The undersigned, approved by the Doctoral Dissertation Committee, have examined the dissertation titled

BRING YOUR OWN DEVICE PROGRAMS WITHIN THE ENTERPRISE:
THE ANTECEDENT EFFECTS ON BRING YOUR OWN DEVICE ADOPTION AND USE

presented by Steven A. Liegl Jr.

a candidate for the degree of Doctor of Business Administration

and hereby certify that in their opinion it is worthy of acceptance.

Balaji Sankaranarayanan, Ph.D.
Associate Professor of Information Technology and Supply Chain Management
Committee Chair

SIGNATURE: ________________________________

Andrew Ciganek, Ph.D.
Chair of Information Technology and Supply Chain Management
Second Committee Member

SIGNATURE: ________________________________

Aditya Simha, Ph.D.
Associate Professor of Management
Reader

SIGNATURE: ________________________________

BRING YOUR OWN DEVICE PROGRAMS WITHIN THE ENTERPRISE: THE ANTECEDENT EFFECTS ON BRING YOUR OWN DEVICE ADOPTION AND USE

A Dissertation

Presented to

The Graduate Faculty of

The University of Wisconsin – Whitewater

In Partial Fulfillment

Of the Requirements for the Degree

Doctor of Business Administration

By

STEVEN A. LIEGL, JR.

Dr. Balaji Sankaranarayanan, Dissertation Chair

DECEMBER 2021

ACKNOWLEDGEMENTS

This work would not have been possible without the dedicated guidance, expertise, and encouragement from the members of my dissertation committee, Dr. Balaji Sankaranarayanan (Chair), Dr. Andrew Ciganek, and Dr. Aditya Simha (Reader). I would like to thank Dr. Sankaranarayanan for the countless hours spent emailing, talking on the phone and Zoom, suggesting new ideas, and giving me the needed information to bring this all together. Your passion for educating motivated my willingness to succeed and minimized the moments of discouragement. I am eternally grateful for your sacrifices to prioritize my dissertation and am forever humbled. To Dr. Andrew Ciganek, thank you for the time spent with me to discuss the many options available to me with the data to which I had access. Your insight and ideas are visible within the outcome of this work.

In addition, I would like to thank the faculty, staff, and visiting speakers who came together to run this program for us. The many nights and weekends that were spent together will leave a lasting impression on all of us. To my fellow cohort, the students who kept me motivated throughout the process, I look forward to the continued friendship and support. Just knowing that we were in this together made it even more achievable.

Most importantly, thank you to my family; my wife, Heather, daughter Rachael, and two sons Seth and Marcus (Fred). I know this journey has taken a significant amount of sacrifice from each of you. This would not have been possible without your support; thank you.

BRING YOUR OWN DEVICE PROGRAMS WITHIN THE ENTERPRISE: THE ANTECEDENT EFFECTS ON BRING YOUR OWN DEVICE ADOPTION AND USE

STEVEN A. LIEGL JR.

Dr. Balaji Sankaranarayanan, Dissertation Chair

ABSTRACT

Traditionally, organizations have provided the necessary task-related devices (e.g., laptops, smartphones, tablets) for employees. However, recent years have seen alternative devices belonging to employees or other sources used in corporate settings for completing work tasks. With the desires for flexible work conditions and constant connection, bring your own device (BYOD) policies have become ubiquitous. Building on adoption theories and prior BYOD research, this dissertation seeks to create a foundational model for evaluating the factors associated with BYOD adoption and use.

In Essay 1, I focus on understanding and enumerating the patterns of BYOD use in corporate settings based on various user-level factors over a period of time. I conducted time series analyses on secondary data of employees' systems captured in their databases to demonstrate the change over time and provide future forecasting of BYOD adoption. Findings showed that in an organization that has a BYOD program there are varying levels of individual usage, regardless of device type, and receiving a financial incentive can have an impact on adoption and use.

In Essay 2, I drew upon adaptive structuration theory (AST) and tested a research model of BYOD adoption and use. I theorized that security, data ownership, privacy, and financial factors influence exploratory and exploitative task and technology adaptation of BYOD. Further, I posited that such adaptation will positively impact BYOD use. The research model was tested using a survey of employees on their use of BYOD in corporate settings. Findings showed that the antecedent factors have a significant influence on exploratory and exploitative task and technology adaptation, which in turn influence BYOD use within the organization. Therefore, this study highlights the mediating role of task and technology adaption factors, demonstrating the significance of adaptive structuration in the BYOD context.

Findings from this dissertation have important academic implications to the BYOD literature, extending the application of AST to the context of BYOD. Notably, findings from this dissertation have practical significance to help organizations understand data ownership, security considerations, and financial incentives which encourage BYOD adoption and use.

Keywords: BYOD Use, Task Adaptation, Technology Adaptation, Adaptive Structuration Theory, Security Controls, Data Ownership, Financial Incentives.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

TABLE OF CONTENTS (CONT.)

TABLE OF CONTENTS (CONT.)

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

Chapter 1: Dissertation Introduction

The global work environment and the need to be always connected has been on the upswing in recent years (McCune, 1999). As a result, the reliance on continually interacting with company data and performing critical business tasks is growing at astonishing rates (Schmidt, 2012; Thomson, 2012). These interactions can be as simple as checking email or as complex as setting critical security parameters (Wang, Weeger, & Gewald, 2017). In the past, the requirements and offerings that employers provided significantly varied from what is often required or requested today (Thomson, 2012).

To meet this need, two methods are currently utilized in organizations. First, issuing corporate-owned devices allows employees access while in the office environment and working remotely (Astani, Ready, & Tessema, 2013). Second, companies continue to implement bring your own device (BYOD) environments that can support the use of employee-owned devices (Evans, 2013). In some cases, the BYOD policy is the only solution provided to employees, with overall organizational program support (Alaskar & Shen, 2016). The decision to adopt BYOD can have several antecedent conditions; financial controls, security needs, and business demand are vital drivers (Munroe, 2013).

Connectivity with corporate systems is only one piece of the puzzle that enables employees easy access when they are not in the standard brick and mortar buildings (Fisher & Allen, 2015). Having adequate security measures varies, providing simple or complex methods depending on individual organization requirements (Eslahi, Naseri, Hashim, Tahir, & Saad, 2014). Like the processes that evolved to make BYOD a reality, security requirements and capabilities have also been required to advance to reduce the overall risk of unauthorized access or data loss (Wittmann, 2011).

Individual employees have the ability and, in some cases, the requirement to modify how they perform tasks or use the technology. Schmitz, Webb, and Teng (2010) provided context demonstrating how individuals adjust behaviors based on personal traits, ultimately impacting their overall performance. Adopting new or existing technology in the enterprise will likely have varying results and dynamic effects as technology and tasks evolve (McFarlan, 1984; Parsons, 1983).

Combined, these factors can define the overall success or failure of the BYOD policies (Porter & Millar, 1985). The broad employee acceptance and use of the BYOD environment can play a significant role (Lee, Warkentin, Crossler, & Otondo, 2017). While companies see great value, there are specific requirements that employees will need to be aware of and accept as part of their decision to enroll in BYOD (Caldwell, Zeltmann, & Griffin, 2012).

Research Questions

With many organizations deciding to eliminate corporate device options and opt for the BYOD model, the introduction of new obstacles requires proper analysis and preparation (Caldwell et al., 2012). The obstacles range from device support options, security requirements, and defining who will bear the financial burden for the environment required to ensure a functionally acceptable solution while providing necessary data protection (Violino, 2012). What was once an avenue for simple application access, such as basic email, has expanded into the world of sensitive corporate data (Munroe, 2013). These added requirements will require modifications to the overall support model from both an organizational and employee perspective (Astani et al., 2013)

In a traditional configuration, a standard device and solution would support remote connectivity for employees and contractors. With the expansion of the BYOD programs, additional variables are now presented that must be factored in when deciding on an appropriate solution (Evans, 2013). As part of any solution, there is an associated cost that may be shared or absorbed by either the employer or employee. This factor is somewhat of a moving target as security requirements are modified and the company’s overall policy matures (Scarfo, 2012).

While these factors impact both the organization and employee, there is limited information available to understand BYOD's adoption rates across an employee base. This will allow organizations to analyze and predict the employee adoption rate and impact before investing in this approach. Therefore, this dissertation seeks to address the following overarching research questions:

1. What are the impacts of security controls, corporate data ownership, privacy controls, and financial incentives on task and technology adaptation and BYOD adoption?
2. Are there any impacts of task and technology adaptation on BYOD use?

Research Methods

This dissertation utilizes a combination of primary and secondary data in the two essays. In Essay 1, titled “Bring Your Own Device Adoption and Use: The Impacts of Data, Security and Financial Factors,” I analyze secondary data to understand and enumerate how antecedent factors impact BYOD adoption and use over time. The employee data consisted of multiple levels and job types. In Essay 2, titled “Bring Your Own Device Adaptation: The Antecedents Influencing Individual Adaptation to Technology Capabilities,” the focus is on addressing individual decisions to adopt and use BYOD based on BYOD policy choices. This study explains how individuals adapt their tasks and technology to influence BYOD use in the organization through the use of a survey. The survey focuses on the individual use of BYOD within the organization and provides the context to allow for an understanding of the effects of the various antecedents and mediating factors of adaptive structuration theory.

Contributions

The purpose of this study was to determine whether hardware, security, and financial policies have a significant impact on BYOD adoption and use. Through the use of secondary data and the conducting of an employee survey, the impact of various antecedents and mediating factors were established. Current research has focused on the organizational and individual benefits and how they impact BYOD policies (Eslahi et al., 2014). These findings were considered, and the focus shifted to how the evolution of this practice, along with the need to protect data, is embraced within an organization (Violino, 2012). As more organizations migrate fully to a BYOD policy and the sensitive data access requirements increase, there is an implicit expectation that the security requirements and risks will also increase (Thomson, 2012). The conditions will likely impact how employees leverage their devices while maintaining a clearly defined ownership relationship of data and devices (Smith, 2017). As technology changes along with the security landscape, requirements are likely to be altered, creating the possibility that this relationship also shifts (Schmidt, 2012).

In addition to the technology advancing, state legislation also places new requirements on how employers provide these services. For example, on January 1, 2019, Illinois implemented legislation requiring employers to offer a financial incentive to those employees required to use personal phone and internet services. Providing a view of how forced reimbursement has impacted overall BYOD adoption will give an insight into what can be expected from future behaviors and how it will affect the environment requirements and cost. Like most decisions, financial components are weighed to determine whether there is a cost advantage or a cost disadvantage; these new laws modify the formula (Ludwig, 2018). Also, combining use and adoption with adaptation will provide a view of the data that is an indicator of whether the antecedent factors have the majority of the impact on what we would classify as BYOD success and the foundation for deciding to implement such a program in place of the traditional corporate device configuration.

References

Alaskar, M., & Shen, K. N. (2016). Understanding bring your own device (BYOD) and employee information security behaviors from a work-life domain perspective. In *AMCIS 2016 proceedings*. Retrieved from https://aisel.aisnet.org/

Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems*, *14*(2), 195–201. https://doi.org/10.48009/2_iis_2013_195-201

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (bring your own device). *Competition Forum*, *10*(2), 117–121. Retrieved from http://iblog.iup.edu/americansocietyforcompetitiveness/competition-forum/

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., & Saad, E. H. M. (2014). BYOD: Current state and security challenges. In *2014 IEEE Symposium on Computer Applications and Industrial Electronics*, (pp. 189–192). doi:10.1109/ISCAIE.2014.7010235

Evans, D. (2013, August 23). *What is BYOD, and why is it important?* Retrieved from https://www.ware247.co.uk/Content/CMS/Files/What%20is%20BYOD.pdf

Fisher, W., & Allen, C. (2015). Road warriors and information systems security: Risks and recommendations. *Journal of Management Information and Decision Sciences*, *18*(1), 84–96. Retrieved from https://www.abacademies.org/journals/journal-of-management-information-and-decision-sciences-home.html

Lee, J., Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of monitoring mechanisms on bring your own device adoption. *The Journal of Computer Information Systems*, *57*(4), 309–318. doi:10.1080/08874417.2016.1184032

Ludwig, S. E. (2018, January 11). Why organizations should still care about BYOD. *Security*, *55*(1), 26–27, 31. Retrieved from https://www.securitymagazine.com/

McCune, J. C. (1999). Technology dependence. *Management Review*, *88*(1), 10–12. Retrieved from https://www.amanet.org/

McFarlan, F. W. (1984). Information technology changes the way you compete. *Harvard Business Review*, *62*(3), 98–103. Retrieved from https://hbr.org/

Munroe, F. (2013). Technological transformation—Implications for compliance from big data to BYOD. *Journal of Health Care Compliance*, *15*(6), 41–46. Retrieved from https://lrus.wolterskluwer.com/store/product/journal-of-health-care-compliance/

Parsons, G. L. (1983). Information technology: A new competitive weapon. *Sloan Management Review*, *25*(1), 3. Retrieved from https://sloanreview.mit.edu/

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review*, *63*(4), 149–160. Retrieved from https://hbr.org/

Scarfo, A. (2012). New security perspectives around BYOD. In *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications* (pp. 446–451). doi:10.1109/BWCCA.2012.79

Schmidt, J. (2012). Not your parents' workplace anymore—Managing the new security realities of BYOD. *Security*, *49*(9), 25. Retrieved from https://www.securitymagazine.com/

Schmitz, K., Webb, K., & Teng, J. (2010). Exploring technology and task adaptation among individual users of mobile technology. In *ICIS 2010 Proceedings*. Retrieved from https://aisel.aisnet.org/

Smith, W. P. (2017). Can we borrow your phone? Employee privacy in the BYOD era. *Journal of Information, Communication & Ethics in Society*, *15*(4), 397–411. doi:10.1108/JICES-09-2015-0027

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2), 5–8. doi:10.1016/S1353-4858(12)70013-2

Violino, B. (2012). The BYOD security challenge: The growing variety of new devices makes supporting and controlling access to systems and data much more challenging for IT. *Insurance Networking News*, *15*(8), 29.

Wang, X., Weeger, A., & Gewald, H. (2017). Factors driving employee participation in corporate BYOD programs: A cross-national comparison from the perspective of future employees. *Australasian Journal of Information Systems*, *21*, 1–22. doi:10.3127/ajis.v21i0.1488

Wittmann, A. (2011, November 14). BYOD? First get serious about data security. *InformationWeek*, (1316), 46. Retrieved from https://www.informationweek.com/

CHAPTER 2: BRING YOUR OWN DEVICE ADOPTION AND USE: THE IMPACTS OF DATA, SECURITY, AND FINANCIAL FACTORS

ABSTRACT

Organizations provide corporate-owned devices to employees both in the office environment and from a remote location. Recently, firms have started embracing bring your own device (BYOD) policies which allow employees to use their own devices in the work environment, offering an alternative option for providing information systems access to employees. Prior research has looked at several strategic and operational factors related to BYOD introduction in an organization, with employees choosing to either adopt BYOD early, late, or ignore it entirely. However, prior research on BYOD has not delved into changes in BYOD use over time. Notably, several factors, including financial and security, can impact BYOD use, which I examined.

This research study addresses the research question by examining employees' use of BYOD devices through the lens of these critical factors. I conducted a time series analysis of secondary data on employees' use of BYOD devices. The secondary data consisted of security protocols, financial incentives provided, and data ownership details. Findings from this study provide an understanding of the evolution of BYOD use over time in a corporate setting. Specifically, this study demonstrates that financial incentives can have an impact on the overall adoption and use of BYOD while the device hardware type does not appear to have an impact.

Keywords: BYOD use, Task adaptation, Technology Adaptation, Adaptive Structuration Theory, Security Controls, Data Ownership, Financial Incentives.

Chapter 2: Bring Your Own Device Adoption and Use: The Impacts of Data, Security, and Financial Factors

The extant literature provides a detailed view of the increasing requirements of a globally connected work environment. The reliance on secure capabilities to interact with company data and perform critical business tasks is growing at an astonishing rate (Schmidt, 2012; Thomson, 2012). These interactions can be as simple as a basic email or as complex as advanced security interfaces (Wang, Weeger, & Gewald, 2017). The current work environment has warranted two distinct approaches for managing the technology needs of employees (Ozigbo, 2013). First, organizations provide corporate-owned devices to employees in offices and remote locations (Astani, Ready, & Tessama, 2013). Second, companies are implementing bring your own device (BYOD) platforms, which can support the use of employee-owned devices within office environments (Evans, 2013). In some cases, the BYOD policy is the only supported solution in terms of employee preference and overall organizational program support (Alaskar & Shen, 2016). This decision has several supporting factors, but financial controls, security needs, and business demand are vital drivers.

One factor that can define the overall success or failure of the corporately adopted BYOD policies is the broad employee acceptance and use of the environment in which companies have invested (Lee, Warkentin, Crossler, & Otondo, 2017). While companies see great value, there are specific requirements that employees need to be aware of and accept as part of their decision to enroll in this BYOD service (Ragowsky, Licker, & Gefen, 2012). With many organizations deciding to eliminate corporate device options and opting for the BYOD model, it is important to highlight the obstacles involved (Caldwell, Zeltmann, & Griffin, 2012). The obstacles range from device support options, security requirements, and defining who will bear the financial burden for the environment required to ensure a functionally acceptable solution while providing necessary data protection (Violino, 2012). In a traditional configuration, a standard device and solution would support remote connectivity for employees and contractors (Santhanam & Hartono, 2003). With the expansion of BYOD programs, these additional variables significantly impact the security and connectivity solutions (Evans, 2013).

The purpose of this exploratory study was to determine whether security controls, corporate data ownership, and financial incentives have a positive or negative impact on end-user BYOD technology adoption. Current research has focused on the organizational and individual benefits and how they impact BYOD policies (Eslahi, Naseri, Hashim, Tahir, & Saad, 2014). This study shifted the focus of BYOD use and sought to understand how this practice's evolution and the need to protect data are embraced within an organization (Violino, 2012). As more organizations migrate fully to a BYOD policy and the sensitive data access requirements increase, there is an implicit expectation that the security requirements and risks will also increase (Rizzuto, 2011; Stephenson, 2014). The conditions will likely impact how organizations and employees leverage their devices while maintaining a clearly defined ownership relationship (Venkatesh, Morris, Davis, & Davis, 2003). As technology changes along with the security landscape, requirements are likely to be altered, creating the possibility that this relationship also shifts (Schmidt, 2012).

Theoretical Background and Literature Review

Theory Overview

Three theoretical positions have been examined to establish the various relationships associated with BYOD. With the need to develop the individual layer and the leadership position on supporting the structure needed for a successful program, two theories could be utilized. The unified theory of acceptance and use of technology provides the necessary framework to understand why a user's behavior is associated with BYOD. Task–technology fit can help determine how the leadership team applies criteria for making BYOD decisions. Lastly, the technology threat avoidance theory addresses one of the enterprise's core concerns with personal device use. Security and data protection provide some foundational considerations across the entire program. While the theories impact multiple aspects of the technology layers, the focus for this study was placed on both the on-premise and remote worker mobile device environments.

Unified Theory of Acceptance and Use of Technology Theory

Venkatesh et al. (2003) introduced the unified theory of acceptance and use of technology as a theory to define a user's planned behavior. While technology adoption can be simply captured in the number of people who own or use any device throughout their day, this theory allows researchers to dissect the overall behaviors. In addition to managing the broad adoption and use behaviors, there are implications associated with boundaries placed on individuals that can impact their willingness to consider using or adopting technology solutions provided by sponsoring companies (Weeger, Wang, & Gewald, 2015). As business processes are altered to be technology-driven, there is a need to understand how each user leverages specific hardware to perform each task versus an aging process that was once paper-driven.

Task–Technology Fit Theory

In addition to the overall acceptance model, there is a theoretical view of how tasks and technology directly impact the mobile workforce (Zhang, Guo, Wang, Chen, & Wei, 2011). Task–technology fit provides another theory that allows one to understand better how users may decide which devices or applications can best assist them. Also, organizations can evaluate the overall employee base and incorporate processes and equipment that will meet the need, increasing the likelihood that all defined outcomes will be positively impacted (Leonardi, 2013). While a user may prefer a specific type or brand of the device, applications and technology platforms may not provide the flexibility to make these individual decisions. Conducting proper investigation and understanding the technology will establish the baseline related to the applications and hardware supported across the various workgroups (Sofuoglu & Basoglu, 2008).

Technology Threat Avoidance Theory

With the continued technology deployment, there has been an increased concern for the security threat associated with managing security policy for devices and users (Cho & Ip, 2018). Applying technology threat avoidance theory to decisions can directly impact the decision to allow for BYOD and the criteria used in the overall enrollment and use process. Much like similar theories, this enables researchers to understand better why individuals decide to adopt BYOD and to what extent. There is a direct connection between security policy, user adoption, and the use of a corporate BYOD policy (Alaskar & Shen, 2016). Establishing risk acceptance clarifies how technology will either be accepted or avoided based on user intentions (Butler & Gray, 2006). Not only does the risk need to be set for each application, but it must also be selected based on individual users and their access levels.

Bring Your Own Device Options

With the need to provide remote access in real-time, BYOD programs have expanded and taken on many forms (Evans, 2013; Stephenson, 2014). While many options are available for providing this type of connectivity, several factors are considered when deciding what to select

(Ghosh, Gajar, & Rai, 2013). Cost is one factor that is important with a device management solution, and it can vary greatly, in some cases resulting in higher prices than a traditional corporate-provided solution (Brandel, 2012).

Supporting data can help the organization evaluate the solution options to meet their needs and user requirements (Redman, Girard, & Wallin, 2011). Much like all things related to technology, it is essential to evaluate needs continuously, even after the solution is selected and implemented (Disterer & Kleiner, 2013). Goedert (2013) provided insight into the evolution of BYOD and the importance of understanding the device capabilities and the business requirements. This will increase the likelihood that both objectives are met and continuous support requirements are maintained (Weeger et al., 2018).

Technology Benefits

In support of work tasks completed using technology, organizations provide devices to employees configured to access secure corporate data when not on the corporate network (Munroe, 2013). As individual technology capabilities have advanced, including the ubiquity of smartphones and tablets, many organizations no longer provide employees and contractors with devices but instead allow them to select what they prefer to use (Thomson, 2012). As part of the individual requirements for technology, there has been an equal need to migrate to a personal device-supported environment. This shift requires users to agree with the approach and accept providing the hardware needed.

The success of this new approach has had varying results globally (Bartis & Mitev, 2008). In addition to the individual job function criterion, there is a need to measure success against criteria such as happiness, productivity, and increased collaboration (Wang et al., 2017). Swanepoel (2015) provided feedback on how organizations are required to provide the mechanism for allowing employees to perform their work regardless of whether it involves a personal or corporate device. Giving an employee the ability to utilize personal devices can impact overall job performance and alter the financial obligation (Devaraj & Kohli, 2003).

Knowing that there is a certain level of dependence on information systems within an organization and the underlying applications and infrastructure, a new option for organizations has come to market in the form of cloud computing (Butler & Gray, 2006). The introduction and expansion of cloud computing, user access capabilities, and application hosting has provided alternative methods for organizations to give necessary system access and, in some cases, disaster recovery (Battleson, West, Kim, Ramesh, & Robinson, 2016).

The user of cloud computing can provide an innovative way of enabling information systems access within an organization while managing the overall investment in infrastructure and supporting resources and adding varying layers of reliability and flexibility (Gangwar, 2017). The flexible architectural design capabilities for cloud computing improve functionality and, in many cases, offer multiple access ports and locations that house the applications and critical data that organizational processes utilize (Leonardi, 2013).

With the growing demand and reliance on cloud computing, or software as a service (Munroe, 2013), there must be an understanding that this environment is also prone to failures, resulting in a potential impact. As a result of the potential for failure, cloud architects need to build measures to protect from data and user access loss. The potential impact of cloud reliability is a widespread outage due to the overall design and unknown factors related to access port and data storage location (Loukis, Kyriakou, Pazalos, & Popa, 2017). The cloud design usually provides a working platform supporting several customers versus location-specific infrastructure that only impacts a single site (Yousif, 2018). Looking at the environment from the angle of Moosakhani, Mohammadi, and Modiriasari (2011), it is described as a virtual enterprise that is enabled with the collaboration of many companies, reducing the potential risks of system and data loss. Cloud computing allows individuals to perform work tasks in a manner similar to using on-premise solutions but introduces an alternate foundation for leveraging the internet versus local infrastructure (Lu & Ramamurthy, 2011). Cloud computing can also be described as virtual computing, leveraging on-premise platforms provided by the organization's information technology teams (Gangwar, 2017). This form of cloud computing does not have to rely on an outside organization or infrastructure, changing the risk profile.

Each solution provides benefits and challenges from the system and information technology support aspects (Ragowsky, Ahituv, & Neumann, 1996). As a result of the on-premise solutions requiring a company to have a physical location to house equipment, there are increased costs and requirements from a support perspective. The benefit of the on-premise solution is the ownership and ability to control many things surrounding the overall environment and experience (Battleson et al., 2016). Cloud services provide the opportunity for additional reliability, but the lack of control, dynamic costing, and potential technology limitations may not always be quickly resolved.

User Impact

Connecting anytime and anywhere provides the opportunity to increase a work–life balance and the flexibility to perform work tasks regardless of location (Waterfill & Dilworth, 2014). This flexibility comes with some restrictions as privacy policies vary but often provide some limits on what rights an employee has when using a personal device for company use (Smith, 2017). While there has been much support of the benefits of using a personal device to access data, several implications exist that can positively or negatively impact the individual

(McInerney, 1999). One of the impacts is the device owner's privacy limitations regarding restricting access from the sponsoring organization (Weeger et al., 2015).

One of the critical factors for individuals is the desire to limit the number of devices carried. This desire can influence users and set aside some of the concerns of mixing personal and business on their devices (Disterer & Kleiner, 2013). As part of the individual device use, specific requirements are placed on the employee by the sponsoring organization, in many cases resulting in installing a mobile device management application that allows for limited or expanded management by the organization (Hovav & Putri, 2016).

Organizational Responsibility

Ludwig (2018) pointed out the many vital factors that must be considered when deciding what an organization selects as its approach. One of the motivations for BYOD approach selection is the perceived expectation that costs will be lowered for an organization, which is not always the case (Brandel, 2012). Along with the cost savings expectation of internal teams, there is an expectation that allowing employees to select their devices of choice will provide some level of engagement, resulting in increased productivity and a potentially positive impact on morale (Wang et al., 2017). The device selection freedom is evident when working with a group of individuals who cannot agree to a single type of device or operating system (A. S. Bharadwaj, 2000).

As part of the evaluation process, multiple areas, including legal requirements, are engaged to determine implications for introducing the BYOD program (Stephenson, 2016). With the introduction of company data on personal devices, specific legal requirements can vary depending on the organization and industry (Dhingra, 2016). The legal requirements can relate to device confiscation, data protection, and how the information is retrieved from a personal device (Eslahi et al., 2014).

There are many options available to an organization as it decides whether to offer a BYOD program (Mukherji, 2002). These options influence whether employees will elect to adopt the use, resulting in a valued investment (A. Bharadwaj, Keil, & Mähring, 2009). The adoption focus is placed on the individual regarding how the overall organization is impacted. With BYOD taking on many different forms and affecting several types of hardware and applications, it is undoubtedly refined based on individual requirements.

Literature Review Summary

The extant literature has provided a solid foundation for understanding the BYOD environments' adoption and implementation across the enterprise. Also, specific information has been provided to identify the security concerns that may impact an organizational decision to deploy this technology and how individuals will apply it when deciding to adopt the technology program (Beckett, 2014). One thing exact in the literature is the evolving strategy around using personal devices in the professional environment. The technology has evolved in many ways in an effort to provide core functionality while offering necessary protection (Mukherji, 2002). One item that needs further investigation is the defined cost of deploying both a corporate device and a personal device program. While there are anticipated variances between both examples, it is unclear which would provide a more cost-effective solution while maintaining adequate functionality and security.

Eliminating the high upfront device costs is appealing to many, but that accounts for just one component in the cost structure. As pointed out, cloud computing offers up another option and challenge as organizations and individuals demand access to their data, regardless of the device type and location from which they work. The cloud model may alter the method that organizations use to offer up and store critical data. While cloud computing does not necessarily introduce a new technical solution for the individual, it allows organizations to access information through other methods. These methods present various data points related to security, data protection, and financial implications.

Methodology

Secondary Data Collection and Analysis

Data collected from 7,900 employees within a large midwestern regulated electric and natural gas utility organization were examined. Multiple secondary data sets available through existing company databases were utilized to capture the details necessary for this study. Two sources of secondary data were the employee database and the mobile device management platform. The secondary data were associated with employee records, enrollment details in the mobile device management tool, and financial reporting, demonstrating information related to employee compensation as part of their enrollment. The sample size was limited to those who have adopted BYOD or utilize a corporate device. To provide an opportunity for time series analysis, data were gathered from various points in time, both pre-legislation and post-legislation implementation in Illinois (i.e., the employer requirement to reimburse employees for business use of personal devices and home internet service). In other words, data from different years were utilized to show the change in security and financial policy and the correlation between penetration and activity levels. Employee data, mobile device management tools, and financial reporting were leveraged to compile the adoption and use measures. Details related to adoption, hardware type, and financial treatment were also gathered from the data sets. These specific details provided what was needed to perform a complete analysis of each factor's adoption effects.

Antecedent and Control Variables

The antecedent values were measured using employee information from human resource systems, mobile device management databases, and financial reporting systems. These measures showed the types of hardware, activity level, and overall level of adoption among employees. The intent was to show the policy's impact on employees' desire to opt-out entirely or accept a corporate device as an alternative.

Several control variables were used in the study. Age, gender, tenure, and job function were among the variables used to control and prevent any distortion of the collected results over time. One consideration is any modifications to a job function that would potentially impact the desire or requirement to use technology within the role. As the secondary data were gathered, any additional control variables were identified and documented.

Data Analysis Procedures

Time series analysis was utilized to analyze the data, with the information being categorized based on the employee database's output and the device management system over various points in time. This categorization allowed for the grouping of the user base into the following identifiers:

1. Corporate user: A user utilizing a corporate-provided device.
2. BYOD user: A user that is using a personal device to access corporate information.
3. Inactive user: A non-user who has downloaded and registered in the mobile device management application but has demonstrated limited or no documented use.

4. Active user: A user who has downloaded and registered in the mobile device management application and has a higher interaction rate.

For purposes of this analysis, an inactive user demonstrated system access three times per week or less. An increased interaction rate would be those that showed access four times or more per week.

As part of the analysis, a *t*-test was performed to demonstrate the significance of the relationship with other variables.

There was a need to combine financial and mobile device management systems data with the demonstrated use behaviors. As part of the data collection, a separate extraction was taken from the mobile device management system, which identified the user count and identified the level of user interaction within the environment. In addition, an extraction from the financial reporting system was performed, which identified the users receiving a financial incentive for using a personal device. As part of the data preparation process, the data were aggregated into a single format to support performing the analysis. The data being leveraged spanned several years, displaying the pre- and post-policy change timeframe.

Results

The following section provides the analysis and presentation of the results. This section begins time series data, including the forecasting data for the following 12-month period. This study was initiated to understand the antecedent impact of BYOD use within an organization. The dimensions performed using Statistical Package for the Social Sciences (SPSS) were analyzed in the various models.

The secondary data consisted of three years of user data, device management data, and financial incentive information. The data sets included specific information related to device type, operating system, and frequency of use. The inclusion of the data was restricted to those actively enrolled in BYOD or the corporate device program.

Time series analyses were performed using the SPSS software (IBM SPSS Statistics, Version 27.0). Time series analysis is a technique that provides the opportunity to compare multiple data sets that span over a period of time. Time series analysis helps researchers to better understand the impact of an event that has either a positive or negative effect on the independent variable. In this study, the intent was to determine the impact that various antecedents have on the level of use documented in the BYOD mobile device management tool. In addition to providing the details related to the level of relationship, the time series analysis can be used as a forecasting tool, which can prove valuable in making informed decisions on the overall success and potential impact in future periods. It is critical to evaluate the analysis results to look at the overall significance determined across the variables and the cross-variable correlations.

The impacts of the level of use among the active and inactive users of the BYOD program was first explored in order to establish the level of activity that each user has with the environment. The effect of activity level can vary based on user preference, security controls, or the desire not to be an active user (Rizzuto, 2011). The benefit of the time series activity view is the correlation opportunity that can be provided to connect it with points in time when changes may have been implemented. The time series analysis is shown in Figures 1 and 2. Figure 1 utilizes the BYOD count as the dependent variable and active and inactive user counts as the independent variables.

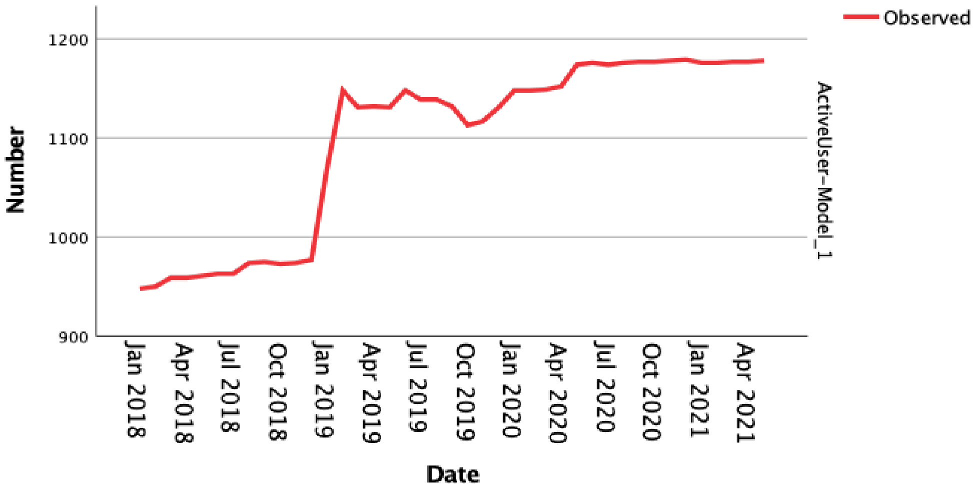


Figure 1. Level of use among active bring your own device users.

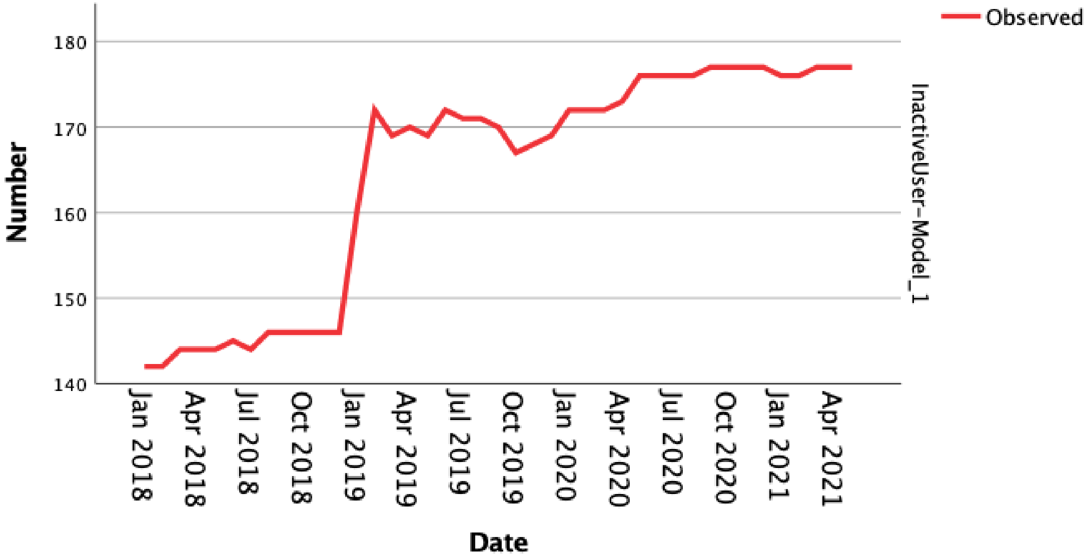


Figure 2. Level of use among inactive bring your own device users.

The results of the time series analysis showed no significant relationship among active users between being an enrolled BYOD user and the level of usage realized. However, the relationship is significant for the population, period of time, and BYOD enrollment status among inactive users.

Next, I conducted a time-series analysis with the financial incentive program as the independent variable. The dependent variable used across the analysis changed as both BYOD enrollment and corporate device enrollment were utilized. This was to aid in understanding if the inclusion of a financial incentive program impacts the adoption of the BYOD program and the corporate-provided device count. The time-series analysis is shown in Figures 3 and 4.

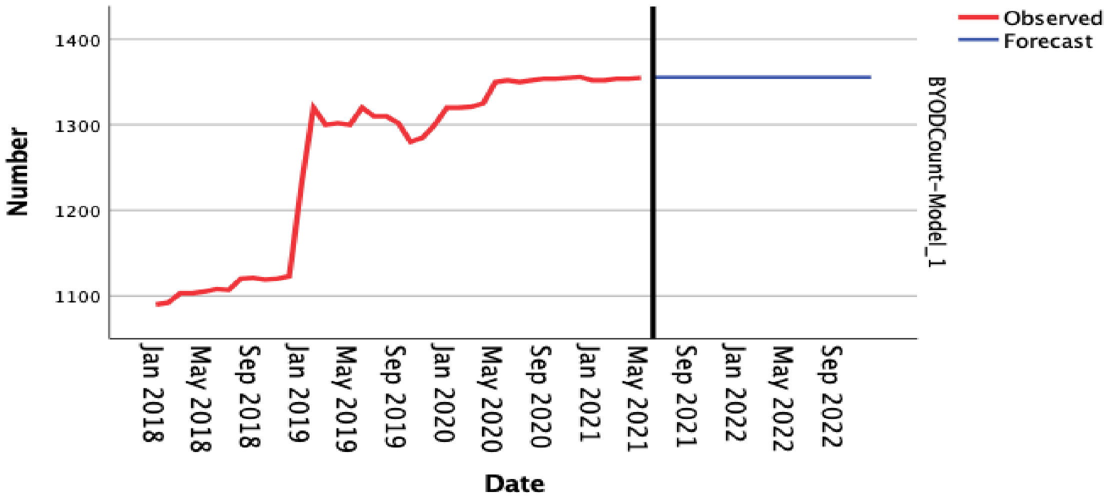


Figure 3. Bring your own device users and financial incentive.

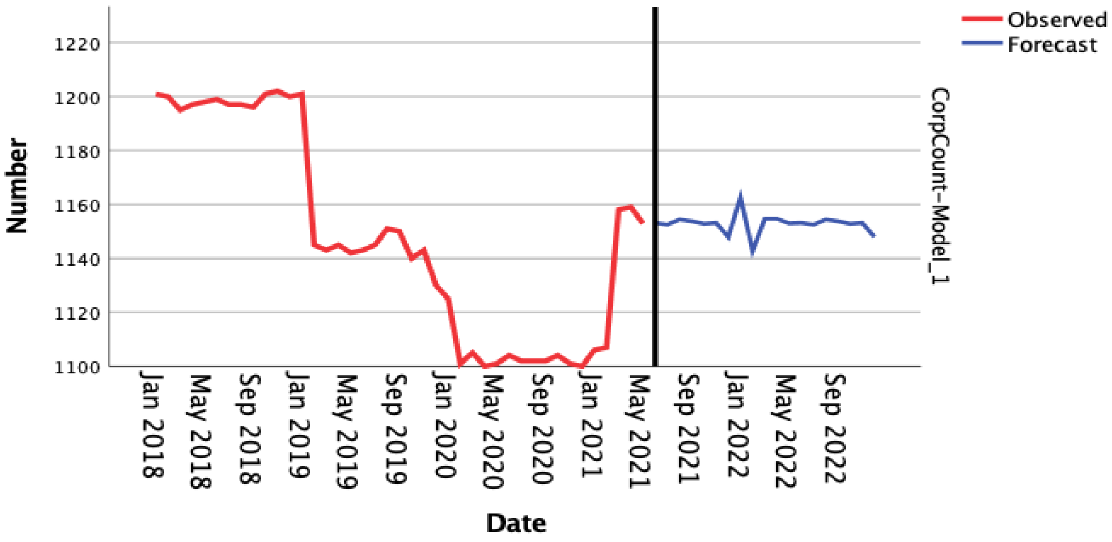


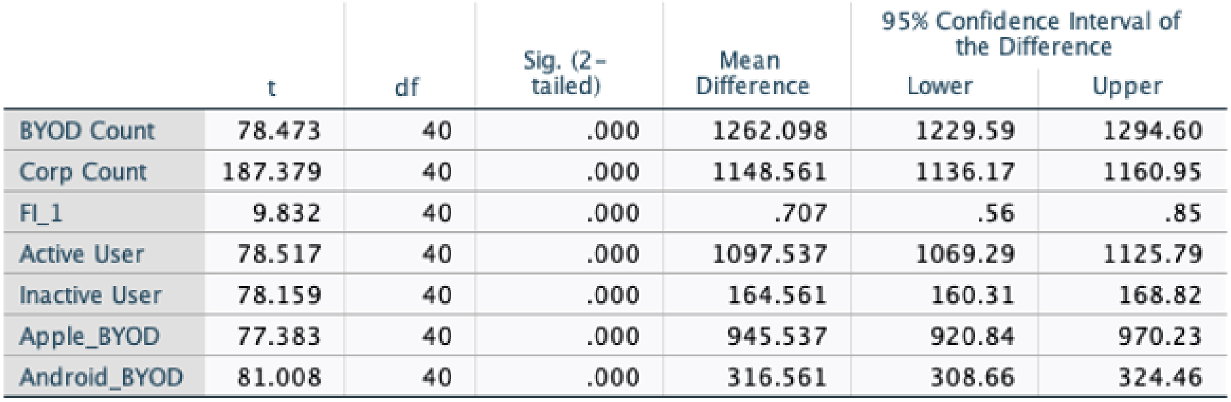
Figure 4. Corporate device and financial incentive.

Results show that neither BYOD enrollment nor corporate device enrollment has a significant relationship with financial incentives. Still, there was a visible shift in the overall count around the same time the mandatory financial incentive went into effect. In addition to showing the impact of the financial incentive offering, the forecasting model predicted that the enrollment level will remain pretty flat for the next 12-month period.

Figure 4 also provides a similar data point with a focus on the corporate data program. While there was a reduction in enrollment around the same time period, there was a visible increase in the enrollment numbers in May 2021 due to an increased deployment of company smartphones. Contributing factors to this change in value include the adoption of BYOD use cases introducing value and the decision to deploy smart devices to field employees. This population of employees previously carried basic phones with only calling and texting capabilities.

In addition to the time series analysis performed, I conducted a *t*-test including all the involved variables. This analysis intended to determine the level of relationship that device type, level of activity, and program enrollment have when comparing the time period average mean. Figure 5 depicts the output of the analysis performed.

Overall, the results demonstrate that there are contributing factors to the increase or decrease in BYOD enrollment. It is not clear whether the device type contributes to the type and level of use, primarily due to the corporate provided solution being configured to work the same regardless of device or operating system type.



	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
BYOD Count	78.473	40	.000	1262.098	1229.59	1294.60
Corp Count	187.379	40	.000	1148.561	1136.17	1160.95
FI_1	9.832	40	.000	.707	.56	.85
Active User	78.517	40	.000	1097.537	1069.29	1125.79
Inactive User	78.159	40	.000	164.561	160.31	168.82
Apple_BYOD	77.383	40	.000	945.537	920.84	970.23
Android_BYOD	81.008	40	.000	316.561	308.66	324.46

Figure 5. One-Sample Test

Table 1

Correlations of Variables

Variable	Active User	BYOD Count	Corp Count	Inactive User	Apple BYOD	Android BYOD
Active User	1.000					
BYOD Count	1.000	1.000				
Corp Count	-0.894	-0.893	1.000			
Inactive User	1.000	1.000	-0.891	1.000		
Apple BYOD	0.999	0.999	-0.895	0.999	1.000	
Android BYOD	0.992	0.992	-0.879	0.992	0.985	1.000

Discussion

In this study, I sought to understand how multiple variables may impact the general use of devices within an enterprise BYOD program. With many organizations developing programs and evaluating current programs, it is critical to establish value and relationships. The time-series analysis and the *t*-test analysis revealed interesting findings regarding the influences of independent variables on BYOD use. I discuss these findings in the following paragraphs.

The time-series analysis of BYOD use among active users did not yield significant results (p = .365). This may be because the level of use among BYOD users did not vary significantly over the time period captured. However, the time-series curve revealed that the level of use among active BYOD users increased from just below 1,000 to greater than 1,100 between January 2018 and April 2021. There was increased use of nearly 200 users in January 2019, representing a positive inflection point in BYOD adoption and use among employees. Since April 2020, which marked the beginning of the COVID pandemic, the adoption and use among active BYOD users has remained stable. This implies that the level of adoption and use has reached a saturation point. As previously noted, although the time-series tests were not statistically significant, there was a notable increase (January 2019) and then a saturation (April 2020 onwards) in BYOD use among active users during the time period studied.

The *t*-test provided the level of relationship between the various hardware types, level of BYOD usage, and the enrollment type of the device. This analysis demonstrates that while the hardware type does not have a significant relationship, the level of use as it relates to both corporate and BYOD device usage does have a varying level of significance.

Limitations of this Study

This particular study focused on secondary data within a single industry that has not had a history of providing the option of BYOD. Due to this limitation, the amount of data available to provide an expansive view of the overall impact of the antecedent factors was minimal. The available data did give an overview of how these factors impact the overall program enrollment and use. In addition, the application used to support the enrollment of personal devices is not well known in the industry and implementation may present some complications for companies. Having a more industry-known application that promotes access to corporate information in alternate ways may impact the results. Lastly, some of the information is not identified within the databases provided, and having direct interaction with users can increase the data points that are part of the evaluation.

Implications for Research

The results of this exploratory study have the potential to contribute to current research, specifically as it relates to the measurement of use in addition to adoption. Although the relationships lacked statistical significance, the graphs showed upward or downward trends. This implies that there are likely to be mediated relationships between the antecedent factors and the dependent variable. Therefore, to enhance current and future research, additional variables such as mediators or moderators can be considered that would establish additional relationships between user adoption and level of usage.

Findings from this study show that there has been increased usage over the last three years, but there has also been a trend upward towards increased adoption and widespread use. One additional variable to investigate is how the work-from-home policy, implemented two years ago, may have impacted the adoption rate. One factor that has and will only increase its impact on BYOD adoption is the hardware options available to consumers and the ease of use of the device management platform.

With the industry selected having limited history of supporting BYOD programs, it would also provide additional value to expand to other industries that have a variety of program types and lengths. Providing a continuance of the data stream has the capability of increasing data points associated with device type, level of use, operating system, and the control variables. In this regard, an interesting factor could be the number of current employees, grouped by union and non-union, currently not taking full advantage of the BYOD methods available to them.

Lastly, as COVID-19 pandemic conditions provide modifications to working conditions, potential new BYOD use cases and variables may appear that can be utilized in future research. This change in condition also has the potential of having the reverse effects that can also be captured in future research.

Implications for Practice

Many organizations have not made the decision to eliminate their corporate device programs. The rationale for such decisions could emanate from the need to maintain security and privacy within the organization. As major cybersecurity threats such as ransomware attacks are on the rise, it is imperative for companies to maintain their security posture. However, it is likely that BYOD programs will increase in popularity due to the ease of use and usefulness of the programs. Further, additional factors, such as hardware availability and preference, can also drive the adoption and use of such programs, creating potential limitations and opportunities.

This particular study only reviewed the current iOS and Android operating systems, not considering Windows or other operating systems. However, hardware components continue to evolve every day. New improvements are brought about in how devices function and operate in a particular environment. Therefore, as hardware vendors change the way devices work and the level of tasks that can be accomplished increases, there is a possibility that additional opportunities will be presented to change programs to incorporate such devices.

While this exploratory study contained financial incentive information related to government legislation, there may be other examples where employers provide voluntary incentives. Such incentives may drive the behaviors of employees to either adopt or ignore BYOD. Further, a shift in this type of policy is also likely to alter the results of this study as individuals may be more receptive to using personal technology if they are compensated.

Conclusion

Having a BYOD program has provided some benefits to organizations and individuals. The level of benefit will require some additional research and user interaction. As organizations evaluate the purpose and policies related to device usage, it is evident that supporting multiple types of hardware, having usable policies, and considering financial incentives can impact the overall success of the program.

While this exploratory study did not drive any specific hypotheses, it provides the foundation for outlining some future research that can increase program success. Adding additional data points will increase the value of the outcome. As noticed in the data used in this analysis, having individuals enrolled in a program does not suggest that they are being provided a suitable solution or that they are using the technology at the individual level. As organizations move through technology changes, such as more employees working remotely, having a high-level view of the user and organizational impact will help support the BYOD decisions made and will help with better forecasting the potential need.

References

Alaskar, M., & Shen, K. N. (2016). Understanding bring your own device (BYOD) and employee information security behaviors from a work-life domain perspective. In *AMCIS 2016 proceedings*. Retrieved from https://aisel.aisnet.org/

Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems*, *14*(2), 195–201. doi:10.48009/2_iis_2013_195-201

Bartis, E., & Mitev, N. (2008). A multiple narrative approach to information systems failure: A successful system that failed. *European Journal of Information Systems*, *17*(2), 112–124. doi:10.1057/ejis.2008.3

Battleson, D. A., West, B. C., Kim, J., Ramesh, B., & Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: An empirical investigation. *European Journal of Information Systems*, *25*(3), 209–230. doi:10.1057/ejis.2015.12

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, *18*(2), 66–79. doi:10.1016/j.jsis.2009.04.001

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, *24*(1), 169–196. doi:10.2307/3250983

Brandel, M. (2012). BYOD: Where the costs are. *Network World*, *29*(20), 16, 21. Retrieved from https://www.networkworld.com/

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly*, *30*(2), 211–224. doi:10.2307/25148728

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (bring your own device). *Competition Forum*, *10*(2), 117–121. Retrieved from http://iblog.iup.edu/americansocietyforcompetitiveness/competition-forum/

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659–673. doi:10.1080/17517575.2017.1404132

Devaraj, S., & Kohli, R. (2003). Performance impacts of information technology: Is actual usage the missing link? *Management Science*, *49*(3), 273–289. doi:10.1287/mnsc.49.3.273.12736

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science*, *78*, 179–184. doi:10.1016/j.procs.2016.02.030

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

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., & Saad, E. H. M. (2014). BYOD: Current state and security challenges. In *2014 IEEE Symposium on Computer Applications and Industrial Electronics*, (pp. 189–192). doi:10.1109/ISCAIE.2014.7010235

Evans, D. (2013, August 23). *What is BYOD, and why is it important?* Retrieved from https://www.ware247.co.uk/Content/CMS/Files/What%20is%20BYOD.pdf

Gangwar, H. (2017). Cloud computing usage and its effect on organizational performance. *Human Systems Management*, *36*(1), 13–26. doi:10.3233/HSM-171625

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62–70. Retrieved from https://www.rroij.com/global-research-in-computer-science.php

Goedert, J. (2013). Mobile device management software: The answer to BYOD? *Health Data Management*, *21*(2), 32, 34, 36, 38, 40. Retrieved from https://www.healthdatamanagement.com/

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49. doi:10.1016/j.pmcj.2016.06.007

Lee, J., Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of monitoring mechanisms on bring your own device adoption. *The Journal of Computer Information Systems*, *57*(4), 309–318. doi:10.1080/08874417.2016.1184032

Leonardi, P. M. (2013). When does technology use enable network change in organizations? A comparative study of feature use and shared affordances. *MIS Quarterly*, *37*(3), 749–775. doi:10.25300/misq/2013/37.3.04

Loukis, E., Kyriakou, N., Pazalos, K., & Popa, S. (2017). Inter-organizational innovation and cloud computing. *Electronic Commerce Research*, *17*(3), 379–401. doi:10.1007/s10660-016-9239-2

Lu, Y., & Ramamurthy, K. (2011). Understanding the link between information technology capability and organizational agility: An empirical examination. *MIS Quarterly*, *35*(4), 931–954. doi:10.2307/41409967

Ludwig, S. E. (2018, January 11). Why organizations should still care about BYOD. *Security*, *55*(1), 26–27, 31. Retrieved from https://www.securitymagazine.com/

McInerney, C. R. (1999). Working in the virtual office: Providing information and knowledge to remote workers. *Library & Information Science Research*, *21*(1), 69–89. doi:10.1016/S0740-8188(99)80006-1

Moosakhani, M., Mohammadi, S., & Modiriasari, M. (2011). Critical success factor in IT project risk management in virtual enterprise: Multi case study. *Journal of Information Technology Management*, *3*(6). Retrieved from https://jitm.ut.ac.ir/

Mukherji, A. (2002). The evolution of information systems: Their impact on organizations and structures. *Management Decision*, *40*(5/6), 497–507. Retrieved from doi:10.1108/00251740210430498

Munroe, F. (2013). Technological transformation—Implications for compliance from big data to BYOD. *Journal of Health Care Compliance*, *15*(6), 41–46. Retrieved from https://lrus.wolterskluwer.com/store/product/journal-of-health-care-compliance/

Ozigbo, N. C. (2013). Impact of organizational culture and technology on firm performance in the service sector. *Communications of the IIMA*, *13*(1), 69–81. Retrieved from https://iima.org/wp/ciima/

Ragowsky, A., Ahituv, N., & Neumann, S. (1996). Identifying the value and importance of an information system application. *Information & Management*, *31*(2), 89–102. doi:10.1016/S0378-7206(96)01072-5

Ragowsky, A., Licker, P. S., & Gefen, D. (2012). Organizational IT maturity (OITM): A measure of organizational readiness and effectiveness to obtain value from its information technology. *Information Systems Management*, *29*(2), 148–160. doi:10.1080/10580530.2012.662104

Redman, P., Girard, J., & Wallin, L.-O. (2011, April 13). *Magic quadrant for mobile device management software* [Report ID G00211101]. Retrieved from https://www.gartner.com/en/documents/1632331/magic-quadrant-for-mobile-device-management-software

Rizzuto, T. E. (2011). Age and technology innovation in the workplace: Does work context matter? *Computers in Human Behavior*, *27*(5), 1612–1620. doi:10.1016/j.chb.2011.01.011

Santhanam, R., & Hartono, E. (2003). Issues in linking information technology capability to firm performance. *MIS Quarterly*, *27*(1), 125–153. doi:10.2307/30036521

Schmidt, J. (2012). Not your parents' workplace anymore—Managing the new security realities of BYOD. *Security*, *49*(9), 25. Retrieved from https://www.securitymagazine.com/

Smith, W. P. (2017). Can we borrow your phone? Employee privacy in the BYOD era. *Journal of Information, Communication & Ethics in Society*, *15*(4), 397–411. doi:10.1108/JICES-09-2015-0027

Sofuoglu, E., & Basoglu, N. (2008). Exploring the characteristics and impact of information technology crisis on a company. In D. F. Kocaoglu, T. R. Anderson, & T. U. Daim (Eds.), *PICMET '08 - 2008 Portland International Conference on Management of Engineering & Technology* (pp. 811–817). doi:10.1109/PICMET.2008.4599689

Stephenson, P. (2014). Mobile device management. *SC Magazine*, *25*(7/8), 36–37. Retrieved from https://www.scmagazine.com/

Stephenson, P. (2016). Mobile device management. *SC Magazine*, *27*(7/8), 42–43. Retrieved from https://www.scmagazine.com/

Swanepoel, R. (2015, June). BYOD: Are You Missing the Boat? *Accountancy SA*, 32–33. Retrieved from https://www.accountancysa.org.za/

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2), 5–8. doi:10.1016/S1353-4858(12)70013-2

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. doi:10.2307/30036540

Violino, B. (2012). The BYOD security challenge: The growing variety of new devices makes supporting and controlling access to systems and data much more challenging for IT. *Insurance Networking News*, *15*(8), 29.

Wang, X., Weeger, A., & Gewald, H. (2017). Factors driving employee participation in corporate BYOD programs: A cross-national comparison from the perspective of future employees. *Australasian Journal of Information Systems*, *21*, 1–22. doi:10.3127/ajis.v21i0.1488

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal*, *40*(2), 26–36. Retrieved from https://lrus.wolterskluwer.com/store/product/employee-relations-law-journal/

Weeger, A., Wang, X., & Gewald, H. (2015). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems, 56*(1), 1–10. https://doi.org/10.1080/08874417.2015.11645795

Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., Grant, G., & Pittayachawan, S. (2018). Determinants of intention to participate in corporate BYOD-programs: The case of digital natives. *Information Systems Frontiers*, *22,* 203–219. doi:10.1007/s10796-018-9857-4

Yousif, M. (2018). Cloud computing reliability—Failure is an option. *IEEE Cloud Computing*, *5*(3), 4–5. doi:10.1109/MCC.2018.032591610

Zhang, N., Guo, X., Wang, F., Chen, G., & Wei, Q. (2011). Task-technology fit in mobile work: Exploring the links between task attributes and technology characteristics. In *2011 10th International Conference on Mobile Business* (pp. 268–274). doi:10.1109/ICMB.2011.47

CHAPTER 3: BRING YOUR OWN DEVICE ADAPTATION: THE ANTECEDENTS INFLUENCING INDIVIDUAL ADAPTATION TO TECHNOLOGY CAPABILITIES

ABSTRACT

Increasingly, information technology has become a primary tool for many employees' work-related activities. Many organizations are required to decide whether to invest in a corporate-owned platform or permit employee-owned devices for work purposes in the workplace. Recent years have seen many organizations adopting the bring your own device (BYOD) model, wherein employees can utilize their own devices to access corporate data and systems. Organizational adoption of BYOD notwithstanding, what factors drive an individual employee to adopt BYOD in an organization? This research question requires careful examination but has not gained significant research attention.

The adaptive structuration theory was applied to address this research question and develop a framework of the antecedents of BYOD adaptation and use in an organization. Security, privacy, data ownership, and financial factors are posited to have a significant impact on the task and technology adaptation of BYOD systems. Further, BYOD adaptation (task, technology) is posited to have a positive influence on BYOD use. To test the research model, this dissertation used a primary survey from 2,958 employees of an organization, with analysis using partial least squares and structural equation modeling techniques. Findings support the positive and significant relationship among many of the antecedent factors and mediating variables. In addition, findings from the study have academic relevance, as they can inform the understanding of the applicability of adaptive structuration theroy to the context of BYOD adaptation and use. Further, from a practical standpoint, this study provides better understanding of the why and how, specifically in relation to implementing and participating in a BYOD program. Specifically, while the antecedents had varying significant effects on overall BYOD use, it is evident that the mediating factors related to adaptive structuration theory had significant effects throughout the findings.

Keywords: BYOD use, Task adaptation, Technology adaptation, Security controls, Data ownership, Financial incentives, Privacy controls.

Chapter 3: Bring Your Own Device Adaptation: The Antecedents Influencing Individual Adaptation to Technology Capabilities

With the individual and organizational push for efficiency and advanced technology of choice, BYOD programs have expanded to enterprises of all sizes. These programs can provide an augmented approach to equipping employees, or in some cases, there is a single approach to support the overall needs and strategy (Beckett, 2014). While many factors can determine the outcome of any technology-driven environment, there are several key factors that must be evaluated to better understand the overall BYOD initial decision-making and success criteria (Swanson & Ramiller, 1997). Prior research has provided a level of detail that allows for a better understanding related to overall program and technology adoption (Disterer & Kleiner, 2013). With adoption being a key factor measuring overall strategy success, there is an opportunity to investigate the overall use or effectiveness of the BYOD program. This success measurement will assist in establishing the value of implementing such a program (Brandel, 2012).

In addition to understanding the level of adoption and usage at the individual level, there is tremendous value in identifying any alterations that individuals make to their normal usage techniques bases on controls or limitations placed on a device by a given organization. Also, there is the potential for individual adaptation based on technology advancement and consumer awareness (Disterer & Kleiner, 2013). As individuals become familiar with their technology landscape, there is the possibility that new methods are discovered, resulting in the potential for either a positive or negative impact on the workgroup and organization (Huang, Wu, Lu, & Lin, 2016).

With technology integrations, there is a need to ensure adequate security measures are in place to support both the security of the data and enhanced capabilities for the individuals expected to leverage the investment (Swanson & Ramiller, 1997). It is necessary to have an initial understanding of the requirements and an ongoing review of any restrictions needed to support advances in technology, task adaption needs, and user data needs. Understanding which factors are driving behaviors provides some additional context, allowing organizations to make decisions supporting aspects of any solution (Orlikowski, 1992).

Due to the financial structure in the utility industry, additional focus is placed on that key factor. While technology advancements and data protection offer up an argument within themselves, the utility industry is driven by the financial treatment of investments. Understanding how the decisions impact the capabilities will likely have an impact on various aspects of use. Aligning investment value with technology value demonstrates a consolidated view that will assist in defining the decision criteria used at the various levels within an organization (Davis, 1989).

Literature Review

Theory Overview

Traditionally, organizations provided devices configured to access secure corporate data when not on the corporate network. With the advancement of smartphones and tablets, many organizations are no longer providing employees and contractors with devices but rather allowing them to select what they prefer to use (Thomson, 2012). While companies may decide to migrate to a personal device-supported environment, it requires the support of the employees who must agree with the approach.

It has been shown that globally this bring your own device approach is widely supported with various levels of success. It has been measured against criteria such as happiness, productivity, and increased collaboration. Swanepoel (2015) provided feedback on how organizations are required to provide the mechanism for allowing employees to perform their work regardless of whether it involves a personal or corporate device. Giving employees the ability to utilize their own devices can impact overall job performance and alter the financial obligation across the organization (K. Schmitz, Webb, & Teng, 2010).

There is a certain level of dependence on information systems within an organization and the underlying applications and infrastructure; a new option for organizations has come to market over the last few years to address this dependence (Venkatesh et al., 2012). The evolution of cloud computing has provided alternative methods, such as BYOD systems, for organizations when looking at providing access to critical applications and, in some cases, disaster recovery (Battleson, West, Kim, Ramesh, & Robinson, 2016). Utilizing cloud computing for BYOD can provide an innovative way of enabling information system functionality within an organization while reducing the investment in infrastructure and supporting resources and adding varying layers of reliability and flexibility (Gangwar, 2017). Depending on the architectural design for the cloud computing functionality, there are often multiple access ports and locations that house the applications and critical data that organizational processes utilize. This provides opportunities for employees to use their own devices (BYOD) at home or in organizational settings.

With the growing demand and reliance on cloud computing, or software as a service (Munroe, 2013), there has to be an understanding that this environment is also prone to failure, resulting in a potential impact. Cloud architects need to build measures to protect against these potential failures. The potential impact of cloud reliability can be a widespread outage due to the overall design; the cloud design usually covers several customers versus a location-specific infrastructure that would only impact a single location (Yousif, 2018). Moosakhani, Mohammadi, and Modiriasari (2011) described the environment as a virtual enterprise that is enabled with the collaboration of many companies, lowering the potential risks. Cloud computing and BYOD allow individuals to interact with systems in similar ways as on-premise solutions but create a new foundation for leveraging the internet versus local infrastructure. This setup does not have to rely on an outside organization or infrastructure that is not owned by the organization in need, changing the risk profile.

Both cloud computing and on-premise solutions provide benefits and hindrances in terms of system and support (Ragowsky, Ahituv, & Neumann, 1996). As a result of the on-premise solutions requiring a company location to house equipment, there are increased costs and additional requirements from a support perspective. The benefit of the on-premise solution is the ownership and ability to control many things surrounding the overall environment and experience. Cloud services and BYOD provide the opportunity for additional reliability, but the lack of control, dynamic costing, and potential technology limitations are disadvantages that may not always be quickly resolved.

A review of the existing literature on BYOD use and its antecedents is provided in this section. The adaptive structuration theory (AST) is described in detail, and prior work is identified on individual behavior or decisions that can have an impact on the success or failure of this technology platform. Existing research on the antecedent factors affecting individual BYOD use in organizations is also identified.

Adaptive Structuration Theory

As a framework, AST assists in explaining how specific factors can provide for the need to adapt the completion of a task or how to use a certain component of technology to complete a task (K. W. Schmitz, Teng, & Webb, 2016). Information and technology within an organization play a key role in bridging the gap among processes. Finding the common point where technology can be used to collect, analyze, and use the data is critical (DeSanctis & Poole, 1994). K. W. Schmitz, Teng, and Webb (2016) adjusted the overall theory to establish some boundaries for the individual user. When looking at the impact of BYOD in the enterprise, there is great value in applying this theory at the individual level and understanding how it provides a benefit or hindrance to the overall success criteria.

As BYOD has increased in popularity, new constructs have been introduced that provide support for the need to adapt both process and technology to accomplish tasks, regardless of the age of the task or process (Orlikowski, 2000). Advancements in technology have not kept the same pace as many enterprise information systems, resulting in the need to implement modifications to the various components within existing processes; these modifications can come in the form of altered processes or altered technology to allow for increased efficiency and, in some cases, overall success (Mcguckin, Streitwieser, & Doms, 1998).

The framework of AST establishes an additional level of detail needed to determine where antecedent factors and technology intersect, resulting in a change to either the process or the technology used. In addition, understanding where the modifications take place assists with the detailing of process modifications that impact others across the organization.

Antecedent Factors of Bring Your Own Device Use

Device options. With the expanding footprint of many organizations and the need to provide remote access in real-time, the expansion of BYOD programs has expanded and taken on many forms (Evans, 2013; Stephenson, 2014). While there are many options available for providing this type of connectivity, similar factors are considered when deciding what to select (Ghosh, Gajar, & Rai, 2013). Cost is one such factor that is important with a device management solution, and it can vary greatly, in some cases resulting in higher prices than a traditional corporate solution (Brandel, 2012).

There are several avenues with supporting data to assist an organization in evaluating a solution to meet their needs (Redman, Girard, & Wallin, 2011). Much like all things related to technology, it is essential to continuously evaluate organizational needs, even after the solution is selected and implemented (Huang et al., 2016). Goedert (2013) provided an insight into the evolution of BYOD and the importance of understanding the device capabilities along with the business requirements. This will increase the likelihood that both objectives are met and continuous support requirements are maintained.

Security and privacy controls. With advancements in technology comes the need to investigate and invest in adequate security controls to ensure both the organization and individual are protected (Eslahi, Naseri, Hashim, Tahir, & Saad, 2014). Organizations tend to focus on restricting access to environments and protection of data that could introduce troublesome conditions if misused. Individuals view things from various perspectives, including the use of their personal devices and the desire to be able to perform tasks as efficiently as possible. Bringing these two components together has been the focus for several years and will likely continue to be a focus as both technology and organizations shift to the changing conditions (Cragg & Zinatelli, 1995). Beckett (2014) provided context that explains the popularity of introducing additional BYOD capabilities within an organization and the problems that can be introduced at the same time. Balancing the factors for a favorable decision is what organizations are faced with today (Violino, 2012). Establishing a risk matrix can help determine what will be acceptable processes and also which controls should be focused on without limiting the capabilities of both the device and employee (Scarfo, 2012).

Financial incentives. One of the key drivers to organizations making the shift to BYOD is the potential cost savings experienced through the reduced hardware and service plans requirements (Brandel, 2012). The hardware and service plan costs represent hard cost savings; capturing the soft cost savings or increased costs needs to be evaluated as part of the decision-making process that organizations face (Ragowsky et al., 1996). Aside from the technology demand that is placed on organizations, there is a need to define where the cost for supporting the necessary access will be absorbed. In some cases, the organization provides subsidies to employees, while in other cases, the employees are responsible for all costs associated with the device and service plan. This factor has the potential for being highly influential on the overall success or failure of the BYOD program. In some cases, local government legislation has taken on the responsibility for making this decision; in most cases, it is left up to the employer to decide.

Literature Review Summary

In sum, prior research has shown that BYOD use can be impacted by hardware options, security implications, and financial impact. Organizations tend to adopt BYOD due to employees' desire to use the device of choice, the ability to control the security of the data, and financial treatment factors, and factors such as data privacy, hardware support options, and financial obligations predict the success or failure of BYOD adoption. Prior research also has shown that AST provides a strong theoretical foundation for understanding adoption in these contexts (K. Schmitz et al., n.d.). Research on AST has delved into the overall use of technology to both support processes as well as use available data to perform business functions. Findings have revealed that while technology has played a role in the overall business functions, there is a desire to adapt both technology and process to the changing technology capabilities and also to the potential restrictions that organizations place on devices with the intent of supporting security and privacy needs (K. W. Schmitz et al., 2016).

Therefore, prior literature and AST have highlighted the need as well as the opportunity to adapt to BYOD capabilities while adjusting tasks based on both comforts with BYOD technology and the limitations. A critical research gap is to understand why and how individuals elect to adopt and use BYOD technology. In addition, a key question is also what process drives the intent to alter work processes based on BYOD technology in the post-adoptive context? Previous studies have focused on individuals or organizations at a broad level, limiting the capabilities of providing an in-depth understanding of the demonstrated outcomes. To add to the current findings, a deep dive into a specific organization or industry will provide context for the decisions made around technology as well as an understanding of the how and why behind BYOD use by the individuals within the organization.

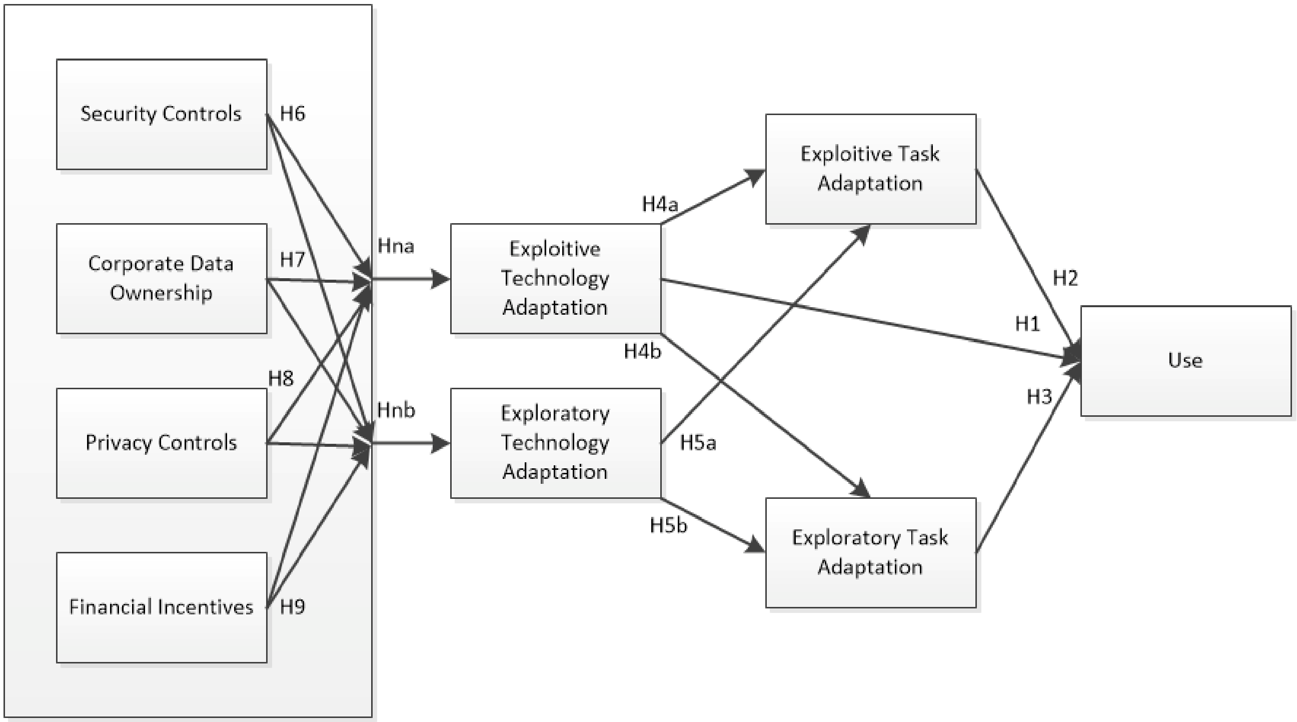

Security Controls
Corporate Data Ownership
Privacy Controls
Financial Incentives
H6
H7
H8
H9
Hna
Hnb
Exploitive Technology Adaptation
Exploratory Technology Adaptation
H4a
H4b
H5a
H5b
Exploitive Task Adaptation
Exploratory Task Adaptation
H1
H2
H3
Use

Figure 6. Research model

Research Model and Hypotheses Development

Figure 6 shows the adapted AST research model being used for this study (K. W. Schmitz et al., 2016). I posited that security controls, corporate data ownership, privacy controls, and financial incentives will have a positive impact on BYOD use through the mediating role of exploratory and exploitive technology and task adaptation.

Bring Your Own Device Use

BYOD use has been defined as the extent to which an employee uses the BYOD device(s) in their organization (Evans, 2013). In a time when employees prefer to use their own devices for accessing company data and performing work tasks, it is important to support a multitude of devices. As part of the growth of these programs, many device manufacturers have implemented steps in their process to provide efficiencies to companies (Cox, 2012). While the employee base may have a multitude of devices, there may be restrictions placed on which devices will be supported, resulting in an impact on the overall penetration and usage (Violino, 2012). In an environment that does not support the devices that are most used by the employee population, there may be limited desire for employees to participate in the enrollment and use of a BYOD program (Weeger, Wang, & Gewald, 2015).

Exploitive Technology Adaptation

Exploitive technology adaptation involves users personalizing the technology to fit their needs, customizing the capabilities to benefit the workgroup (K. W. Schmitz et al., 2016). Exploitative technology adaptation is present and demonstrated in multiple ways with existing technology solutions provided within the organization. In many cases, all employees are provided similar hardware and applications, but the understanding and willingness of each person to adapt to the features of the solution varies (Huang et al., 2016). As an example, BYOD allows everyone the opportunity to take a specific piece of hardware and customize it to meet their needs. While several individuals may have identical hardware, it is assumed that everyone will configure the device to their needs while still delivering on the assigned task (Jong & Hartog, 2010). This study hypothesizes that:

*H*1: Exploitive technology adaptation will be positively associated with BYOD use.

Exploitive Task Adaptation

Exploitive task adaptation occurs when individuals alter their normal task process without modifying the existing structure or processes (K. W. Schmitz et al., 2016). An example of this behavior is demonstrated when a user introduces an alternate method to complete a task (Stephenson, 2014). A field employee deciding to use a BYOD device as a hotspot to upload completed work while mobile versus waiting until returning to an office environment is an example of exploitative task adaptation. While the normal process of submitting work is followed, the introduction of a new task completion method creates an opportunity to impact the level of use. This study hypothesizes that:

H_2: Exploitive task adaptation will be positively associated with BYOD use.

Exploratory Task Adaptation

Exploratory task adaptation results from individuals attempting to transform their current task processes with the desire to create new objectives (K. W. Schmitz et al., 2016). This offers up an opportunity to create or introduce significant processes (Davis, 1989). The expectation is that the end state target remains the same despite any alteration of the steps taken to achieve the results. The utility industry has historically relied on several paper-driven processes to deliver work orders to the field employees. While there were no technology changes implemented, a slight modification was introduced into the process that altered the process of delivering the same paperwork via email to the crew. This example was driven by the need to establish efficiency without the ability to provide any additional technology solutions to the workgroup. In an environment driven by customer satisfaction and scheduling of costly labor, this adaptation resulted in positive results. This study hypothesizes that:

H_3: Exploratory task adaptation will be positively associated with BYOD use.

Exploratory Technology Adaptation

Exploratory technology adaptation results from the modification of technology solutions introducing new capabilities or features (K. W. Schmitz et al., 2016). This introduction of modified technology solutions can be influenced by the information technology device support structure within the organization. Whereas exploitive technology adaptation allows for similar outcomes, exploratory technology adaptation allows for the deviation from current processes (Christensen & Overdorf, 2000). It is expected that technical knowledge, along with an understanding of the organization, creates an opportunity to support the advancement of technology (Cragg & Zinatelli, 1995). There can be risk introduced with the introduction of untested technical solutions, but the opportunity to improve results generates interest to support this concept.

The outcome of exploratory technology adaptation can vary across industries and organizations. In the example of the utility industry, it is expected to have a positive outcome due to the established processes that today lack technology solutions but are easily altered. As a result of both positive and negative results possible, there is no hypothesized effect.

Task Adaptation Mediating Effects

Task adaptation is theorized to mediate the effect of technology adaptation on use. One can expect that as technology use changes, task processes are also modified to support the expected outcome. While tasks can be completed using various levels of technology, they do not necessarily support an expected use outcome (Orlikowski, 2000). The process knowledge level and technical capabilities of everyone involved will result in varying levels of understanding and desire to introduce modified methods. An organization may receive a benefit from the introduction of new technology; it cannot guarantee that the overall use will be impacted. Use is individual-driven based on the success of supporting tasks, in conjunction with the provided technology (K. W. Schmitz et al., 2016). The effects have an increased possibility of varying results based on the expected task outcome. This study hypothesizes that:

> H_4: The effect of exploitive technology adaptation will be mediated by (a) exploitive task adaptation and (b) exploratory task adaptation and is positively associated with BYOD use.

With the variations that can be present with exploratory technology adaptation, the possibility exists for wide variations compared to exploitive technology adaptation. In a situation where an individual is focused on the task process, limited technology modifications may be sought. As the opportunity for exploratory technology increases, there is a need to open the possibilities for modifying the tasks and processes to provide support. Without the combination of both, there is a limited possibility for a positive level of outcome. This study hypothesizes that:

> H_5: The effect of exploratory technology adaptation will be mediated by (a) exploitive task adaptation and (b) exploratory task adaptation and is positively associated with BYOD use.

Security Controls

Security controls are defined as the presence of a security policy that can either support or inhibit the ability of device users to access critical information, allowing for mobility and increased efficiencies (Dhingra, 2016). Prior research has shown that as the environment evolves across the business environment, there is a need to identify the particular organization's needs (Scarfo, 2012).

Whether a mobile technology solution is corporate- or personal device-focused, there is a need to have clear and adequate security policies that deliver the expected results (Cho & Ip, 2018). In the case of the expanding BYOD market, there have been policies put in place that both enable and restrict access to specific data sets and applications. The intent of providing these controls can have both positive and negative effects, depending on how policies are implemented (Eslahi et al., 2014). Having the proper balance allows for the security policy to support the usage and create opportunities to expand the capabilities to various devices and business needs (Violino, 2012). This study hypothesizes that:

H_{6a}: Security controls will be positively associated with exploitive technology adaptation.

Users consider many factors when deciding on BYOD participation, including security controls. With the desire to have access to necessary information, technology advancements and security controls will have an impact on both process and technology decisions (Cragg & Zinatelli, 1995). Specifically, the need to adjust to new technology as it is presented while still supporting old technology will be necessary. In addition, as more data becomes part of ongoing processes and various methods are used to access the data, it will be necessary to make modifications of the security controls currently in place (Violino, 2012). Users will be forced to expand their creativity to stay within the boundaries put in place to ensure a secure environment.

In support of the need to allow for flexibility, there must be a measured level of negotiation, with the established processes providing a foundation for decision-makers. In addition to the capabilities associated with the physical device and managing processes, all advancements in the addition of any associated physical security appliance implementation. This study hypothesizes that:

H_{6b}: Security controls will be positively associated with exploratory technology adaptation.

Corporate Data Ownership

In this study, corporate data ownership is defined as the extent to which sensitive data is protected within the organization. Prior research has shown that while providing remote access and flexibility to the employees, there is a need to ensure that sensitive data is protected (Morrow, 2012). In addition to the organization driving a policy that protects itself, there needs to be disclosure of the privacy rights that employees have when using their devices (Smith, 2017). In many cases, the device remains the ownership of the individual. Still, there are specific provisions to allow the sponsoring company the right to access the data on the device or the permission to confiscate it at any time (Smith, 2017). As a result, individuals who choose to accept the ownership and permission guidelines will increase their possibility of a positive experience.

With these types of policies in place, there will likely be those who accept and a base population that does not. Having a clear strategy will provide the foundational information needed to evaluate appropriate solutions and the methods with which the policies will be implemented and supported (Beckett, 2014). When looking at the arguments of data ownership and policy clarity, it is important to have a clear policy that will provide both the organization and the individual the details necessary to make an informed decision on adopting. Lacking or not disclosing this information can have a negative impact. As outlined, the security policies are necessary to enable and protect both the organization and the individual. This study hypothesizes that:

> H_{7a}: Corporate data ownership will be positively associated with exploitive technology adaptation.

With there being multiple methods for the proper storage of corporate data, the type of device and quantity of data will have an influence on what method can be used for storing data. Just a few short years ago, it was easy to believe that a USB portable storage device would be sufficient for storing and transferring data between devices or employees. As the data volumes have grown, and with the advancements in remote working, this type of device will no longer meet the need (Munroe, 2013). One of the challenges with users making the decision as to what methods will be used is related to employer rights to manage or have access to personal devices (Smith, 2017). As users continue to identify ways to manage their work location status and access information needed to perform functions, the balancing of need versus want may result in multiple modifications. This study hypothesizes that:

> H_{7b}: Corporate data ownership will be positively associated with exploratory technology adaptation.

Privacy Controls

Privacy controls are present on both corporate-owned devices and personal devices. At the same time, there can be a strong opinion among individuals who have concern regarding corporate control of their personal devices (Smith, 2017). As employees are asked to use personal devices to perform work functions, it is necessary to ensure that the mobile device management processes are used to provide clear details associated with how device privacy is maintained (Ghosh et al., 2013). Privacy control concerns can be explored from two viewpoints. First, as an employee, there is a concern with personal device monitoring or confiscation. Second, as an employer, there is a concern with personal device usage that can have an impact on data protection and the completion of company tasks with a personal device (Astani, Ready, & Tessema, 2013). In the event of an investigation or legal action, both the individual and the organization can be placed in an uncomfortable situation. Defining clear privacy controls will have a positive impact on the program and its use. This study hypothesizes that:

H_{8a}: Privacy controls will be positively associated with exploitive technology adaptation.

For many, there is a general concern regarding the use of personal data and lack of privacy when allowing organizations unregulated access to devices (Violino, 2012). The level of access provided will generate the desire to alter the device type or methodology used to access the necessary data. As organizations move to an environment that either pushes for more personal device use or employees insist on having capabilities to use their device of choice, privacy controls will continue as a consideration. This study hypothesizes that:

H_{8b}: Privacy controls will be positively associated with exploratory technology adaptation.

Financial Incentives

In this study, financial incentives are defined as the compensatory benefits offered to the employees for using BYOD devices. Prior research has shown that the device management environment varies with how organizations elect to provide employees with provisions to use their devices for their job functions (Grensing-Pophal, 2014). While policies vary across employers, there is likely a direct relationship between employee adoption and financial incentives. Compensation for use of a personal device for company tasks has been a topic of debate. As a result, there has been increasing discussion regarding whether the organization has an obligation to provide some financial reimbursement (Disterer & Kleiner, 2013). In many cases, the refusal of an organization to provide some level of compensation has impacted employee enrollment, which may drive up the corporate device count or inhibit productivity. This study hypothesizes that:

H_{9a}: Financial incentives will be positively associated with exploitive technology adaptation.

Financial incentives have an impact on both the organization and the individual. When viewing the incentives as purely a financial tool for the organization, it allows for the potential reduction of overhead costs of hardware while enabling employees to use their device of choice. When looking at the financial aspect from an employee perspective, it is expected in many cases that an incentive should be provided primarily because the use of a personal device saves the company and costs the individual money. Both involuntary and voluntary programs have varying outcomes (Brandel, 2012). If the decision is individual-driven, or voluntary, the likelihood of an increased level of motivation and acceptance is much greater. The willingness of an individual to invest in technology to perform work functions will require a financial commitment. This study hypothesizes that:

H_{9b}: Financial incentives will be positively associated with exploratory technology adaptation.

Methodology

Measures

Table 2 provides the scale measures used in this study. Adapted measures from prior works were modified for the context of BYOD adoption and use. New measures were created for some constructs and were validated using a pilot study. As part of the pilot study, the survey was distributed to 24 respondents who were also considered topic experts with full participation. Applicable feedback from the pilot group was incorporated into the final survey instrument. All measures use a scale from 1 to 7, (*Strongly Disagree* to *Strongly Agree*).

Table 2

Scale Measures

Construct	Scale Used (1–7, *Strongly Disagree* to *Strongly Agree*)
BYOD Use	Adapted from K. W. Schmitz et al. (2016)
Exploitive Technology Adaptation	Adapted from K. W. Schmitz et al. (2016)
Exploratory Technology Adaptation	Adapted from K. W. Schmitz et al. (2016)
Exploitive Task Adaptation	Adapted from K. W. Schmitz et al. (2016)
Exploratory Task Adaptation	Adapted from K. W. Schmitz et al. (2016)
Security Controls	New measures
Corporate Data Ownership	New measures
Privacy Controls	New measures
Financial Incentives	New measures

Data Analysis Procedures

This study utilized partial least squares and structural equation modeling (PLS-SEM) techniques to analyze the survey data. The process for PLS-SEM has significant advantages over traditional SEM techniques (Chin, Marcolin, & Newsted, 1998). For instance, PLS-SEM can be used to analyze small samples. It also provides flexibility in analyzing reflective scales, formative scales, and second-order factors and is well suited for exploratory analysis of constructs and relationships (Gefen, Straub, & Boudreau, 2000). Therefore, the use of PLS-SEM techniques is considered to be appropriate in this study. First, reliability and validity of constructs were established in PLS by verifying with established standards of factor loadings and average variance extracted (AVE) estimates, as well as verifying against the correlation across constructs (Fornell & Larker 1981; Nunnally, 1978). This was followed by the testing of the hypotheses using the structural model in PLS-SEM, following Ringle, Wende, and Becker (2015).

Upon completion of the survey and compiling of the responses, the data were categorized based on various components. Initially, splitting those who actively participate in BYOD versus nonparticipants provided a relevant picture of the level of penetration within the organization. The goal of analyzing the survey response details was to establish how both decision-makers and active business users utilize personal technology to complete core business functions. In addition to the base determination, a focus was then placed on how everyone is influenced by the antecedent factors and the resulting mediating effect on exploitive and exploratory technology adaptation. The combination of these various components established key metrics associated with potential impacts on the level of BYOD use within the organization. These impacts can assist in establishing success criteria and influence decision-making in the future as it relates to the investment in a corporate or BYOD environment.

Survey Response Analysis

To capture the details necessary for this proposal, I conducted an online survey in June 2021 using the Qualtrics platform. The survey was distributed to eligible employees within a regulated electric and natural gas utility company. Eligibility requirements were limited to:

- full-time employee status
- exempt employee status (salaried)
- 18 years of age

The survey was distributed to 2,958 eligible employees at various levels within the organization. Specifically, the survey was conducted with executive leadership, middle managers, supervisors, and front-line employees. In addition to the multiple levels, there was representation from all core business units: finance, executive, information technology, and electric and gas distribution.

Respondents were informed that the purpose of the survey was to assist in understanding the impact of BYOD within the organization and were provided an estimated time of completion of 10 minutes. Respondents were informed that the participation was strictly voluntary and that the results would be anonymous. In addition to the system access qualifications, the researcher could accept or reject work. Out of the 1,002 surveys completed, 61 were incomplete and removed from the analysis, resulting in 941 usable responses or a response rate of 31.8%.

Data Collection

The survey included 29 questions, which were broken out into four sections. Section 1 was comprised of the disclosure as well as the qualifications questions; Section 2 consisted of the questions related to BYOD use characteristics; Section 3 consisted of questions related to financial incentives; finally, Section 4 gathered demographics. The survey was adapted from previous literature (K. W. Schmitz et al., 2016). A pilot study and expert review were completed with peer industry specialists and academic experts to verify validity and reliability. Modifications were made to the survey based on feedback from participants before the full data collection.

Variable and Measurement Definitions

While there is a conceptual definition of each of the variables in the literature review, the operational definition follows. Some constructs were developed with a 7-point Likert scale adapted from K. W. Schmitz et al. (2016), while the antecedent measurements were newly developed questions related to the specific topic being addressed. The question development was directly associated with policy and process within the corporate environment. The survey instrument is located in Appendix A.

Use. The construct Use measures the individual level of personal device use in a BYOD program (five items; 1 = *Strongly disagree*, 7 = *Strongly agree).*

Adaptive structuration theory and mediating effects. K. W. Schmitz et al. (2016) provided a theoretical model to assist in understanding the mediating effects from the following dimensions.

Exploitive task adaptation. This measure addresses the level at which an individual user modifies work tasks without adjusting the process to fit his or her needs (five items; 1 = *Strongly disagree*, 7 = *Strongly agree).*

Exploitive technology adaptation. This measure addresses the level at which an individual user modifies technology to fit his or her needs (five items; 1 = *Strongly disagree,* 7 = *Strongly agree).*

Exploratory task adaptation. This measure addresses the level at which an individual user modifies work tasks with the intent of adjusting the process to fit his or her needs (five items; 1 = *Strongly disagree*, 7 = *Strongly agree).*

Exploratory technology adaptation. This measure addresses the level at which an individual user modifies personal technology with the intent of creating new capabilities to fit his or her needs (five items; 1 = *Strongly disagree,* 7 = *Strongly agree).*

Security controls. This construct measures the individual perception of security controls that may be applied to the use of personal technology within the organization (five items; 1= *Strongly disagree*, 7 = *Strongly agree).*

Data ownership. This construct measures the individual perception of how the distinction of personal versus company-owned data is present while using a personal device (five items; 1 = *Strongly disagree,* 7 = *Strongly agree).*

Privacy controls. This construct establishes the individual level of understanding of how privacy is maintained while using a personal device in the organization (five items; 1 = *Strongly disagree*, 7 = *Strongly agree).*

Financial incentive. This construct measures how the receiving, or not receiving, of a financial incentive impacts using a personal device within the organization (five items; 1 = *Strongly disagree*, 7 = *Strongly agree).*

Control Variables

Organization tenure and job function were controlled for the broad group of individual data utilized. Any modifications to a job function or work location changes that would potentially impact the desire or requirement to use technology within the role were considered.

Results

Measurement Model

The following section provides the analysis and presentation of the results. This section begins with the respondents' demographics, then proceeds into the reliability and factor analysis. This study was initiated to understand the antecedent impact of BYOD use within an organization. The analysis of the dimensions performed with Smart PLS is found in Model 1.

The data sample demographics for the participants who completed the study for the model are contained in Table 3. The demographics are followed by Table 4, which includes the outer loadings, *t*-values, and composite values. Any item indicator with < 0.7 was removed. All *t*-values were greater than 1.96, and the composite reliability on the individual constructs were all > 0.7, substantiating that the scale in the study is reliable. Construct validity was established by checking convergent and discriminant validity. Table 5 provides information on the item-to-item construct correlations. The item-to-construct correlations showed that the loadings on the constructs were higher than the cross-loadings on other constructs. Convergent validity was established as each measure of AVE was > 0.5. Discriminant validity was verified by comparing the construct correlations with the square root of AVE in Table 6. The diagonal elements in Table 6 represent the square root of AVE; those values are higher when compared to all the construct correlations in the corresponding columns. This established discriminant validity for the constructs.

Table 3

Sample Respondent Characteristics

Characteristic	Count	%
Age		
18–25	40	4%
26–30	37	4%
31–35	76	8%
36–40	95	10%
41–45	132	14%
46–50	123	13%
51–55	185	20%
56–60	160	17%
61–65	64	7%
> 65	10	1%
Unidentified	19	2%
Gender		
Male	630	67%
Female	311	33%
Level of Education		
Less than High School	0	0%
High School or GED	93	10%
Associate's Degree or Equivalent	119	13%
Bachelor's Degree	524	56%
Master's Degree	175	19%
Doctorate Degree	14	1%
Unidentified	16	2%
Years with Company		
< 1 year	34	4%
1–5 years	143	15%
6–10 years	162	17%
11–15 years	126	13%
16–20 years	137	15%
> 21 years	320	34%
Unidentified	19	2%

(continued)

(continued)

Characteristic	Count	%
Years in Profession		
< 1 year	32	3%
1–5 years	86	9%
6–10 years	124	13%
11–15 years	108	11%
16–20 years	125	13%
> 21 years	448	48%
Unidentified	18	2%
Position in Company		
Individual contributor	498	53%
Front line leader	198	21%
Middle manager	192	20%
Director or above	53	6%

Table 4

Constructs and Measures

Items	Indicators	Loadings	*t*-value
	Use (Composite Reliability = .969)		
USE_1	Using my personal device enables me to accomplish more work tasks.	0.930	159.033
USE_2	Using my personal device improves the quality of work I do.	0.905	115.601
USE_3	Using my personal device makes it easier to do my job.	0.935	131.879
USE_4	Using my personal device enhances my effectiveness on the job.	0.958	253.219
USE_5	Using my personal device gives me greater control over my work.	0.919	116.880
	Exploitive Technology Adaptation (ITECH; Composite Reliability = .944)		
ITECH_1	I have experimented with new features on my personal device, as they were intended to be used.	0.882	86.602
ITECH_2	I have changed the settings/preferences on my personal device to alter the way I interact with it.	0.867	58.745
ITECH_3	I have taken advantage of the adaptability of the features available on my personal device, as they were intended to be used.	0.929	154.382
ITECH_4	I have customized some features on my personal device, as they were intended to be used.	0.918	104.714

(continued)

Items	Indicators	Loadings	*t*-value
Exploratory Technology Adaptation (RTECH; Composite Reliability = .937)			
RTECH_1	I have developed a way of using my personal device, which deviates from how it is normally used.	0.871	62.792
RTECH_2	I have used at least one personal device feature or capability differently from how it is normally used.	0.927	111.460
RTECH_3	I have modified something on my personal device to use it differently from how it is normally used.	0.934	134.995
RTECH_4	I like to experiment with new features or capabilities on my personal device to deviate from how it is normally used.	0.815	48.234
Exploratory Task Adaptation (RTASK; Composite Reliability = .921)			
RTASK_1	I have tried to perform work-related tasks that were not possible without my current personal device.	0.752	36.428
RTASK_2	I strive to find ways to take on new work responsibilities by using my personal device.	0.854	72.645
RTASK_3	My current personal device has allowed me to frequently attempt new tasks I could not do in the past.	0.912	127.796
RTASK_4	Overall, use of my current personal device has enabled me to try new and different work-related tasks.	0.926	163.694

(continued)

Items	Indicators	Loadings	*t*-value
Exploitive Task Adaptation (ITASK; Composite Reliability = .921)			
ITASK_1	I try hard to figure out ways to do my existing work tasks better by using my current personal device.	0.896	112.036
ITASK_2	Using my personal device has forced me to find new ways of performing work tasks.	0.750	32.171
ITASK_3	I strive to find ways to do my existing work tasks faster with features on my current personal device.	0.919	160.860
ITASK_4	Overall, I am doing my best in taking advantage of various features of my current personal device to perform my existing tasks better.	0.879	91.770
Security Controls (SC; Composite Reliability = .869)			
SC_1	The corporate BYOD program security controls in my organization enable me to perform work tasks.	0.793	34.236
SC_2	The corporate BYOD program security controls installed on my personal device(s) provide a secure solution.	0.743	26.480
SC_3	The corporate BYOD program security controls have improved how I do my work tasks.	0.852	58.546
SC_4	I am using my personal device(s) more because of the corporate BYOD program security controls.	0.770	37.297

(continued)

Items	Indicators	Loadings	*t*-value
Corporate Data Ownership (CDO; Composite Reliability = 1.000)			
CDO_4	The current mobile device management application on my personal device enables me to protect data.	1.000	
Privacy Controls (PC; Composite Reliability = .931)			
PC_1	I am confident that my personal data remains private if enrolled in the corporate BYOD program.	0.906	83.077
PC_2	I understand the function the mobile device management application provides to protect data.	0.772	29.820
PC_3	Privacy controls in the corporate BYOD program enable me to work without any worry about my personal data.	0.910	74.377
PC_4	I have confidence that my personal data will be protected if enrolled in the corporate BYOD program.	0.916	89.318
Financial Incentives (FI; Composite Reliability = .941)			
FI_1	The financial incentive I receive for participating in the BYOD program is acceptable.	0.878	12.066
FI_2	I participate in the BYOD program because of the financial incentives.	0.890	16.357
FI_3	I have invested in personal devices to perform work tasks because of the financial incentives.	0.917	17.240
FI_4	Financial incentives are the best part of my organization's corporate BYOD program.	0.891	16.525

Table 5

Item-to-Item Correlations

	Corporate Data Ownership	Financial Incentives	Exploitive Task Adaptation	Exploitive Technology Adaptation	Privacy Controls	Exploratory Task Adaptation	Exploratory Technology Adaptation	Security Controls	Use
CDO_4	1.000	-0.052	0.284	0.284	0.432	0.198	0.020	0.415	0.303
FI_1	-0.029	0.878	-0.006	-0.071	0.032	-0.019	-0.041	0.044	-0.022
FI_2	-0.056	0.890	0.018	-0.054	-0.021	-0.013	0.019	0.006	-0.018
FI_3	-0.056	0.917	0.019	-0.057	-0.018	-0.004	0.025	0.020	-0.042
FI_4	-0.051	0.891	-0.020	-0.063	-0.010	-0.039	0.003	0.007	-0.022
I-Task_1	0.267	0.003	0.896	0.335	0.235	0.636	0.285	0.347	0.499
I-Task_2	0.159	-0.013	0.750	0.250	0.101	0.531	0.332	0.285	0.285
I-Task_3	0.264	0.014	0.919	0.394	0.176	0.665	0.345	0.324	0.515
I-Task_4	0.273	-0.007	0.879	0.416	0.203	0.614	0.251	0.332	0.517
I-Tech_1	0.252	-0.077	0.403	0.882	0.183	0.359	0.306	0.262	0.360
I-Tech_2	0.218	-0.062	0.293	0.867	0.135	0.266	0.337	0.205	0.260
I-Tech_3	0.282	-0.040	0.395	0.929	0.170	0.335	0.296	0.277	0.355
I-Tech_4	0.263	-0.073	0.369	0.918	0.135	0.307	0.321	0.221	0.312
PC_1	0.374	-0.013	0.188	0.149	0.906	0.151	-0.009	0.393	0.201
PC_2	0.368	0.019	0.183	0.222	0.772	0.155	0.001	0.323	0.165
PC_3	0.388	0.010	0.166	0.109	0.910	0.122	-0.060	0.405	0.191
PC_4	0.377	-0.025	0.199	0.112	0.916	0.158	-0.018	0.417	0.206
R-Task_1	0.128	-0.008	0.487	0.263	0.056	0.752	0.297	0.227	0.332
R-Task_2	0.172	0.001	0.638	0.312	0.208	0.854	0.346	0.339	0.408
R-Task_3	0.172	-0.025	0.627	0.305	0.155	0.912	0.317	0.329	0.448

(continued)

	Corporate Data Ownership	Financial Incentives	Exploitive Task Adaptation	Exploitive Technology Adaptation	Privacy Controls	Exploratory Task Adaptation	Exploratory Technology Adaptation	Security Controls	Use
R-Task_4	0.204	-0.043	0.684	0.343	0.151	0.926	0.343	0.329	0.480
R-Tech_1	-0.024	-0.003	0.278	0.265	-0.035	0.321	0.871	0.098	0.048
R-Tech_2	0.038	0.017	0.310	0.300	0.010	0.328	0.927	0.091	0.082
R-Tech_3	0.030	-0.007	0.329	0.334	-0.017	0.362	0.934	0.104	0.090
R-Tech_4	0.024	-0.013	0.309	0.334	-0.037	0.327	0.815	0.029	0.102
SC_1	0.391	0.016	0.259	0.188	0.348	0.206	-0.016	0.793	0.282
SC_2	0.522	0.006	0.273	0.251	0.436	0.189	-0.036	0.743	0.342
SC_3	0.260	-0.007	0.281	0.220	0.346	0.324	0.120	0.852	0.310
SC_4	0.211	0.051	0.348	0.202	0.281	0.365	0.165	0.770	0.274
USE_1	0.297	-0.033	0.499	0.332	0.200	0.434	0.079	0.339	0.929
USE_2	0.216	-0.008	0.530	0.331	0.154	0.494	0.128	0.333	0.906
USE_3	0.304	-0.027	0.470	0.351	0.229	0.426	0.067	0.361	0.935
USE_4	0.297	-0.039	0.505	0.348	0.206	0.454	0.065	0.354	0.958
USE_5	0.297	-0.027	0.492	0.322	0.226	0.452	0.083	0.379	0.919

Note. The bolded section in each column represents the construct associated with the corresponding items in each row.

Table 6

Discriminant Validity

	DATAOWN	FININC	I-Task	I-Tech	PRIV	R-Task	R-Tech	SEC	Use
DATAOWN	1.000								
FININC	-0.052	0.894							
I-Task	0.284	0.001	0.864						
I-Tech	0.284	-0.070	0.410	0.899					
PRIV	0.432	-0.002	0.212	0.175	0.878				
R-Task	0.198	-0.023	0.711	0.356	0.169	0.864			
R-Tech	0.020	-0.002	0.346	0.348	-0.022	0.377	0.888		
SEC	0.415	0.023	0.373	0.271	0.438	0.358	0.091	0.791	
Use	0.303	-0.028	0.538	0.362	0.218	0.487	0.091	0.379	0.930

Note. The bolded section in each column represents the square root of the average variance extracted. Control variables: Position in Company retained, remaining control variables dropped due to being insignificant. DATAOWN – Data Ownership; FININC – Financial Incentives; PRIV – Privacy Controls; SEC – Security Controls.

Model 1 Results

Model 1 hypothesized that antecedents have an effect on BYOD use and the mediating effects of AST create a positive impact on BYOD use. Using PLS to evaluate the main effects of antecedents and independent variables, there is support for many of the hypothesized dimensions.

Starting with the antecedents, security controls was significant and positive on two of the four mediating dimensions: exploitive technology adaptation (β = .187, *t* value = 4.870) and exploratory technology adaptation (β = .125, *t* value = 2.785). Corporate data ownership was significant and positive on one of the four mediating dimensions: exploitive technology adaptation (β = .200, *t* value = 5.232). Privacy controls were found to be significant on one of the four mediating dimensions: exploratory technology adaptation (β = -0.077, *t* value = 1.917). Financial incentives were not found to be significant on one of the four mediating dimensions: exploitive technology adaptation (β = -0.063, *t* value = 1.886).

The independent variables were positive and significant in seven of eight mediating dimensions. These factors are exploitive technology adaptation–use (β = .199, *t* value = 5.924), exploitive task adaptation–use (β = .354, *t* value = 8.626), exploratory task adaptation–use (β = .237, *t* value = 6.017), exploitive technology adaptation–exploitive task adaptation (β = .228, *t* value = 6.507), exploitive technology adaptation–exploratory task adaptation (β = .170, *t* value = 4.917), exploratory technology adaptation–exploitive task adaptation (β = .244, *t* value = 7.525), and exploratory technology adaptation–exploratory task adaptation (β = .294, *t* value = 8.743).

Finally, while this was not hypothesized, there was a positive significant direct effect of the control variable position in company to the variable use (β = .138, *t* value = 5.790).

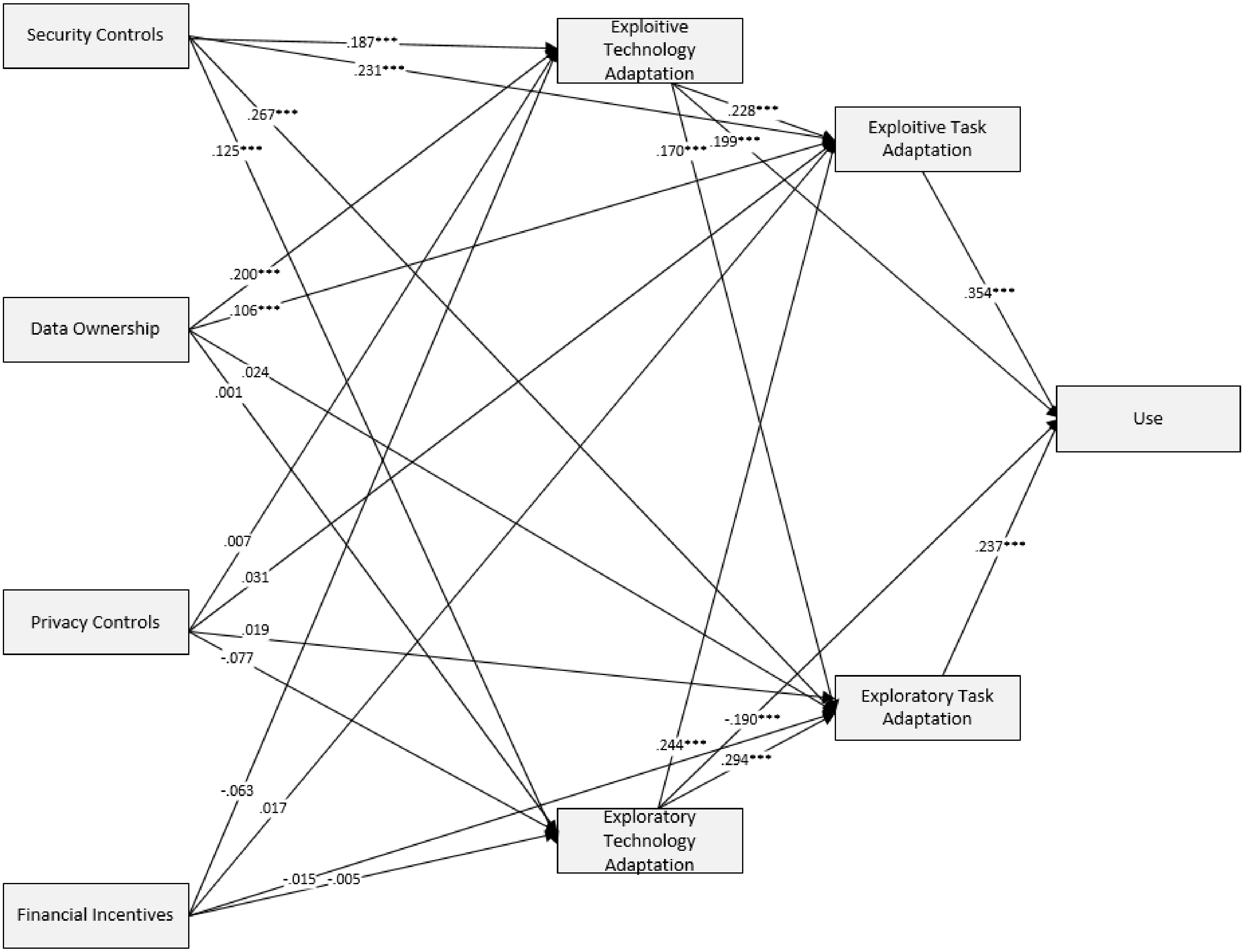


Figure 7. Structural model for main effects.

Table 7

Summary of Results (Main Effects)

Hypothesis	Result	Standard β	*t* value
Exploitive Technology Adaptation → Use	H_1: Supported	0.199***	5.924
Exploitive Task Adaptation → Use	H_2: Supported	0.354***	8.626
Exploratory Task Adaptation → Use	H_3: Supported	0.237***	6.017
Exploitive Technology Adaptation → Exploitive Task Adaptation	H_{4a}: Supported	0.228***	6.507
Exploitive Technology Adaptation → Exploratory Task Adaptation	H_{4b}: Supported	0.170***	4.917
Exploratory Technology Adaptation → Exploitive Task Adaptation	H_{5a}: Supported	0.244***	7.525
Exploratory Technology Adaptation → Exploratory Task Adaptation	H_{5b}: Supported	0.294***	8.743
Security Controls → Exploitive Technology Adaptation	H_{6a}: Supported	0.187***	4.870
Security Controls → Exploratory Technology Adaptation	H_{6b}: Supported	0.125**	2.785
Corporate Data Ownership → Exploitive Technology Adaptation	H_{7a}: Supported	0.200***	5.232
Corporate Data Ownership → Exploratory Technology Adaptation	H_{7b}: Not Supported	0.001	0.023
Privacy Controls → Exploitive Technology Adaptation	H_{8a}: Not Supported	0.007	0.192
Privacy Controls → Exploratory Technology Adaptation	H_{8b}: Supported	-0.077*	1.917
Financial Incentives → Exploitive Technology Adaptation	H_{9a}: Supported	-0.063*	1.886
Financial Incentives → Exploratory Technology Adaptation	H_{9b}: Not Supported	-0.005	0.118

$p < 0.1$, *$p < .05$, **$p < .01$, ***$p < .001$.

Discussion

This study makes three important contributions to the extant literature. First, the study extends extant literature by applying the concept of AST to the BYOD context within a corporate environment. As the use of BYOD expands across multiple industries, important factors related to the implementation and ongoing success of such programs will be important. Second, the mediating influence of exploitative and exploratory adaptation in task and technology is important as individuals continue to work with advancing technology and applications. This ongoing work will drive the possibility of needing to alter the technology or methods of using BYOD to accomplish work tasks. Third, the influence of antecedent conditions will likely be an ongoing fluid environment due to the changing security and data ownership requirements. As more modifications are made to organizational financial incentive programs, there is likely to be an impact on the level of impact related to use.

Study findings showed that exploitive technology adaptation has a positive influence on BYOD use. As users exploit the features available in the technology as the features were intended to be used, they are more likely to use their own devices for work-related purposes. This is an important finding since, as per AST, adaptation to technology can enable favorable outcomes (K. W. Schmitz et al., 2016). Therefore, this finding implies that in the BYOD context, encouraging BYOD users to exploit their own device features can have important impacts on how they approach and conduct work-related tasks.

The findings also showed that exploratory technology and task adaptation has limited influence on BYOD use. The primary driver for this outcome is likely related to the limited opportunity users have to attempt to deviate from the overall use of the applications and hardware supporting their work tasks. It can be assumed that while individuals will find ways to adapt to their technology, they spend little time looking for permanent solutions to meet needs.

There is a positive influence for many antecedent factors throughout the study. Specifically, security controls have a significant impact on an individual's overall ability to either exploit or explore the adaptation of technology. Both privacy controls and financial incentives indicate a positive influence on exploratory technology adaptation, and that is likely related to the possibility of being offered incentives and the capabilities to alter the process.

Finally, the study found that financial incentives and exploratory technology adaptation did not have a positive or significant relationship. One can assume that this overall relationship has been established as a result of the potential lack of desire to invest time and effort into finding new ways of using technology if not receiving financial incentives. While individuals may be supportive of altering a specific task, they are less likely to purchase additional equipment or newer equipment to support any advanced work.

Limitations of this Study

This study does have some limitations. First, the results are limited to a single industry that does not have a history of providing widespread opportunity for supporting personal device use. Therefore, the study findings may only represent the perceptions of one industry and may not be generalizable to other industries. However, the survey questions and research constructs examined should be applicable across a variety of industries. Second, a large population of employees are field-based and may not have a need for using personal technology to perform work tasks. Although the sample represented a diverse group, the need for BYOD could be more limited in the organization and could have impacted the study findings. Finally, the survey was conducted as a single snapshot measurement.

Implications for Research

The results of this dissertation have the potential to impact a variety of related research. Much of the adoption and use research has been limited to specific aspects of technology hardware components. However, this study highlights the critical role played by exploratory and exploitative technology and task adaptation to the adoption and use of BYOD. Further, this study provides empirical validation of security controls, privacy controls, data ownership, and financial incentives on the mediating factors of technology and task adaptation. Therefore, findings from this study introduce the opportunity to understand how factors such as security and privacy controls may influence decision-making related to program implementation and individual support.

This study focused exclusively on one industry as the study context. Expanding this work to include various industry types will assist in creating a wide view of how personal devices add or reduce value within the organization. In addition to the focus on personal device use, the focus of this research could be expanded to include the specific application use within the industry. Introducing application use along with the hardware components has the potential to provide a detailed picture of how each variable contributes to or detracts from the use of the BYOD program.

The COVID-19 pandemic has altered the way employees work in organizations. Many organizations have changed policies to allow more remote work. In fact, employees have been incentivized to perform their work functions from their homes or other remote settings. With the recent changes in many workplaces and the expansion of remote work, it is likely that there will be an opportunity for more individuals to be in a position to enroll in a personal device use program. In these circumstances, I believe that security and privacy controls will be key factors in the adoption and use of BYOD. As organizations define a balance of enabling capabilities and controlling access, there is likely to be a downstream impact on users. In addition, users may determine that, due to some of the boundaries put in place, they are unable to efficiently perform work tasks, causing a need to alter their work relationship. These behavioral changes in employees due to remote work and BYOD, their work-life balance, and their relationship with their employer could be studied in further detail in future studies.

Implications for Practice

Many organizations have implemented personal device use programs in recent years using limited data to drive to their conclusions. As the industry adjusts to the needs of the workforce and industry trends, there is a likelihood that the information used to support decision-making will be expanded to include additional factors. Today, cost and security are major factors, but with a large population of workers now working in-home or in remote environments, the need to consider additional criteria increases.

Based on study findings, the adaptation factors (i.e., exploit and explore task and technology) can influence BYOD use. Therefore, end-user education may be an effective means to influence BYOD use. For instance, it may be possible to provide basic training that both advanced and basic users can use to influence their ability to put into effect changes to their device use. Further, such training may influence their willingness to invest time exploring new capabilities and methods for establishing new processes and technology.

This study highlights the key contributors that can support a successful personal device program. Organizations will need to take notice of these key factors and be open to adjusting policies and capabilities to increase the value to both the employees and the organization without introducing unnecessary risk.

Conclusion

To provide remote connectivity and data access, organizations are looking to find the right balance between corporate devices and BYOD. Both alternatives have advantages and disadvantages resulting in either successful or limited adoption. In support of the model adopted within the organization, there is a need to clearly identify how AST is leveraged at the individual and enterprise level. There are three factors that impact the overall desire to adopt, and each has varying effects, depending on the individual user. Having adequate consideration for privacy controls, data ownership, security compliance policies, and the overall financial policy will help define the criteria to measure BYOD adoption. Many organizations have relied on more traditional methods of providing devices to the employee base, so exploring a BYOD program will assist with the ongoing transformation.

Findings from this study demonstrate a positive impact on the overall BYOD adoption as it relates to individual employees based on antecedent conditions and mediating factors. When employees can utilize their devices of choice, understand the security compliance policies being applied, and weigh the financial policies, there is a positive impact on the BYOD adoption mediated by technology and task adaptation. However, while technology continues to expand in capability, the adoption rate and usage may not be consistent across all workgroup types, regardless of location. In particular, the regulated utility industry will have to adapt to the changes, needs, and limitations to ensure that a consistent and reliable experience can be made available and alternatives of similar caliber must be made to those not capable of using technology.

Notably, in the case of BYOD, there are established differences in how employees have adopted the use of these capabilities. The differences in what employees believe to be acceptable and the parameters that organizations place on the overall treatment of personal devices will have a widespread impact. Due to this impact, the job level, responsibilities, and desire to select the device to be used need to be considered as vital factors. While the results from this dissertation provide a baseline for the current environment, there are implications related to developing a long-term plan that can fully utilize the capabilities of the BYOD program. Therefore, developing an overarching BYOD strategy, fostering explorative and exploitative technology adaptation, and encouraging and educating employees on BYOD adoption becomes extremely important, especially in a rapidly changing business and technology environment.

References

Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems*, *14*(2), 195–201. doi:10.48009/2_iis_2013_195-201

Battleson, D. A., West, B. C., Kim, J., Ramesh, B., & Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: An empirical investigation. *European Journal of Information Systems*, *25*(3), 209–230. doi:10.1057/ejis.2015.12

Beckett, P. (2014). BYOD – Popular and problematic. *Network Security*, *2014*(9), 7–9. doi:10.1016/S1353-4858(14)70090-X

Brandel, M. (2012). BYOD: Where the costs are. *Network World*, *29*(20), 16, 21. Retrieved from https://www.networkworld.com/

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, *14*(2), 189–217. doi:10.1287/isre.14.2.189.16018

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659–673. doi:10.1080/17517575.2017.1404132

Christensen, C. M., & Overdorf, M. (2000). Meeting the challenge of disruptive change. *Harvard Business Review*, *78*(2), 66–76. Retrieved from https://hbr.org/

Cox, J. (2012). IT groups eschew BYOD: Workers to carry company-owned tablets. *Network World*, *29*(13), 1, 16. Retrieved from https://www.networkworld.com/

Cragg, P. B., & Zinatelli, N. (1995). The evolution of information systems in small firms. *Information & Management*, *29*(1), 1–8. doi:10.1016/0378-7206(95)00012-L

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. doi:10.2307/249008

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science*, *5*(2), 121–147. doi:10.1287/orsc.5.2.121

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

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., & Saad, E. H. M. (2014). BYOD: Current state and security challenges. In *2014 IEEE Symposium on Computer Applications and Industrial Electronics*, (pp. 189–192). doi:10.1109/ISCAIE.2014.7010235

Evans, D. (2013, August 23). *What is BYOD, and why is it important?* Retrieved from https://www.ware247.co.uk/Content/CMS/Files/What%20is%20BYOD.pdf

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. doi:10.1177/002224378101800104

Gangwar, H. (2017). Cloud computing usage and its effect on organizational performance. *Human Systems Management*, *36*(1), 13–26. doi:10.3233/HSM-171625

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(1), 1–76. doi:10.17705/1CAIS.00407

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62–70. Retrieved from https://www.rroij.com/global-research-in-computer-science.php

Goedert, J. (2013). Mobile device management software: The answer to BYOD? *Health Data Management*, *21*(2), 32, 34, 36, 38, 40. Retrieved from https://www.healthdatamanagement.com/

Grensing-Pophal, L. (2014). Be careful with BYOD. *Credit Union Management*, *37*(10), 18–21. Retrieved from https://www.cumanagement.com/

Huang, K.-E., Wu, J.-H., Lu, S.-Y., & Lin, Y.-C. (2016). Innovation and technology creation effects on organizational performance. *Journal of Business Research*, *69*(6), 2187–2192. doi:10.1016/j.jbusres.2015.12.028

Jong, J. D., & Hartog, D. D. (2010). Measuring innovative work behaviour. *Creativity and Innovation Management*, *19*(1), 23–36. doi:10.1111/j.1467-8691.2010.00547.x

Mcguckin, R. H., Streitwieser, M. L., & Doms, M. (1998). The effect of technology use on productivity growth. *Economics of Innovation and New Technology*, *7*(1), 1–26. doi:10.1080/10438599800000026

Moosakhani, M., Mohammadi, S., & Modiriasari, M. (2011). Critical success factor in IT project risk management in virtual enterprise: Multi case study. *Journal of Information Technology Management*, *3*(6). Retrieved from https://jitm.ut.ac.ir/

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8. doi:10.1016/S1353-4858(12)70111-3

Munroe, F. (2013). Technological transformation—Implications for compliance from big data to BYOD. *Journal of Health Care Compliance*, *15*(6), 41–46. Retrieved from https://lrus.wolterskluwer.com/store/product/journal-of-health-care-compliance/

Nunnally, J. (1978). *Psychometric theory* (2nd ed.). New York, NY: McGraw-Hill.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, *3*(3), 398–427. doi:10.1287/orsc.3.3.398

Orlikowski, W. J. (2000). Using technology and tonstituting structures: A practice lens for studying technology in organizations. *Organization Science*, *11*(4), 404–428. doi:10.1287/orsc.11.4.404.14600

Ragowsky, A., Ahituv, N., & Neumann, S. (1996). Identifying the value and importance of an information system application. *Information & Management*, *31*(2), 89–102. doi:10.1016/S0378-7206(96)01072-5

Redman, P., Girard, J., & Wallin, L.-O. (2011, April 13). *Magic quadrant for mobile device management software* [Report ID G00211101]. Retrieved from https://www.gartner.com/en/documents/1632331/magic-quadrant-for-mobile-device-management-software

Ringle, C. M., Wende, S., and Becker, J.-M. (2015). SmartPLS 3. Retrieved from http://www.smartpls.com

Scarfo, A. (2012). New security perspectives around BYOD. In *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications* (pp. 446–451). doi:10.1109/BWCCA.2012.79

Schmitz, K., Webb, K., & Teng, J. (2010). Exploring technology and task adaptation among individual users of mobile technology. In *ICIS 2010 Proceedings*. Retrieved from https://aisel.aisnet.org/

Schmitz, K. W., Teng, J. T. C., & Webb, K. J. (2016). Capturing the complexity of malleable IT use: Adaptive structuration theory for individuals. *MIS Quarterly, 40*(3), 663-686. doi:10.25300/MISQ/2016/40.3.07

Smith, W. P. (2017). Can we borrow your phone? Employee privacy in the BYOD era. *Journal of Information, Communication & Ethics in Society*, *15*(4), 397–411. doi:10.1108/JICES-09-2015-0027

Stephenson, P. (2014). Mobile device management. *SC Magazine*, *25*(7/8), 36–37. Retrieved from https://www.scmagazine.com/

Swanepoel, R. (2015, June). BYOD: Are You Missing the Boat? *Accountancy SA*, 32–33. Retrieved from https://www.accountancysa.org.za/

Swanson, E. B., & Ramiller, N. C. (1997). The organizing vision in information systems innovation. *Organization Science*, *8*(5), 458–474. doi:10.1287/orsc.8.5.458

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2), 5–8. doi:10.1016/S1353-4858(12)70013-2

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. doi:10.2307/41410412

Violino, B. (2012). The BYOD security challenge: The growing variety of new devices makes supporting and controlling access to systems and data much more challenging for IT. *Insurance Networking News*, *15*(8), 29.

Weeger, A., Wang, X., & Gewald, H. (2015). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems*, *56*(1), 1–10. doi:10.1080/08874417.2015.11645795

Yousif, M. (2018). Cloud computing reliability—Failure is an option. *IEEE Cloud Computing*, *5*(3), 4–5. doi:10.1109/MCC.2018.032591610

Appendix A
Survey Instrument and Questions

Construct	Item	Question
BYOD Use (Use)	USE_1	Using my personal device enables me to accomplish more work tasks.
	USE_2	Using my personal device improves the quality of work I do.
	USE_3	Using my personal device makes it easier to do my job.
	USE_4	Using my personal device enhances my effectiveness on the job.
	USE_5	Using my personal device gives me greater control over my work.
Exploitive Technology Adaptation (ITECH)	ITECH_1	I have experimented with new features on my personal device, as they were intended to be used.
	ITECH_2	I have changed the settings/preferences on my personal device to alter the way I interact with it.
	ITECH_3	I have taken advantage of the adaptability of the features available on my personal device, as they were intended to be used.
	ITECH_4	I have customized some features on my personal device, as they were intended to be used.
	ITECH_5	I do not like to change any settings/preferences on my personal device to alter the way I interact with it.
Exploratory Technology Adaptation (RTECH)	RTECH_1	I have developed a way of using my personal device which deviates from how it is normally used.
	RTECH_2	I have used at least one personal device feature or capability differently from how it is normally used.
	RTECH_3	I have modified something on my personal device to use it differently from how it is normally used.
	RTECH_4	I like to experiment with new features or capabilities on my personal device to deviate from how it is normally used.
	RTECH_5	I do not like to modify anything on my personal device to use it differently from how it is normally used.
Exploratory Task Adaptation (RTASK)	RTASK_1	I have tried to perform work-related tasks that were not possible without my current personal device.
	RTASK_2	I strive to find ways to take on new work responsibilities by using my personal device.

Construct	Item	Question
	RTASK_3	My current personal device has allowed me to frequently attempt new tasks I could not do in the past.
	RTASK_4	Overall, use of my current personal device has enabled me to try new and different work-related tasks.
	RTASK_5	Using my personal device prevents me from attempting new work tasks.
Exploitive Task Adaptation (ITASK)	ITASK_1	I try hard to figure out ways to do my existing work tasks better by using my current personal device.
	ITASK_2	Using my personal device has forced me to find new ways of performing work tasks.
	ITASK_3	I strive to find ways to do my existing work tasks faster with features on my current personal device.
	ITASK_4	Overall, I am doing my best in taking advantage of various features of my current personal device to perform my existing tasks better.
	ITASK_5	Using my personal device prevents me from being efficient while performing existing work tasks.
Security Controls (SC)	SC_1	The corporate BYOD program security controls in my organization enable me to perform work tasks.
	SC_2	The corporate BYOD program security controls installed on my personal device(s) provide a secure solution.
	SC_3	The corporate BYOD program security controls have improved how I do my work tasks.
	SC_4	I am using my personal device(s) more because of the corporate BYOD program security controls.
	SC_5	My organization's corporate BYOD program security controls prevent me from performing work tasks.
Corporate Data Ownership (CDO)	CDO_1	The corporate data ownership policy is well-defined in my organization
	CDO_2	My organization enables me to access corporate data on my personal device easily.
	CDO_3	The corporate data ownership policy prevents me from accessing corporate data on my personal device.
	CDO_4	The current mobile device management application on my personal device enables me to protect data.
	CDO_5	I am not currently enrolled in the corporate BYOD program because of data ownership concerns.

Construct	Item	Question
Privacy Controls (PC)	PC_1	I am confident that my personal data remains private if enrolled in the corporate BYOD program.
	PC_2	I understand the function the mobile device management application provides to protect data.
	PC_3	Privacy controls in the corporate BYOD program enable me to work without any worry about my personal data.
	PC_4	I have confidence that my personal data will be protected if enrolled in the corporate BYOD program.
	PC_5	I am not currently enrolled in the corporate BYOD program because of privacy controls.
Financial Incentives (FI)	FI_1	The financial incentive I receive for participating in the BYOD program is acceptable.
	FI_2	I participate in the BYOD program because of the financial incentives.
	FI_3	I have invested in personal devices to perform work tasks because of the financial incentives.
	FI_4	Financial incentives are the best part of my organization's corporate BYOD program.
COVID-19 (COV)	COV_1	Current COVID-19 pandemic conditions have changed where I work.
	COV_2	Due to the COVID-19 pandemic, I now use a personal device to complete work tasks.
	COV_3	Due to the COVID-19 pandemic, I purchased additional personal technology to support my work tasks.
	COV_4	Due to the COVID-19 pandemic, my work life has been negatively affected.

VITA

Steven A. Liegl Jr. was born May 8, 1973, in West Bend, Wisconsin. He completed his undergraduate work at Wisconsin Lutheran College in Milwaukee, Wisconsin, where he received a B.S. in Business Management and Leadership (2013). He completed his M.B.A. at the University of Wisconsin–Whitewater in Whitewater, Wisconsin (2017). Steven currently holds the role of Director of Infrastructure and Operations within the Information Technology department at WEC Energy Group, headquartered in Milwaukee, Wisconsin. In addition to his full-time employment responsibilities, Steven enjoys serving as a lecturer, teaching various information technology and business courses at the University of Wisconsin–Whitewater and University of Wisconsin–Oshkosh.