov/800-53/Rev4

Peredo, M. (2017). *Critical elements affecting mobile device management adoption by information technology and information assurance practitioners in Southern California*. Retrieved from https://fairfax.instructure.com/courses/81/files/7597?module_item_id=10403

Souppaya, M., & Scarfone, K. (2016a). *Guide to enterprise telework, remote access, and bring your own device (BYOD) security*. NIST Special Publication 800-46 Revision 2. Doi:10.6028/NIST.SP.800-46r2

United States Department of Defense (n. d). *DOD protected critical infrastructure program*. Retrieved from https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-Global-Security/Defense-Critical-Infrastructure-Program/

United States Department of Defense (2017). *Defense critical infrastructure program (DCIP): USDOD mission-based critical asset identification process (CAIP) Manual 3020.45*. Retrieved from https://www.hsdl.org/?view&did=801336

U.S Organization Forces Reserve, (n. d.). *U.S Organization Forces Reserve, augment. reinforce. support*. Retrieved from https://www.marforres.servicemans.mil/About/Media-Info/

Vacca, J. (2009). *Computer and information security handbook*. Burlington, MA: Elsevier Science & Technology

Wani, T., Mendoza, A., & Gray, K. (2019). BYOD in hospitals - Security issues and mitigation strategies. *Proceedings of the Australasian Computer Science Week Multiconference* (ACSW 2019). ACM, New York, NY, USA. Article 25. doi:10.1145/3290688.3290729