2017

An Exploratory Study of the Approach to Bring Your Own Device (BYOD) in Assuring Information Security

Coleen D. Santee
Nova Southeastern University, santee@nova.edu

An Exploratory Study of the Approach to Bring Your Own Device (BYOD) in Assuring Information Security

by

Coleen D. Santee

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2017

We hereby certify that this dissertation, submitted by Coleen Santee, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Frank Nasuti, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Steven R. Terrell, Ph.D. Date
Dissertation Committee Member

_____ _____

Maxine S. Cohen, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Yong X. Tao, Ph.D., P.E., FASME Date
Dean, College of Engineering and Computing

College of Engineering and Computing
Nova Southeastern University

2017

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Exploratory Study of the Approach to Bring Your Own Device (BYOD) in Assuring Information Security

by
Coleen D. Santee
April 2017

The availability of smart device capabilities, easy to use apps, and collaborative capabilities has increased the expectations for the technology experience of employees. In addition, enterprises are adopting SaaS cloud-based systems that employees can access anytime, anywhere using their personal, mobile device. BYOD could drive an IT evolution for powerful device capabilities and easy to use apps, but only if the information security concerns can be addressed. This research proposed to determine the acceptance rate of BYOD in organizations, the decision making approach, and significant factors that led to the successful adoption of BYOD using the expertise of experienced internal control professionals. The approach and factors leading to the decision to permit the use of BYOD was identified through survey responses, which was distributed to approximately 5,000 members of the Institute for Internal Controls (IIC). The survey participation request was opened by 1,688 potential respondents, and 663 total responses were received for a response rate of 39%.

Internal control professionals were targeted by this study to ensure a diverse population of organizations that have implemented or considered implementation of a BYOD program were included. This study provided an understanding of how widely the use of BYOD was permitted in organizations and identified effective approaches that were used in making the decision. In addition, the research identified the factors that were influential in the decision making process. This study also explored the new information security risks introduced by BYOD. The research argued that there were several new risks in the areas of access, compliance, compromise, data protection, and control that affect a company's willingness to support BYOD. This study identified new information security concerns and risks associated with BYOD and suggested new elements of governance, risk management, and control systems that were necessary to ensure a secure BYOD program. Based on the initial research findings, future research areas were suggested.

Acknowledgements

This dissertation has been a constant companion and is a dream realized. I owe so much gratitude to my husband and children for their constant support and encouragement. I would not have made it without you. Included in my journey has been my circle of friends and sisters that encouraged me and kept me accountable. You're the best, and you helped me endure to the finish.

I also would like to extend a heartfelt thank you to my committee chair, Dr. Frank Nasuti, for his advice, patience, and constant support to stay focused on the goal. I would also like to thank my dissertation committee members, Drs. Maxine Cohen and Steven Terrell, for their valuable comments and suggestions. I appreciate all of you and am so thankful to have had your guidance.

Lastly, I must give all thanks to almighty God, who surrounded me with such great supporters and gave me strength to carry on despite all that has happened these past ten years.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The pervasive use of personal smart devices combined with the growth of cloud services has resulted in abundant access to advanced information technologies on personal mobile devices. According to Armando, Costa, Verdeme, and Merlo (2014), two primary factors are responsible for the rapid adoption of mobile devices: one is the powerful mobile operating systems that provide advanced device capabilities, and the other is the market place delivery model for literally millions of diverse apps that cater to the user's needs. The expectation to utilize these smart devices and advanced capabilities in all aspects of a daily routine has resulted in the BYOD (Bring Your Own Device) phenomenon, which is the use of personal mobile devices, such as smartphones and tablets, for work related purposes (Banham, 2013). The term "consumerization" has been coined to describe the larger impact on organizations when high-tech products and services for the consumer market spread over into the business environment (Castro-Leon, 2014).

BYOD is increasing rapidly in the business environment due to two primary factors. First, these advanced devices and applications are readily available for personal use and are finding their way into the workplace, causing significant information security

challenges for organizations (Earley, Harmon, Lee, & Mithas, 2014). Second, enterprises are adopting SaaS (Software-as-a-Service) cloud-based applications that leverage the features of mobile devices to provide a robust technology experience for employees. These new technology devices and advanced applications are challenging the traditional approach to information security controls, which include provisioning, controlling access to, and protecting equipment, systems, and data.

BYOD is a strategic trend that could catapult the capabilities of organizational systems forward, increasing the productivity of the workforce by capitalizing on advanced device capabilities, delivering user friendly functionality, and providing nearly instant access to information. BYOD could drive an IT evolution that leverages powerful device capabilities and easy to use apps, but only if its use is permitted in the organization. Organizations are tasked with balancing the expectations of users and reaping the benefits of robust mobile-capable SaaS applications, while protecting the confidentiality, integrity, and availability of information. Kumar and Singh (2015) suggest that the growing cultural trend of BYOD is the top new threat to information systems.

Traditional means of securing data through unwieldy controls and absolute policies are perceived as an intrusion of privacy and enacting excessive controls on personal property. Effective policies, new tools, and appropriate controls must be enacted to securely adopt these new technology paradigms, so that organizations can realize the full benefits of BYOD, while not overly restricting personal use of the device. Organizations that solve the information security conundrum of BYOD may position

themselves with a high performing workforce that utilizes high tech systems to drive business innovation and outperform competitors.

The continual advancement of personal mobile technology and SaaS solutions can provide significant benefits to the organization, such as improving employee productivity and satisfaction, driving business innovation, and providing cost reductions. Because employees want to use their personal devices in the workplace and the organization can realize tangible benefits by supporting BYOD programs, it is important to identify the areas of information security risk and institute appropriate internal controls. Although SaaS vendors claim high levels of information security that are aligned with security standards and produce attestation statements to ensure their diligence, organizations must understand that malicious attacks will be directed at the mobile device.

Allowing personal data and apps to coexist with sensitive business data on a personal device that is largely outside the control of the organization introduces substantial risks to information security. Robert Rhodes states that "mobile devices are one of the biggest risks IT professionals have to deal with" (Rhodes & Kaplan, 2012, pg. 24). Traditional information security efforts target protection of information and systems within the boundaries of IT control. BYOD distributes access, data, and processing to an external device beyond the four walls of a protected data center.

To embrace the productivity opportunities, organizations must establish BYOD programs that address device security, data protection, and appropriate access methods. These advanced IT capabilities are important to the success and growth of the organization (Haes & Grembergen, 2008), and internal control is essential to ensuring

that the organization is protected with standard controls and processes (Tarantino, 2009). Employees prefer the use of productivity apps to more efficiently handle their work tasks, while using the same device to interact with social media and access cloud based storage and collaboration sites (Banham, 2013). BYOD programs must manage devices that are not organizationally owned to comply with a variety of regulations and business requirements (Taylor, 2013). Taylor also suggests that although technology solutions are available to manage data on mobile devices, policies and education are critical to the success of BYOD programs. Strong usage policies that are monitored and enforced should require that employees separate personal mobile apps from business apps, use encryption when transmitting data, and prohibit the storage of sensitive information on a personal device (Banham). In addition, BYOD introduces significant risk when employees download personally identifiable information, confidential customer information, or proprietary business data, because the device can easily be stolen, lost, or compromised (Drew, 2012; Eisenberg, Kallner, & Ben-Harrush, 2014).

Organizations are tasked with balancing the expectations of users while protecting the confidentiality, integrity, and availability of information. In order to realize the benefits that can drive business innovation and a high performing workforce, enterprises must find a successful approach to adopting BYOD. Organizations strive to establish and continually improve general information security controls since organizations are dependent on information that is captured, stored, and managed by a constantly changing technology environment (Van Grembergen, De Haes, & Guldentops, 2004). Now they are challenged with understanding the new sources of risk introduced by BYOD to

business information, in order to adequately protect sensitive data, establish effective policies, and comply with a variety of laws and regulations (Khoo, Harris, & Hartman, 2010). Adequate internal controls are typically established and enforced by internal audit professionals in the organization to assure an organization is effective and efficient in meeting the organization's goals, while ensuring compliance with policies and regulations.

Problem Statement

The availability of smart device capabilities, easy to use apps, and collaborative solutions has raised the expectations of employees, leaving them dissatisfied with the less personalized and isolated technology experience found in most workplaces. Employees wish to utilize their smart device capabilities to experience a robust technology experience with business email, calendaring, file sharing, and other collaborative solutions. In addition, enterprises are adopting SaaS cloud-based systems, which provide a high quality, intuitive, and personalized technology experience anytime, anyplace, on any device; and employees prefer their own personal mobile device. The BYOD movement is fueling the expectations of employees for user centric applications that may help organizations realize improved productivity and greater employee satisfaction, while at the same time presenting one of the greatest information security concerns (Rhodes & Kaplan, 2012). Organizations are tasked with balancing the expectations of users while protecting the confidentiality, integrity, and availability of information.

The protection of organizational assets is a key priority, and the constantly changing, increasingly complex, and progressively pervasive information technology

environment makes this all the more difficult (McFadzean, Ezingeard, & Birchall, 2006; Sanchez, Villafranca, Fernandez-Medina, & Piattini, 2006). Despite the productivity opportunities, organizations must establish BYOD programs that include effective policies, appropriate access methods, compliance with applicable regulations, device security, data protection, and proper controls.

Ensuring authorized access to business systems and data on an unmanaged device is a significant challenge for information security efforts. The most significant threat introduced by BYOD is the loss or theft of sensitive customer or business data (Banham, 2013) when it is not adequately protected during transmission, at rest on the device, or when the device is lost or stolen (Eisenberg et al., 2014).

Effective controls and audit programs are required to ensure BYOD programs comply with a multitude of legal and regulatory requirements (Taylor, 2013). In addition, information security efforts must be able to detect the breach of an account or device, and identify and respond to malicious behavior quickly. Effective policies, new tools, and appropriate controls must be enacted to securely adopt these new technology paradigms, without disregarding the rights and privacy of the employee.

There is a wealth of research and information security standards that identify appropriate controls to mitigate information security risk. However, there is little understanding of the specific approach that can lead to successful adoption of a BYOD program. This research was conducted to understand which organizations permitted BYOD, what approach was followed to evaluate and assess the risks, and what specific factors affected a company's decision to adopt BYOD. In addition, specific information

security risks associated with BYOD were identified so that appropriate internal controls that lead to successful programs can be put in place to enable the high tech advantages that both employees and organizations seek (Harris, Kinkela, & Hayes, 2011).

Dissertation Goal

The goal of this research was to explore how widely BYOD is permitted in organizations, the approaches that were used in the decision making process to allow the use of BYOD, the factors that affected a company's willingness to support BYOD, and the specific information security risks that were associated with a BYOD program. This study used exploratory research to identify the decision making approach and the significant factors leading to the successful adoption of BYOD programs. The intended research proposed that several new information security risks, including access, compliance, compromise, data sharing, and control, may affect a company's willingness to support BYOD. Access is concerned with ensuring authorized access of an unmanaged device to business systems and data. Compliance is concerned with abiding by the requirements of regulations and policies even when the device is outside the control of the company. Compromise is concerned with the breach of an account or device, and being able to identify and respond to malicious behavior quickly. Data sharing is concerned with the protection of data such that sensitive information is never downloaded or shared inappropriately. Control is concerned with having jurisdiction over user activity, data, and the device in order to adequately protect the company's interests.

Research Questions

Given the opportunities and challenges that BYOD presents to organizations, this research explored five research questions to understand how BYOD was securely adopted by organizations.

RQ1: How widely is the use of BYOD permitted in organizations?

The first research question attempted to determine if BYOD is permitted in organizations to establish the actual rate of acceptance, and to classify the research into categories of organizations that do use BYOD and those that do not. According to a 2013 study by iPass Inc., 72% of organizations have a mobile strategy, but only 37% feel that it is effective (iPass Inc., 2013). This research question established the acceptance of BYOD for this study, and explored the factors that influenced the decision.

RQ2: What approach was employed to evaluate BYOD?

The second research question attempted to determine what type of methodical approach was used as the organization decided whether to permit BYOD. In particular, the research investigated the assessment of risk and approach to decision making as an organization considers a BYOD program. This study suggests that a risk assessment is critical to identifying specific risks introduced by BYOD and defining appropriate information security controls to provide reasonable assurance against identified risks. Further, the research attempted to determine the level of involvement of various organizational stakeholders in the decision to allow the use of BYOD. Auditors and other internal control professionals are responsible for assessing risk to the organization

and they may have extensive expertise in information security. This study expected that the participation of internal control professionals was necessary to effectively assess risk and identify reasonable controls to allow the use of BYOD. However, the research found that the BYOD decision was made without the involvement of internal control professionals for a majority of the organizations.

The findings associated with this question identified effective approaches to evaluate a BYOD program, including risk assessment and the decision making participants and process.

RQ3: What factors affected the decision to allow BYOD programs?

The third research question identified the significant factors that contribute, positively or negatively, to a decision regarding the adoption of BYOD. The study investigated the specific elements that influenced the decision making process and identified those that proved to be relevant in the decision to allow BYOD. The findings associated with this question identified the significant factors that affected the decision to allow BYOD, establishing an understanding of the new information security concerns and risks associated with BYOD.

RQ4: How are BYOD programs monitored and controlled?

The fourth research question applied to organizations that allow BYOD, and it identified the additional governance, risk management, and control systems to ensure that the organization is not exposed to unreasonable risk. It was identified that formal BYOD policies were required for a majority of the participants, and it was necessary to identify

the specific aspects of policy that contributed to a successful BYOD program. This study sought to understand the additions to regular systems of governance, risk management, and control for successful BYOD programs.

The findings associated with this question identified the new elements of governance, risk management, and control systems to provide reasonable assurance that the BYOD program was operating effectively and securely.

RQ5: What new information security risks are associated with BYOD programs?

The fifth research question sought to understand the new information security concerns and risks that were associated with BYOD. BYOD presents a multi-layered opportunity to organizations, while introducing significant information security concerns (Earley et al., 2014). Perceived new risks and concerns associated with BYOD were identified by organizations that did not allow BYOD, and perceived and actual new risks and concerns were identified by organizations that do allow BYOD. BYOD is associated with significant information security concerns in the broad areas of device security, data security, and data availability. This study found that there were several factors, including access to data, compliance with policies, compromise of the device, protection of sensitive data, and control of the device that may introduce new risks and affect a company's willingness to support BYOD. It was important to accurately determine dominant information security risks in order to identify the associated mitigating controls that contribute to a successful BYOD program.

Relevance and Significance

The BYOD movement has accelerated the availability of user-centric applications that can help organizations realize improved productivity and greater employee satisfaction. In addition, SaaS solutions that provide significant organizational benefit and user centric capabilities that increase employee productivity feature robust mobile experiences accessible by any device, anywhere. Organizations can benefit greatly from BYOD, but not unless information security concerns are understood and mitigated.

The findings of this study provide an understanding of how widely the use of BYOD was permitted in organizations, and identified effective approaches that were used in making the decision. In addition, the research identified the factors that were influential in the decision making process. Finally, this study identified new information security concerns and risks associated with BYOD and suggested new elements of governance, risk management, and control systems that were necessary to ensure a secure BYOD program.

Barriers and Issues

It was essential to the validity of the research to have the opinions of experienced auditors and other internal control professionals. Because the input of these internal control professionals was extremely valuable to the research, the Institute for Internal Controls (IIC) was identified as an organization with a membership of internal control professionals; most hold the Certified Internal Controls Auditor (CICA) credential. Working with IIC ensured that this research was based on reputable and active internal control professionals, and assisted in engaging them in this effort.

The prospect of identifying information security concerns and controls for BYOD may be viewed as futile, due to the rapidly changing landscape of device capabilities, cloud solutions, and collaborative apps. Because of this, the resulting research was in danger of being out of date before it finished. In addition, an organization that bases its BYOD program on the results may experience a false sense of security, due to changes in risks that may happen literally overnight. This research was conducted as quickly as possible to ensure the findings were relevant.

To help reduce the impact of change, the research was focused to provide thoroughness, yet quick turnaround. The review of literature, surveys, and analysis was conducted and completed within an aggressive time schedule. Participants in the study understood that the effort was time sensitive, and responded promptly to provide relevant findings.

Assumptions, Limitations and Delimitations

The Institute for Internal Controls (IIC) was identified as an organization with an active membership of approximately 5,000 internal control professionals. The survey distribution did not reach some of these members because of anti-spam software or firewalls. The research was conducted on the members that did receive and complete the survey instrument.

It was expected that certified internal control auditors were experienced in BYOD considerations. This research assumed that valid feedback based on a competent opinion was obtained from these participants.

This study focused on the adoption of BYOD from the perspective of certified internal audit professionals in organizations that recognize the importance of this position. The research findings may not be generalizable based on the scope of potential organizations represented and the voluntary nature of participation. Because organizations have different goals and objectives, it is unlikely that the research findings can be generalized across all organizations.

Gathering information on BYOD security processes was a sensitive proposal. Internal audit professionals may have be reluctant to participate, possibly to avoid disclosure of sensitive information security details to individuals outside the organization (Kotulic & Clark, 2004).

Definitions of Terms

In order to properly establish the scope and complexity of this study, the definition of relevant terms was established.

Information Security

According to Anderson (2003), many definitions of computer security are based on confidentiality, integrity, and availability. Whitman and Mattord (2013) state that "information security (InfoSec) is the protection of information and its critical characteristics (confidentiality, integrity, and availability), including the software and hardware that use, store, and transmit that information through the application of policy, training and awareness programs, and technology" (pg 4). Effective information security is provided through a combination of technical controls, management processes, cultural

elements, and governance (DaVeiga and Eloff, 2007). This research was based on a definition of information security that considers the protection of information and information systems through technical controls, management processes, a culture of security, and effective governance.

Bring Your Own Device (BYOD)

This research defined BYOD according to Banham's (2013) definition of "the use of personal mobile devices like tablets and smartphones for work related purposes."

Consumerization

Castro-Leon (2014) states that consumerization is also known as bring your own device (BYOD). This research defines consumerization as the impact on organizations when high-tech products and services offered to the consumer market are demanded in the business environment. Furthermore, these demands for the new high tech experience are being driven by the users, in a role reversal with traditional IT (Castro-Leon).

Internal Control

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a framework that is regarded as the standard for internal control. This research aligned with COSOs (2013) definition of internal control as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (pg. 3).

Internet of Things (IoT)

This research defined IoT as a large network of things that connect through the Internet. Things include people and devices, and connections can be people to people, people to devices, and devices to devices. Devices include appliances, such as coffee makers or lamps; machines, such as cars or airplanes; and things, such as sensors and monitors. According to Dutton (2014), many of these things carry information with them through embedded sensors or monitors, making simple physical objects into information and communication technologies.

SaaS (Software as a Service)

SaaS is a cloud based delivery model in which software is subscribed to by a business, eliminating the need to install and maintain software and hardware on-premise in a traditional data center. Most SaaS offerings feature a robust user interface designed for mobile devices.

List of Acronyms

BYOD – Bring Your Own Device

CICA – Certified Internal Controls Auditor

COBIT – Control Objectives for Information and related Technology

ERM – Enterprise Risk Management

FERPA – Family Educational Rights and Privacy Act of 1974

GLBA – Gramm-Leach-Bliley Act of 1999

HIPAA – Health Insurance Portability and Accountability Act

IIC – Institute for Internal Controls

IoT – Internet of Things

ISO/IEC – The International Organization for Standardization

IT – Information Technology

ITIL – Information Technology Infrastructure Library

MAM – Mobile Application Management

MDM – Mobile Device Management

NIST – US National Institute of Information Standards and Technology

PCI DSS – Payment Card Industry Data Security Standard

PII – Personally Identifiable Information

SaaS – Software-as-a-Service

SEC – Security and Exchange Commission

SOX – Sarbanes-Oxley Act of 2002

Summary

With the expanding capabilities of smart devices, easy to use apps, and collaborative options that are freely available to the general population, employees have begun to expect the same technology experience and convenience in the workplace. In addition, enterprises are adopting SaaS cloud-based systems that offer a robust mobile experience and give employees access anytime, anywhere using their personal, mobile device. Each Information Technology (IT) department has a responsibility to protect data, systems, and equipment, and must address the information security concerns of BYOD so that organizations can benefit from these powerful device capabilities and easy to use apps. The findings of this study provide an understanding of how widely the use of

BYOD was permitted in organizations, and identified effective approaches that were used in making the decision. In addition, the research identified the factors that were influential in the decision making process. IT must be able to permit BYOD without compromising essential information security controls. This study identified the new information security risks introduced by BYOD and suggested new elements of governance, risk management, and control systems that are necessary to ensure a secure BYOD program.

Chapter 2

Review of the Literature

Overview

This chapter provides an overview of information security research themes and the important works relating to the information security implications of BYOD. Literature in the significance of BYOD and the impact on information security and IT management is reviewed. Literature in the specific information security topics of risk management; information security policies, standards, regulations, and governance; and internal controls is reviewed followed by a summary of the findings.

BYOD

Technology has progressed from being a commodity service provider of information and processing, to being a strategic asset in the current operations of the business, an enabler of competitive advantage, and the means to achieve greater efficiency and productivity (Van Grembergen et al., 2004). Furthermore, "consumerization", the trend of rapidly advancing, high-tech products and services being introduced into the consumer market, is causing concern as employees clamor to connect their personal devices to business networks and thus expose sensitive business data to new opportunities for cyber-attacks (Drew, 2012).

Difilipo (2013) submits that “BYOD” refers only to the device component of consumerization, while consumerization more broadly includes the services, availability of apps, devices, and the Internet of Things (IoT). When an employee chooses to use a personal device at work, all of its related services and capabilities are inherently part of the challenge. Employees embrace the use of productivity apps to more efficiently handle their work tasks, while using the same device to interact with social media and access cloud based storage and collaboration sites (Banham, 2013). There are millions of apps available to smartphone users, and The Nielsen Company (2015) reports that smart devices accessed an average of 27 apps per month in the last three months of 2014. This suggests that BYOD is not a device only, but also includes dozens of apps, as well as powerful internal capabilities.

Mobile devices have seen widespread adoption in the workforce, and CompTIA predicts that BYOD will increase 15% annually, reaching a market value of $181 billion by 2017 (Kaneshige, 2014). According to Juniper Research, more than a billion employee-owned smartphones and tablets will be used for work related tasks by the year 2018 (Moon, 2013). Forrester research explains that the appeal of personal mobile devices is especially strong for tasks that engage customers, such as field work or activities that take advantage of the device’s native capabilities, such as GPS or a camera (Yates, 2013). With mobile devices, employees also benefit from constant connectivity and can access the work environment anytime, anywhere (Eisenberg et al., 2014).

According to Armando, Costa, Verdeme, and Merlo (2014), two primary factors are responsible for the rapid adoption of mobile devices: one is the powerful mobile

operating systems that provide advanced device capabilities, and the other is the market place delivery model for literally millions of diverse apps that cater to the user's needs. Increasingly, apps are being integrated to provide further convenience: the camera links with social media to make sharing photos easier; files stored on the device can be integrated with a file sharing app to provide ease of access for multiple devices or users. Kaplan states that BYOD has "enabled employees to act faster and be more responsive and more productive" (Rhodes & Kaplan, 2012). Since employees will use BYOD to be more efficient and effective, businesses must put appropriate controls in place to mitigate the risks to data, reputation, and finances (Banham, 2013).

To securely realize the productivity opportunities, organizations must establish BYOD programs that include device security, data protection, mobile device policies, and appropriate data access methods. Robert Rhodes states that "mobile devices are one of the biggest risks IT professional have to deal with" (Rhodes & Kaplan). According to a recent study, 72% of organizations have a mobile strategy, but only 37% feel that it is effective (iPass Inc., 2013).

Information Security Management

Management of Information Technology includes developing strategic directions, implementing technology to support business goals, and providing competitive advantage. Typical efforts to organize the management of information technology include setting the appropriate priorities, budgeting appropriately to support technology advancements and compliance efforts, and aligning technology goals with the business strategic direction. IT management efforts also include responsibility for protecting the

data assets of the business, as well as leading businesses into new markets and realizing the potential of new technology capabilities (Kamsin, 2004). The challenge of effective information security management is to embrace significant technology advancements while protecting information security assets. Efforts to responsibly manage technology have positioned IT as the organization's change agent. However, the BYOD movement is disrupting the traditional role of IT management as the centralized expert in identifying and driving technology change.

Employees have embraced technology advancements in the form of high tech devices, user friendly apps, and cloud services in their personal lives, and are demanding the same capabilities in the workplace (Castro-Leon, 2014). The rapid adoption of smart devices combined with the explosion of solutions and apps available for these devices have resulted in powerful, user centric capabilities that have quickly outpaced the technology systems provided in most organizations. BYOD has effectively reversed roles, establishing employees as the technology change agents and putting IT in a reactionary role. IT management faces a critical decision: to resist BYOD to continue to exercise utmost control over the organization's technology, or to permit BYOD and become an enabler of highly advanced, decentralized solutions, while still demanding the protection of information security assets.

Traditional management considerations must be maintained despite the pervasive adoption of mobile devices and the global nature of Internet business. These include implementing robust and reliable technology platforms, reducing the likelihood of systems failure, and managing efforts to comply with global data protection regulations.

IT management must now include controls to mitigate the information security risks of BYOD and ensure compliance with policies, laws, and regulations. The number of employees and executives using their own personal devices at work is growing, and the number of malicious software attacks on smartphones has likewise increased (Drew, 2012).

Evolution of Information Security

Da Veiga and Eloff (2007) suggest that information security tactics have evolved through four phases: technology solutions, management support and structure, human considerations, and governance considerations. The ubiquitous nature of BYOD is causing an impact to every phase of information security.

The first phase of information security focused on the technical efforts to secure the confidentiality, integrity, and availability of information systems. To mitigate the information security risks of BYOD, technical controls are needed to protect the device against malicious software, encrypt data at rest and during transmission, and to filter data to stop sensitive data from reaching the mobile device. Additional technical controls may be utilized to remotely locate lost or stolen devices, remotely erase files to prevent unauthorized access, and sound an alarm if the owner is separated from the device. Vendors have quickly responded to provide technology solutions specifically for BYOD, such as mobile device management (MDM) and mobile application management (MAM), that are advancing rapidly to ensure the safety and identify the location of personal devices. However, these types of technical controls for BYOD can be ineffective, since executive management and other employees may be wary of programs

that could remotely erase all data, including personal data, from the device in the event of loss or theft. In addition, controls that monitor the location of the device can be seen as an invasion of privacy. BYOD will challenge currently held beliefs in strong policies and overarching controls that are simply not enforceable or desirable when dealing with personal devices.

The realization that information security was not solely a technology issue required a major shift to involve the support of management (Nolan, 2005). The second phase of information security efforts considered organizational structures and management involvement as critical elements in the effectiveness of information security. BYOD precariously pits support for information security against enthusiasm for the use of personal devices. Executives and CEOs are among those who look to BYOD for productivity gains and convenience of access to work related tasks. Executive management not only supports the use of BYOD within the organization, but is demanding it. While IT may acquiesce to this pressure to allow BYOD, they must enlist the support of executive management to ensure it is permitted securely. However, executive support for the implementation of information security controls must accompany their eagerness for the high tech capabilities of BYOD; it is critical to ensure the protection of information assets.

Through the first two phases of information security efforts, success continued to evade organizations, and the third phase of information security identified the human element as a significant threat to information security, and proposed that the value of information security must be accepted by the organizational culture to effectively

mitigate the risk (Nolan, 2005; Da Veiga & Eloff, 2007). The human aspect of BYOD programs is critical, as the device and its usage are in the hands of the owner. While using a personal device at work, the employee may have to agree with usage policies, accept that passwords or lock codes must be used on the device, comply with restrictions on public Wi-Fi connections, and agree to separate personal and work data. Motivating employees to comply with policies to ensure protection of information assets is a significant challenge and change for organizational culture. Implementing fair policies and appropriate controls is critical to achieving balance between the quest for information security and respect for personal property.

The challenge to achieve more acceptance of information security through a well-established culture called for a more comprehensive view of information security (Nolan, 2005). The fourth phase of information security proposed that information security should be integrated into corporate governance responsibilities to provide a holistic view of information security and ensure adequate protection of information (Entrust, 2004). Information security governance includes responsibility for risk management, accountability for adequate information security controls, and monitoring information security activities (Posthumus & Solms, 2004) and should take into account staff issues, such as leadership, culture, and structure (Dutta & McCrohan, 2002).

The final aspect of information security, governance, is perhaps the most impacting aspect of a BYOD program, since the organization will want to receive the benefits of employee productivity and satisfaction and business innovation, while still enforcing a culture of information security coupled with appropriate controls.

Successful BYOD programs require a significant adjustment to all four phases of information security tactics.

Device Specific Risk

Consumer devices that are used for work purposes were not designed with organizational information security in mind, and new malware that targets mobile devices is being introduced with increasing frequency (Romer, 2014). Because the devices are small and mobile, they are easy to misplace or forget. BYOD introduces significant risk when employees download personally identifiable information, confidential customer information, or proprietary business data, because the device can easily be stolen, lost, or compromised (Drew, 2012). BYOD programs must manage devices that are not organizationally owned to comply with a variety of regulations and business requirements (Taylor, 2013). Although technology solutions are available to manage data on mobile devices, policies and education are critical to the success of BYOD programs (Taylor). Strong usage policies that are monitored and enforced should require that employees separate personal mobile apps from business apps, use encryption when transmitting data, and prohibit the storage of sensitive information on a personal device (Banham, 2013). However, organizations risk securing data through unwieldy controls and absolute policies that are perceived as an intrusion of privacy and excessive controls on personal property.

ESG Research reports that in a study of 315 IT security professionals, nearly all are challenged with mobile device security (Oltsik, 2012). The most significant information security threats identified by these IT security professionals include

enforcing security policies, securing sensitive data on lost or stolen devices, protecting the confidentiality and privacy of sensitive data, managing threats, supporting new devices, and creating security policies (Oltsik).

Some types of sensitive data, such as credit card numbers, must be stored on well secured central servers and should never be accessed from external devices. Sensitive data that can be accessed via BYOD should be transmitted over encrypted connections, and should not be able to be saved on the device.

Multiple layers of security, such as access controls, virus and malware protection, and secure connections are necessary to safeguard personal devices from unauthorized access. Physical security restrictions should be implemented to ensure only authorized personnel can gain access to the data center and the information assets within. Unlike a physical data center that can be locked and monitored, personal mobile devices are beyond the control of an organization's physical security policy. These devices can be left unattended or momentarily ignored while the employee's attention is directed elsewhere, making them an easy target for theft and unauthorized access.

Managing threats to sensitive data includes removing all traces of that data once it becomes obsolete. A control may require the disposal of data and overwriting of the storage media to ensure the data has been obliterated. This control must be extended to include BYOD, and sufficient controls must be implemented to ensure the proper destruction of business data on personal mobile devices.

Risk Management

A critical element of information security is identifying and managing risk. Risk management includes the process of identifying, evaluating, and mitigating risks to an organization's systems and information (Whitman & Mattord, 2014). Information security risk is managed through adequate internal controls and a proactive approach to organizational threats (Harris, Kinkela, & Hayes, 2011). The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed frameworks and guidance on Enterprise Risk Management (ERM), internal controls, and fraud prevention. ERM is a systematic approach to effective risk identification and response, effective monitoring of operations, and a commitment to continuous improvement.

A risk assessment is necessary to evaluate key sources of risk and develop controls to reduce risk (Stephens, 2012). The need to protect data on internal systems from loss is obvious, and the fact that this data could be accessed and stored on a personal device or laptop cannot be ignored. Controls that protect data from being misused, lost, or stolen must be expanded to include appropriate provisions for BYOD.

Disaster is a prevalent risk that is managed by the organization. The need to handle sensitive customer data securely and ensure that its integrity, confidentiality, and availability to authorized access is of utmost importance. This responsibility must also be carefully considered as an organization implements a BYOD program. A disaster is generally associated with a major disruption of critical systems, however, the prevalence of BYOD for time sensitive operations introduces the risk that employees will be unable

to perform work activities if the device is lost, stolen, or unable to connect to organizational systems.

Information Security Policy

Before allowing personal devices to have access to the organizational network, resources, and services, a comprehensive set of policies and procedures are needed to define the terms and conditions of a BYOD program (Armando, Costa, Merlo, & Verderame, 2015; Taylor, 2013). Greengard (2014) states that organizations have insufficient or a complete lack of BYOD policies, and there is a critical need for policies to protect against security risks. According to Johnson and DeLaGrange (2012), 97% of organizations believe that BYOD policies are important, yet 36% of organizations lack a formal BYOD policy. Girard (2013) suggests that the number one reason for mobile security failures are inconsistent security policies, which often define specific device requirements instead of broad information security requirements.

Taylor (2013) suggests that compliance with information security policies is a tough challenge, and can be enhanced with appropriate programs to motivate employees through incentives, disincentives, compliance tactics, and ongoing communication. In addition to acceptable use policies, mobile devices should be subject to rules that delineate legal actions for the device (Armando, Costa, Merlo, Verderame, 2014).

Difilipo (2013) questions whether more policy is an attempt by IT to control, restrict, and lock down access in an environment where they have clearly lost the ability to control. Consumerization has put the individual employee in control of the device they use, which services they desire, and the wide open Internet of Things (IoT) that are

at their disposal. Additionally, rapidly changing devices, operating systems, and carrier features further complicate attempts to adopt standard devices. Although restricting the device to demonstrate control is not the answer, addressing the challenges of BYOD through sensible policy is. BYOD policy cannot be overly prescriptive; it must be broad enough to allow for emerging technology and future services, while at the same time it must be detailed enough to enforce (Difilipo).

Vignesh and Asha (2015) state that most BYOD policies are "vague and generally immature", and go on to suggest that general information security policies do not adequately address security concerns of mobile devices. An effective BYOD policy will include organization, application, and device level policies to protect organization assets while not infringing on employee productivity (Vignesh & Asha).

Policy development requires costly investment in resources to create, review, edit, approve, and communicate formal policy documents, as well as the subsequent investment to enforce the requirements and sanction the offenders. Despite the significant investment, policies are only moderately effective in controlling BYOD usage since the employee may think they are abiding by specific usage policies only to find that policy has been violated by two applications that work together to gain prohibited access to the device (Armando, Costa, Merlo, & Verderame, 2015). Without a thorough understanding of the underlying capabilities of an application, as well as its relationship to other installed applications, it is impossible to be certain that compliance has been achieved. The organization must ensure the protection of data in spite of these

challenges; therefore BYOD usage policies are most effective when enforced automatically.

The organization should define the rules of permissible behavior for BYOD and establish security mechanisms on the device to enforce usage policies to ensure the protection of the organization's networks, systems, and data. Loss of data is the most significant threat of BYOD, and usage policies must be established that require the separation of personal and business data, encryption of data, and prohibit the storage of sensitive data on personal devices (Armando, Costa, Verdame, & Merlo, 2014).

According to Armando, Costa, Merlo, and Verderame (2015), the security capabilities of the personal devices are inadequate against information security threats. IT is responsible for protecting the confidentiality and integrity of the organization's information assets, and must establish appropriate policy that can be enforced on the mobile devices. Armando, et al. (2014) propose that a formal security framework must define and enforce BYOD security policy automatically to prevent malicious applications from being installed on BYOD enabled devices. Greengard (2014) suggests that mobile device security is mandatory on every BYOD device, and must include password protection and data wipe capabilities.

The organization must be intentional in enforcing usage policies, such as what data is permitted on the device, if and how it is stored, and physical security of the device. Other automated policy enforcement must include validation of applications before they are installed to detect malicious behavior and verification of device configuration changes to ensure compliance with BYOD policy. For automated BYOD

policy enforcement to be successful, the user experience on their personal device should not be affected (Armando, Costa, Merlo, & Verderame).

The development of information security policies and controls can be assisted by the availability of information security standards, and the necessity demanded by information security regulations.

Standards-based Information Security

A variety of information security standards have been developed to identify best practice information security processes and provide implementation, management, procurement, and assurance guidelines. The International Organization for Standardization (ISO/IEC) 17799/27002, US National Institute of Information Standards and Technology (NIST), Control Objectives for Information and related Technology (COBIT), and Information Technology Infrastructure Library (ITIL) are a few of the recognized information security standards (Clark, 2009). Information security standards include requirements to ensure compliance with the many laws and regulations developed to protect systems and information against the increasing number of information security threats. These standards span the broad spectrum of complex information security initiatives, providing general guidelines for the identification of security strategy through the assessment of the effectiveness and maturity level of information security processes. The information security standards recommend robust practices, including the following components applicable to compliance: data must be used for authorized purposes only; database privileges must be restricted to appropriate job duty requirements; and, data must be protected according to legislation requirements.

Information security standards recognize the importance of information security policies for successful IT security management (Baskerville & Siponen, 2002).

Obviously, utilizing information security standards to identify applicable internal controls provides immense benefit. The information security standards provide an enormous advantage in its collection and supporting detail of well-defined best. On the other hand, the comprehensive approach of information security standards may not be able to keep pace with the quickly advancing capabilities of BYOD.

Information Security Regulations

The importance of information security has become more apparent with the increase in breaches of personal information, illegal corporate activities, and other cybercrimes. Individuals feel specific concerns for the protection of their private information, and self-regulation by corporations to adequately protect sensitive information has fallen short. The government has responded by creating a series of regulations and standards that address the high profile industries, including financial institutions, healthcare, and educational institutions. In addition, current regulations are being developed to address the overall standards for information security, verified by Security and Exchange Commission (SEC) security audits (Swibel, 2004).

Effective information technology (IT) governance is mandated by a variety of laws and regulations, including the Sarbanes-Oxley Act of 2002 (SOX), the Health Insurance Portability and Accountability Act (HIPAA), state notification laws (such as CA 1786), the Payment Card Industry data security standard (PCI DSS), Gramm-Leach-Bliley Act of 1999 (GLBA), and the Family Educational Rights and Privacy Act of 1974

(FERPA), that have been enacted in response to organizations that falsified financial information or that experienced an information security breach resulting in the compromise of sensitive customer information (Gudivada & Nandigam, 2009). Meeting compliance requirements is of utmost importance to ensure that sensitive data is protected, privacy is ensured, and adequate controls are in place to prevent and detect illegal activities.

Federal laws and regulations, such as FERPA and GLBA, protect student educational records and personally identifiable information (PII). SOX applies to all publicly traded companies and requires significant change to corporate governance, including satisfactory control and monitoring of financial reporting (Beeler, George, & Gardner, 2006). The SOX, HIPAA, FERPA, and GLBA regulations address similar concepts of protecting sensitive data and ensuring privacy of records. These concepts are stated in terms of functionality, and do not address specific information security measures that should be used to accomplish the control, but rather indicate that "appropriate" internal controls should be used (Adler, 2006). Adler suggests that the collective information security and privacy laws and regulations will contribute to an emerging legal standard to which compliance can best be attained with a unified approach. Organizations are beginning to approach compliance as a strategic initiative that affects the entire enterprise (Gudivada & Nandigam, 2009).

In addition to the organization's priorities for protecting sensitive business data, an organization must consider all aspects of complying with laws and regulations that demand protection of personal information, privacy, or copyright. Non-compliance with

associated regulations is subject to fines and penalties, not to mention the intangible damages to reputation or trust. Compliance with increasingly strict laws and regulations, and keeping pace with constantly changing security threats requires diligent evaluation and continual improvement to security processes.

Compliance regulations include common requirements for effective policies and adequate internal controls to protect information, as well as for established response and remediation procedures to ensure timely and appropriate actions in response to information security incidents (Coggrave, 2012). In the event of an incident, internal controls must include the seizure and protection of digital evidence, which is difficult, if not impossible to enact when BYOD programs allow access, processing, and storage of data on a personal mobile device. If confidential data is breached, how can an organization provide evidence regarding the storage and processing of data on a personal device?

Information Security Governance

The success of an organization depends on information that is secure, accurate, reliable, and is available when needed by the appropriate person (Korac-Kakabadse & Kakabadse, 2001). This mission critical dependence on information that is effectively captured, stored, and managed by technology requires a successful information security strategy (Van Grembergen et al., 2004) that is monitored and controlled by effective information security governance. Because of the pervasive use of technology in the knowledge-based economy, business information is exposed to a growing network of

technology, people, and processes (Posthumus & Solms, 2004) in an open environment that extends across commercial, geographic, and political borders (Foley, 2009).

Information security is a corporate governance responsibility, because information security involves strategic and legal issues (Posthumus & Solms, 2004) and must be a priority for the entire organization (Corporate Governance Task Force, 2004; Khoo et al., 2010). Information security governance directs and manages effective information security in support of business strategy, compliance with laws and regulations, and avoidance of disruptions to business operations (Posthumus & Solms, 2004). Effective information security governance is a delicate balance between absolute protection of data and ensuring the business can achieve its objectives.

The board of directors has authority over information security due to recent legislation and codes of conduct, and must exercise responsible governance (McFadzean et al., 2006). The board of trustees and executives are charged with overseeing information security and, at the same time, are demanding the ability to work on their personal devices. Governance of information security on BYOD is a conundrum of information security, personal preference, and perceived overreach of business on the personal device.

Internal Controls

Because organizations have a critical dependence on information and technology, information security controls must be implemented to protect against disruptions due to external and internal threats. Ensuring the information security of an organization involves protecting the confidentiality, integrity, and availability of the data and systems

that are subject to an increasing number of computer abuses and disasters (Sonnenreich, Albanese, & Stout, 2006; Straub & Welke, 1998). The protection of organizational assets is a key priority, and the constantly changing, increasingly complex, and progressively pervasive information technology environment makes this all the more difficult (McFadzean et al., 2006; Sanchez et al., 2006). One significant threat introduced by BYOD is the loss or theft of sensitive customer or business data (Banham, 2013) because the devices are small and portable, and more likely to be lost or stolen (Eisenberg et al., 2014). Other substantial threats are presented by the spam encountered on common social sites, which can lead to malware, viruses, and granting of excessive permissions to the device (Earley et al., 2014).

Internal controls have been mandated by multiple laws and regulations to provide reasonable assurance concerning the reliability and integrity of information systems and business processes (Harris, Kinkela, & Hayes, 2012). Early internal controls focused on processes and procedures for handling data, and relied on independent and objective validation that processes and procedures for handling accounting records were not subject to negligence or fraud. With the introduction of computers, internal controls evolved to a much more complicated effort of validating inputs, processing, and outputs of automated financial management systems. The advent of the many laws and regulations pertaining to accounting records and information privacy resulted in specific legal requirements for satisfactory internal controls. The objective of an internal control function of an organization is to ensure the business operations are efficient and effective, data is accurate and reliable, and operations comply with laws and regulations. Weak internal

controls leave data vulnerable to internal misuse and unauthorized activities (Allen, 2008), and organizations are responsible for implementing internal controls that meet the minimum regulation compliance to ensure that an organization's business practices abide by relevant regulations and laws (Rosario, Pereira, & Silva, 2012).

Identifying and implementing effective internal controls will assure that business processes meet all compliance requirements. A successful information security management system must be periodically checked to assure that the desired controls are maintained. Operational data and results of the information security processes must be audited and adjusted to improve the effectiveness. Audit is the periodic activity performed by an independent party, usually an internal control professional, to assess the risk, governance, and alignment with policy and controls of a business process (Rosario, Pereira, & Silva, 2012).

Harris, Kinkela, and Hayes (2011) suggest that the root cause of potential risks must be identified, and controls implemented to reduce the risk of the triggering event. The first challenge for identifying reasonable internal controls for BYOD is identifying the applicable risks and the appropriate controls to meet compliance requirements. Information security standards provide guidance, but contain a more rigorous security regiment than would be needed at any one organization, defining information security best practices for all organizations and operating environments at a high level, without specifying a particular technology solution, identifying which components are most important, or providing measurements to assess the effectiveness of information security practices (Drugescu & Etges, 2006).

The achievement of effective IT controls for BYOD compliance involves identifying and implementing appropriate information security processes, effective monitoring of security levels, and utilizing appropriate criteria to test information security effectiveness. An effective BYOD policy should exist and compliance should be enforced, device security controls must be established and controlled over the various types of BYOD devices (Semer, 2013).

Summary

Information security has evolved through various approaches to assure data and systems are protected from internal and external threats. Due to the ever changing and sophisticated nature of malevolent attacks, information security efforts are constantly evolving and adjusting. The BYOD phenomenon has introduced novel challenges to information security that could be the most difficult challenge yet. In order to realize the benefits of BYOD, organizations must successfully assess and mitigate the information security risks

A clear understanding of the risk associated with BYOD will result in better decision making, identification of proper controls to meet compliance requirements, reduced information security failure and losses, and more efficient work processes. In addition, properly implemented BYOD program controls will result in an improved work environment, with less crisis management and a more organized, proactive approach.

Chapter 3

Methodology

Overview

This chapter identifies the approach that was used for the research study, explains the instrument design and validation, and describes the study participants. The approach used for data analysis is identified and the resource requirements are explained.

Research Methodology

Due to the prevalence of BYOD and the lack of prior research, this study used exploratory research to investigate how widely the use of BYOD is permitted in organizations, identified effective approaches that were used in making the decision, and identified the factors that were influential in the decision making process. Exploratory research was appropriate for this study, since there was little existing literature available on the adoption of BYOD. Exploratory research was suitable to establish initial research in the problem area which can be used for future research (Singh, 2007). This study of BYOD created a foundation for future research efforts.

Exploratory research utilizes available literature, data, and formal data collection methods. This research was carried out in three stages: instrument development and validation, data collection, and data analysis as shown in Figure 1.

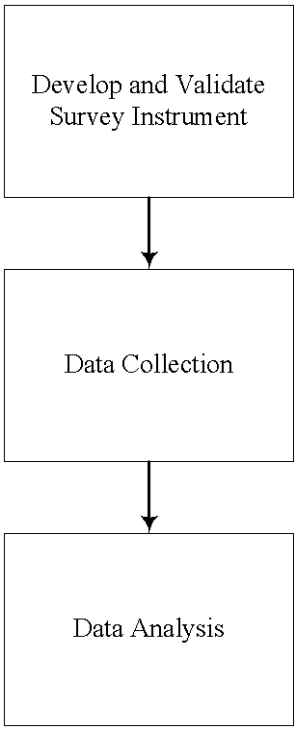


Figure 1. Phases of Research

Instrument Development and Validation

In the first stage of research, the survey instrument was developed. The research began with a review of existing literature and trade magazines related to BYOD and internal controls. Using data from these sources, typical methods, factors, and risks associated with the adoption of BYOD were defined for each question. The survey was developed based on the methodology for construct development in MIS research developed by Lewis, Templeton, and Byrd (2005), which enhanced Churchill's standard for instrument development (Churchill, 1979) and was successfully tested for use in MIS research. This comprehensive methodology has been used completely in several MIS studies and partially in a number of others (Lewis, Templeton, & Byrd, 2005). The

development of the instrument was followed by the appropriate methods to ensure its validity and reliability.

The survey instrument was developed to communicate the questions clearly, yet was concise and simple to ensure ease of response (Dolnicar, 2003). To determine what specific methods, factors, and controls were associated with the decision to permit BYOD, closed-end questions with a fixed set of answers (yes/no/unknown) were used. Based on the initial response to the question of permitting BYOD, the question path branched to collect data relevant to the decision. The survey question flow is shown in Appendix A.

The survey instrument was constructed to be very clear as to the intent and scope of each question. The domain definition was developed to successfully establish the use of BYOD and identify effective approaches, significant factors, and specific information security concerns. The domain definition included a formal statement and purpose for the study, a description of what the study involved, and a description of what the study did not include (Lewis, Templeton, & Byrd, 2005). The elements of the study, or dimensions, were further identified in the area of demographics, permitted use of BYOD, decision making approach, and factors. This study explored how widely BYOD was permitted in organizations, the approaches that were used in the decision making process, the factors that affected a company's willingness to support BYOD, and the specific information security risks that were associated with a BYOD program.

The survey instrument was developed by identifying important decision making methods, factors, and specific information security concerns. Each research question was

thoroughly investigated through a series of corresponding items on the survey. Grassi, Nucera, Zanolin, Omenaas, Anto, and Leynaert (2007) compared the use of binary and Likert scales in their research with health administrators, and concluded that a binary scale reduced the time required to take the survey, while maintaining validity of the instrument. Dolnicar, Grün, and Leisch (2011) found that surveys using binary scales were simpler and quicker to complete, which may reduce non-response bias.

To ensure validity and reliability, an expert panel of 10 members of the Institute for Internal Controls was selected to evaluate the survey instrument. Members of the Institute for Internal Controls are certified in internal controls and most hold the Certified Internal Controls Auditor (CICA) credential. The members represent a wide range of audit job titles, including internal auditor, external auditor, compliance auditor, fraud auditor or examiner, and consultant. Other internal control professions include accounting professionals, loss prevention professionals, and IT professionals.

The expert panel reviewed each question on the preliminary survey instrument, and indicated if each question was essential, important, or not relevant. The preliminary survey instrument is available in Appendix B. The expert panel was asked for feedback on the presentation, content, clarity, terminology, and usability of each question, as well as the entire instrument. The expert panel indicated that the survey covered the full breadth of content (sampling validity) and that each question measured what it intended to measure (item validity). The survey questions were all validated as essential or important, therefore no questions were removed.

Based on the results of the expert panel, two additional questions were added to the final questionnaire: Were auditors/internal audit involved in the evaluation process for BYOD? and, Was a legal review part of the decision-making process for BYOD? In addition, minor tweaks were made to improve the survey flow and improve the collection of "other" comments. To improve usability, the flow was altered to allow navigation back, although it was not possible to navigate back past the branch that split the response for BYOD allowed. Minor tweaks were made to allow entry of other comments without having to select Other = yes. Minor clarifying language was added to a few of the options.

The content validity of the survey instrument was measured in several ways. Any questions identified as not relevant would be removed from the instrument using the content validity ratio (CVR) formula: $CVR = (n – N/2) / (N/2)$ where N is the number of internal control professionals and n is the number of 'not relevant' ratings. Lawshe (1975) recommended using only essential ratings, however, Lewis, Templeton, and Byrd (2005) justify essential and important as both positive measures of the item. All survey questions were rated as essential or important; therefore no survey questions were removed. Based on the feedback from the expert panel, instrument validity was considered high and the final survey instrument was ready for distribution. The final survey instrument is available in Appendix C.

Data Collection

The final survey instrument was created in online survey software and invitations were delivered via email only, based on the results of Porter and Whitcomb's (2007)

mixed mode contact study, which concluded that paper pre-notifications and reminders did not significantly increase response to the email survey request. An email pre-notification and several email reminders were utilized to improve response rates (Fox, Crask, & Kim, 1988; Schaefer & Dillman, 1998).

Participation from members of the Institute for Internal Controls (IIC) was requested. These members are certified internal control professionals, and most are also Certified Internal Controls Auditors (CICA). The IIC has 5,000 members that represent all industries as well as government agencies. All of these internal control professionals were targeted by this study to include a diverse population of organizations that have implemented or considered implementation of a BYOD program. The final survey instrument was issued to all of approximately 5,000 members via trusted IIC email channels, to improve the rate of response. The IIC members were invited by email to participate in the voluntary research study, and were provided with a Universal Resource Locator (URL) to access the Internet-based survey. The participant invitation to participate in the research study is presented in Appendix D.

Since the survey instrument required the participation of human subjects, the instrument was reviewed and approved by Nova Southeastern University's Institutional Review Board (IRB) prior to beginning the study. The approval letter is included in Appendix E.

Data Analysis

The response quality was assessed by verifying that the response rate from the initial sample exceeded the approximately 20% as suggested by Malhotra and Grover

(1998). Schuldt and Totten (1994) note that 19.3% is an effective response rate for email surveys, although Porter and Whitcomb (2003) reached a response rate of only 17.5% after employing various techniques to improve the response rate. The survey participation request was opened by 1,688 potential respondents, and 663 total responses were received for a response rate of 39%.

Validity of the responses was tested to ensure the data was valid and useful. Tests were conducted for missing data and response set bias, and offending responses were removed from the sample so that only complete responses remained.

Determining reliability is essential in the research process to determine that items have an acceptable level of consistency. The most common measure of reliability is Cronbach's Alpha (Mertler & Vannatta, 2013). Cronbach's Alpha was calculated to verify that the items were consistent in measuring the same underlying concept. The responses in the survey raw data were numeric: 1 = "Yes", 2 = "No", and 3 = "Unknown". Additionally, the survey contained a branch at the item "Does your organization currently allow the use of BYOD?" Because of the branch, the survey items for BYOD Allowed = "Yes" and BYOD Allowed = "No" were separate, even though the constructs they measured were similar. To accommodate for the branch which resulted in separate responses, Cronbach's Alpha was calculated for items measuring approach, factors, security controls, and security concerns for both branches. Cronbach's Alpha > .7 is considered an acceptable measure of shared covariance of items. As indicated in Table 1, Cronbach's Alpha exceeded .7 for all of the items in total and by concept for each branch of the survey.

Table 1. Cronbach's Alpha Goodness of Fit Findings

BYOD Allowed	Concept	Cronbach's Alpha	Number of Items
Yes	Approach	.841	6
	Factors	.705	4
	Security Controls	.919	17
	Security Concerns	.933	11
	All	.934	38
No	Approach	.837	6
	Factors	.834	5
	Security Concerns	.929	11
	All	.895	22

Goodness of fit was conducted using the expected value of 44% for BYOD allowed, based on the findings of Tech Pro Research (2013), which reported that 44% of survey respondents allowed BYOD. Using one degree of freedom, the ratio of Chi-Square was calculated at 2.606. Since the critical Chi-Square for p=.05 is 3.84, this indicates that there is no statistical difference in proportion of BYOD allowed responses in this study. According to these results, shown in Table 2, this study was considered a good fit.

Table 2: Goodness of Fit Statistics

	Observed N	Expected N	Residual
Yes	181	198.0	-17.0
No	269	252.0	17.0
Total	450		

	Frequency
Chi-Square	2.606[a]
df	1
Asymp. Sig.	.106

Resource Requirements

Members of the Institute for Internal Controls are certified in internal controls and represent a diverse selection of organizations in all industries and government agencies. Most of them hold the Certified Internal Controls Auditor (CICA) credential. The members represent a wide range of audit job titles, including internal auditor, external auditor, compliance auditor, fraud auditor or examiner, and consultant. Other internal control professions include accounting professionals, loss prevention professionals, and IT professionals. It was required that a sufficient number of these members are in organizations that permit the use of BYOD.

The research relied on the online Qualtrics Survey Software and IIC member email to distribute the survey instrument and collect responses. A statistical analysis program was used to analyze the results.

Summary

Due to limited research in the area of BYOD adoption, this research study used exploratory research to answer the research questions of how widely the use of BYOD is permitted in organizations, what approaches were used in making the decision, and which factors were influential in the decision making process. Data was collected using a survey instrument that was developed based on current literature findings, tested with a small sample of experts, and validated with the appropriate methods to ensure its validity and reliability. The survey was disseminated through IIC email channels to a total of 1,688 certified internal control professionals that opened the email, resulting in 663 total responses. The Chi-Square goodness of fit was calculated at 2.606, indicating that the

model measures BYOD Allowed within the expected value. Cronbach's Alpha was calculated to verify that all of the survey concepts were consistent in measuring the same underlying concept, and all results exceeded .7, which indicates that the survey is consistent in measuring the concepts.

Chapter 4

Results

Introduction

This chapter details the data collection, analysis of responses, and results of the research study. The statistical method used for data analysis is identified and the overall results are explained. First, the results of the survey evaluation by an expert panel are discussed and data collection details are reviewed, followed by the details of the methods used to analyze the data, and then the results are presented.

Data Collection

The survey instrument was developed to communicate the questions clearly, while at the same time being concise and simple to ensure ease of response (Dolnicar, 2003). Based on the initial response to the question of permitting BYOD, the question path forked to collect data relevant to the decision. To determine what specific methods, factors, and controls were associated with the decision to permit BYOD, closed-end questions with a fixed set of answers (yes/no/unknown) were used.

Expert Panel

To ensure validity and reliability, an expert panel of 10 members of the Institute for Internal Controls was selected to evaluate the survey instrument. The expert panel

was asked to review the survey instrument and indicate if the survey covered the full breadth of content (sampling validity) and if each question measured what it intended to measure (item validity). In addition, the expert panel was asked for feedback on the presentation, content, clarity, terminology, and usability of the instrument. One expert participated in the survey review, indicating that all questions were essential or important. Feedback was provided that two additional questions, legal review and internal auditor involvement in the evaluation, should be added to the survey in the approach section. In addition, minor tweaks were suggested for the survey flow and the presentation of "other" comments. As a result, the survey was updated to include the two new questions and the flow was altered to allow navigation back, although it was not possible to navigate back past the branch that split the response for BYOD allowed. Minor tweaks were made to streamline the handling of "other" comments and minor adjustments were made to clarify technical terminology. The final survey was published and disseminated to the IIC email channel for data collection.

Survey Responses

The email request was issued on November 15, 2016 and data collection continued until December 12, 2016. The initial request, sent by the Chairman of the IIC, invited members to access and complete the online survey. Due to anti-spam filters and firewall settings, the email request was not delivered to 1,126 of the members. Using the IIC email tool, it was determined that of the 6,681 emails that were sent, 1,688 successfully reached and were viewed by active members. During the data collection period, two reminder emails were sent which resulted in increased response activity. Of

the 1,688 potential respondents, 663 total responses were received for a response rate of 39%.

Data Preparation

Before testing the data, pre-analysis data screening was conducted to ensure the data was valid and useful. The responses were downloaded from the Qualtrics Survey Software website in SPSS format with actual values. This format was preferred for ease of analysis with the statistics tool. The survey instrument required item reversal for one question that was negatively worded. When the BYOD Allowed response was "Yes", the participants were presented with "Did the risk assessment indicate that BYOD would not increase the vulnerability of the organization?" whereas if BYOD Allowed was "No", then the participants were presented with "Did the risk assessment indicate that BYOD would increase the vulnerability of the organization?" Item reversal was performed on the negatively worded item for BYOD is "Yes". During data screen, tests were conducted for missing data and response set bias.

Missing Data

The construction of the survey enforced entry of an answer for required questions. The only responses with missing data were those that had been started and not completed. It was determined that 162 responses were started but not completed, resulting in 501 complete responses.

Response Set Bias

Response set bias occurs when respondents select the same answer throughout the entire survey. Response set bias was identified by visually inspecting the data. A total of 51 cases of response set bias were detected, and these responses were made up of all "Yes" or all "Unknown" answers. The surveys with response set bias are identified in Table 3. After the response set surveys were removed, 450 responses remained for further analysis.

Table 3: Response Set Bias

BYOD	Result Sets	Survey Number
Yes	All Yes	47, 308, 408
No	All Yes	13, 134, 181, 185, 205, 265, 336, 421, 422, 438, 450, 456, 488, 489, 492, 495
No	All Unknown	2,33, 72, 75, 103, 147, 162, 166, 230, 243, 245, 262, 276, 283, 294, 300, 301, 313, 323, 375, 380, 387, 393, 399, 403, 429, 444, 449, 453, 460, 463, 467

The Qualtrics "anonymous" setting ensured that IP address, email address, and other personal identifying data was not collected during response. Thus, all responses for the identifying data were constant (Status = "IP Address", Progress = "100", Finished = "True", and Distribution Channel = "anonymous".) Therefore, these variables were removed from the response set.

Demographic Findings

A total of 213 problematic responses were removed during the pre-analysis data screening, leaving 450 responses for analysis.

As shown in Table 4, nearly 60% of respondents represent organizations that do not permit BYOD. The rate of 40.2% of respondents from organizations that currently do permit BYOD is consistent with the findings of Tech Pro Research (2013), which reported 44% of survey respondents allowed BYOD.

Table 4: Use of BYOD Distribution

		Frequency	Percentage
Does your organization currently allow the use of BYOD?	Yes	181	40.2
	No	269	59.8

The research responses were classified into two categories: allowed BYOD and did not allow BYOD. The Chi-Square test of independence was used throughout the data analysis phase to establish significant relationships between these two categories of responses and the other variables in the survey, and was appropriate for the nominal data collected by this survey. An alpha of .05 was used for this study and the dependent variable was BYOD Allowed.

The Chi-Square test of independence results for the general demographics with these categories revealed that there are no significant statistical differences in demographics (Table 5) between organizations that allowed BYOD and those that did not. The descriptive statistics for demographics of the BYOD categories are shown in Appendix F.

Table 5. Chi-Square Test of Independence for Demographics for BYOD Categories

Item	Pearson Chi-Square	Critical Value	df
Title/Role	4.398	9.488	4
Primary Business Activity	21.251	24.996	15
Number of Employees	5.652	7.815	3
Conduct Business	1.629	5.991	2

As shown in Table 6, 76.9% of respondents selected from the provided title/role options, with the majority falling into the title/role of Internal Auditor. Since the second largest response was "Other", with 104 responses, the data was visually inspected for significant title/roles. The data contained title/roles related to compliance, internal control, manager, and director; however, all 104 of the "Other" responses were unique title/roles.

Table 6: Title/Role Distribution

	Frequency	Percentage
Internal Auditor	218	48.4
Other	104	23.1
Accountant	47	10.4
Consultant	45	10.0
External Auditor	36	8.0

As shown in Table 7, the majority (49.3%) of the respondents were from organizations with over 1,500 employees, while the remaining responses were distributed fairly evenly among the other choices (Under 100, 100 to 499, and 500 to 1,500).

Table 7: Size of Organization Distribution

	Frequency	Percentage
Under 100	71	15.8
100 to 499	85	18.9
500 to 1500	72	16.0
Over 1500	222	49.3

As shown in Table 8, the majority of the organizations represented conducted their business operations domestically (63.3%), and one response to this question was missing.

Table 8: Business Operations Distribution

	Frequency	Percentage
Domestically	285	63.3
Globally	164	36.4
Missing	1	.2

The top four business activities (Financial Services/Insurance, State/Local Government, Federal Government, and Business/Professional Services) accounted for 61.3% of responses. Because the selection "Other" comprised 9.8% of the responses, the responses were visually inspected for significant occurrences of business activities. Five entries were related to financial services/insurance, and correction of these entries brought the frequency of "Financial services/insurance" to 125 and the frequency to 27.8%. Seven "Other" responses were related to "Utilities" (Oil and gas, nuclear power), and correction of these entries brought the frequency for "Utilities" to 21 and the percentage to 4.7%. Three additional "Other" responses related to "Business/professional

services" were corrected, as well as two "Other" responses related to "Retail/wholesale" and one "Other" response related to "Technology". The result of these corrections lowered the "Other" category to a frequency of 26 and a percentage of 5.8%. The top four business activities accounted for 63.1% as a result of the corrections. The distribution of corrected business activities is shown in Table 9.

Table 9: Primary Business Activity Distribution

	Frequency	Percentage
Financial Services/Insurance	125	27.8
State/Local Government	58	12.9
Federal Government	51	11.3
Business/Professional Services	50	11.1
Education	33	7.3
Other	26	5.8
Healthcare	23	5.1
Manufacturing	21	4.7
Utilities	21	4.7
Retail/Wholesale	13	2.9
Construction/Architecture	7	1.6
Technology	7	1.6
Consumer Products/Goods	5	1.1
Telecommunications	5	1.1
Agriculture/Forestry	3	.7
Entertainment/Recreation	2	.4

Data Analysis

Descriptive statistics are shown in Appendix G for approaches used in the decision making process for BYOD. Six questions were utilized to determine the decision making approach for BYOD, although the questions were phrased slightly differently based on whether the organization permitted BYOD or not in order to provide

clear instructions. The essence of the six questions for the approach to decision making was the same.

Comparison of the descriptive data for the approach to decision making indicates that conducting a risk assessment, involving management, following a formal process, and performing a legal review had a higher percentage of “Yes” answers than “No” answers for both organizations that allow BYOD and those that do not. Further, involving auditors/internal audit in the evaluation process and involving auditors/internal audit in the decision-making process had a higher percentage of “No” answers than “Yes” answers for both organizations that allow BYOD and those that do not.

Table 10 shows that the Chi-Square values for four of the six approaches exceed the critical value, indicating that these four approaches were significantly related to the decision to allow BYOD. Significant approaches include conducting a formal risk assessment, involving management in the decision-making process, following a formal decision making process and conducting a legal review. Organizations that allow BYOD were significantly more likely to utilize these four approaches in the decision to allow BYOD. Further, for both organizations that allow BYOD and those that do not, there was consistency in not involving auditors/internal audit in the evaluation or the decision making process.

Table 10. Chi-Square Test of Independence for BYOD Approach

Item	Pearson Chi-Square	Critical Value	df
Was a formal risk assessment conducted to prepare for BYOD?	23.177	5.991	2
Was management involved in the decision-making process for BYOD?	10.866	5.991	2
Were auditors/internal audit involved in the evaluation process for BYOD?	2.841	5.991	2
Were auditors/internal audit involved in the decision-making process for BYOD?	2.267	5.991	2
Was a formal decision making process followed?	15.552	5.991	2
Was a legal review part of the decision-making process for BYOD?	7.532	5.991	2
Did the risk assessment indicate that BYOD would not increase the vulnerability of the organization?	92.722	7.815	3

Additionally, the Chi-Square value for risk assessment results exceeds the critical value, indicating that the risk assessment results are significantly different for organizations that allow BYOD and those that do not. As shown in Table 11, the majority of organizations that conducted a risk assessment to evaluate the risks of BYOD found that BYOD would increase the vulnerability of the organization. For the organizations that did allow BYOD and conducted a risk assessment to prepare for BYOD, 46.3% of the risk assessments indicated that BYOD would increase the vulnerability of the organization; whereas a significantly higher percentage (88.6%) of organizations that do not permit BYOD responded that the risk assessment indicated that BYOD would increase the vulnerability of the organization.

Table 11. Risk Assessment Results

Did the risk assessment indicate that BYOD would increase the vulnerability of the organization?	Yes	No	Unknown
BYOD Currently Permitted	46.3%	26.3%	27.4%
BYOD Currently Not Permitted	88.6%	3.8%	7.6%

The descriptive statistics for the significant factors for a BYOD decision are shown in Appendix H. Four factors were presented when Allow BYOD was "Yes", and five factors were presented when Allow BYOD was "No". Three of these variables were the same for both categories of BYOD Allowed: management support, auditors/internal audit support, and the capabilities of cloud vendor solutions. For the common variables, the percentage of "Yes" answers was higher for both organizations that allow BYOD and those that do not.

For organizations that allow BYOD, 80.7% of participants indicated that management supported the decision to allow BYOD. In addition, organizations that allowed BYOD were highly influenced (64.01%) by the advanced capabilities of mobile devices, and 37.6% were influenced by the capabilities of cloud vendor solutions or apps, such as Salesforce or Workday.

For organizations that did not allow BYOD, 68.8% indicated that management supported the decision to reject BYOD and 65.4% were influenced by information and data security concerns. In addition, 57.6% were influenced to reject BYOD due to the concerns of securing and managing personal mobile devices.

Survey responses indicated that auditors/internal audit did not support the BYOD decision in only 18.8% of organizations that allowed BYOD and 14.9% of organizations that did not allow BYOD. However, for both organizations that allowed BYOD and those that did not, the highest response rate for auditors/internal audit support was Unknown (43.6% and 44.6%). Of the organizations that did not respond "Unknown", 67.6% of organizations that allowed BYOD and 73.1% of organizations that did not allow BYOD indicated that auditors/internal audit supported the BYOD decision.

As shown in Table 12, the Chi-Square results indicate that two of the three common factors were significantly related to the decision to permit BYOD: management support of the decision and the capabilities of cloud vendor solutions. A much higher percentage of organizations that allowed BYOD had management support of the decision, and organizations that did not allow BYOD had a much higher Unknown response (47.2%) for the influence of cloud vendor solutions.

Table 12. Chi-Square Test of Independence for BYOD Significant Factors

Item	Pearson Chi-Square	Critical Value	df
Did management support the decision to allow BYOD?	8.984	5.991	2
Did the auditors/internal audit support the decision to allow BYOD?	1.271	5.991	2
Was the decision to permit BYOD influenced by the capabilities of cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	12.994	5.991	2

The descriptive statistics for the information security controls that are in use for organizations that allow BYOD are shown in Appendix I. All of these variables were presented only to organizations that allow BYOD for the purpose of identifying successful information security controls for those organizations that are considering BYOD.

The use of information security controls does not represent effectiveness against threats, so the information security controls were evaluated in the context of a security breach occurrence. As shown in Appendix J, the Chi-Square test of independence was used to identify which information security controls in use were significantly related to the (lack of) occurrence of an information security breach in the organization due to BYOD. All of the information security controls that were identified during the literature review and included in the survey were identified as significant, as indicated by Chi-Square values that exceed the critical value.

As shown in Table 13, responses that indicted that it was unknown if a risk assessment was conducted had the lowest percentage of known security breaches (7.7%). Organizations that did not conduct a risk assessment had the highest percentage of "No" responses for security breaches (61.7%). The highest response overall (45.3%) was that it was unknown if there was an information security breach due to BYOD, and overall only 12.2% of organizations that allow BYOD acknowledged that an information security breach had occurred.

Table 13. Information Security Breach Occurrence

Have there been any information security breaches at your organization due to BYOD?	Yes	No	Unknown
Risk Assessment Conducted – No	12.8%	61.7%	25.5%
Risk Assessment Conducted – Unknown	7.7%	25.6%	66.7%
Risk Assessment Conducted – Yes, Vulnerability Not Indicated	11.4%	56.8%	31.8%
Risk Assessment Conducted – Yes, Vulnerability Unknown	15.4%	15.4%	69.2%
Risk Assessment Conducted – Yes, Vulnerability Indicated	16.0%	36.0%	48.0%
Overall	**12.2%**	**42.5%**	**45.3%**

The descriptive statistics for new information security risks for BYOD are shown in Appendix K. The same 11 variables were presented to both organizations that allow BYOD and those that do not. All 11 variables had a greater percentage of "Yes" answers than "No" answers for both organizations that allow BYOD and those that do not.

The Chi-Square results (Table 14) show that only two of the variables are not significantly related to the allow BYOD variable for organizations that permit BYOD and those that do not: 1) theft of loss of BYOD device and 2) social engineering schemes to compromise a BYOD device. The remaining nine variables are significantly related to the decision to allow BYOD.

Table 14. Chi-Square Test of Independence for New Information Security Risks for BYOD

Item	Pearson Chi-Square	Critical Value	df
Theft or loss of a BYOD device	3.457	5.991	2
Organization control of BYOD device activity	26.372	5.991	2
Unauthorized access to business systems and data	20.903	5.991	2
Access controls based on business need to know	8.048	5.991	2
BYOD device compliance with policies and regulations	16.845	5.991	2
Protection of sensitive information at all times	17.012	5.991	2
Data is available when needed on a BYOD device	8.225	5.991	2
Social engineering schemes to compromise a BYOD device	2.446	5.991	2
Loss or theft of data on a BYOD device	19.216	5.991	2
Loss or theft of data in transmission to a BYOD device	11.656	5.991	2
Viruses or malicious software that target a BYOD device	10.495	5.991	2

Summary

This section detailed the pre-analysis of the survey responses, which resulted in identification of 213 problematic responses. The remaining 450 responses were tested for validity, reliability, and model fit. Cronbach's Alpha and the Chi-Square Test of Independence showed positive results of reliability and model goodness of fit. The descriptive statistics of the responses were reviewed, and the significant differences between variables for organizations that allow BYOD and do not allow BYOD were identified.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

The goal of this research was to explore how widely BYOD is permitted in organizations, the approaches that were used in the decision making process to allow the use of BYOD, the factors that affected a company's willingness to adopt BYOD, and the specific information security risks that were associated with a BYOD program. This chapter presents the conclusions based on the data analysis. Implications of this research will be identified and future research opportunities will be discussed. Lastly, recommendations and a summary of the research will be presented.

Conclusions

RQ1: How widely is the use of BYOD permitted in organizations?

This study established the actual rate of acceptance of BYOD at 40.2% for organizations that participated in the study. The research responses were classified into allowed BYOD and did not allow BYOD categories for further analysis. The demographics of organizations that allow BYOD and those that do not were not significantly different, establishing that the rate of BYOD is similar regardless of the primary business activity, size, or where the organization conducts business. This finding

provides important insight into the viability of BYOD regardless of organization demographic, and may dispel notions that some business activities require tighter information security controls, affecting the adoption rate of BYOD. Likewise, perceived beliefs that organization size or where they conduct business may affect the adoption rate of BYOD can be dismissed.

RQ2: What approach was employed to evaluate BYOD?

The analysis of the decision making approaches used for BYOD that were considered within this study established that there were approaches that were significantly related to the decision to allow BYOD. The study expected to find that conducting a risk assessment was a critical part of the approach, and confirmed this expectation for organizations that permit BYOD. Of the organizations that allow BYOD, 52.5% conducted a risk assessment to prepare for BYOD; however, only 39% of organizations that did not allow BYOD conducted a risk assessment. This research established that there was a significant relationship between allowing BYOD and conducting a formal risk assessment to prepare for BYOD.

The research determined that the majority of organizations that conducted a risk assessment to evaluate the risks of BYOD found that BYOD would increase the vulnerability of the organization. For organizations that do not permit BYOD, nearly 90% responded that the risk assessment indicated that BYOD would increase the vulnerability of the organization. These results suggest that the organization's decision to reject BYOD was appropriate, at least until information security controls are identified and implemented to mitigate the vulnerabilities due to BYOD.

Further, the research attempted to determine the level of involvement of various organizational stakeholders in the decision to allow the use of BYOD, and determined that the involvement of management was significantly important in the decision making process, and was significantly more important to organizations that allowed BYOD. In addition, participants indicated that a formal decision making process and a legal review were important to the decision making process. The data analysis confirms that the use of these approaches had a significant relationship to the decision to allow BYOD.

This study expected that the participation of internal control professionals was necessary to effectively assess risk and identify reasonable controls to allow the use of BYOD. However, the research found that the BYOD decision was made without the involvement of internal control professionals a majority of the time for both organizations that allow BYOD and those that do not. Not only were internal control professionals not involved in making the decision, they also were not involved in the evaluation process a majority the time for all organizations. However, internal control oversight of BYOD controls and policies was found to be a significant information security control for organizations that allow BYOD and have not suffered a security breach. This finding revealed that the participation of internal control professionals is necessary to assess BYOD controls and policies on an ongoing basis to monitor and control BYOD programs.

RQ3: What factors affected the decision to allow BYOD programs?

This study identified that the following factors were significantly related to the decision to allow BYOD:

- Management support of the decision to allow BYOD
- Capabilities of cloud vendor solutions or apps, such as Salesforce or Workday

For organizations that did not allow BYOD, a majority indicated that information and data security concerns were important factors. Further, these organizations were influenced to reject BYOD due to the concerns of securing and managing personal mobile devices. Analysis of the data reveals that organizations that did not allow BYOD consistently indicated new information security concerns for BYOD at significantly higher rates than organizations that allowed BYOD, reinforcing the finding that information and data security concerns were significant in the decision making process for organizations that did not allow BYOD.

This study expected the support of internal control professionals to be influential in the decision making process, and the "Yes" responses were significantly higher than "No" responses. However, approximately 45% of organizations responded "Unknown". Data analysis revealed that the influence of internal control professionals is not significantly related to the decision to allow BYOD, and confirmed the expectation that internal controls professionals were influential in the decision making process for all organizations.

This study identified two factors that are significantly related to the decision to permit BYOD or not: Management support of the decision and the capabilities of cloud vendor solutions. A much higher percentage of organizations that allowed BYOD had management support of the decision, and organizations that did not allow BYOD had a much higher Unknown response (47.2%) for the influence of cloud vendor solutions.

RQ4: How are BYOD programs monitored and controlled?

This study investigated the additional governance, risk management, and control systems that protect organizations that allow BYOD from unreasonable risk. Having a formal BYOD policy in place and establishing a formal acceptable use policy with specific requirements for BYOD were the most common information security controls in place for organizations that allow BYOD. This research established that all of the 16 information security controls identified during the literature review were significantly related to the lack of occurrence of an information security breach. The adoption of information security controls to mitigate BYOD threats by organizations that allow BYOD is presented in Table 15. 15 of the 16 information security controls identified during the literature review had a higher percentage of “Yes” responses; only one of the information security controls, use of GPS to track device location, had a higher percentage of “No” responses.

Table 15. Information Security Controls in Use for BYOD

Information Security Control for BYOD	Yes	No	Unknown
Formal BYOD policy in place	61.3%	27.1%	11.6%
Formal acceptable use policy exists with specific requirements for BYOD	60.8%	23.8%	15.5%
New internal controls for passwords or lock codes on BYOD devices	58.6%	22.1%	19.3%
Formal data governance process or policy in effect for BYOD	55.8%	25.4%	18.8%
New internal controls for data protection for BYOD	53.6%	20.4%	26.0%
Service restrictions enforced for BYOD	51.4%	26.5%	22.1%
Internal control oversight of BYOD controls and policies	50.8%	26.5%	22.7%
Software that detects viruses or malware required for BYOD	50.8%	23.8%	25.4%
Mobile security software mandatory for BYOD	50.3%	29.8%	19.9%
Policy enforcement required for BYOD	44.8%	21.5%	33.7%
Compliance with device upgrades enforced for BYOD through automatic updates or notifications	42.5%	28.7%	28.7%
Regular risk assessments conducted to monitor BYOD	41.4%	28.7%	29.8%
Sensitive data/privacy filters in use to limit the data that can be accessed with BYOD	41.4%	24.9%	33.7%
Segregation of personal and organizational data mandatory for BYOD	40.9%	29.3%	29.8%
Data usage alerts in place to notify when corporate data is accessed by BYOD	31.5%	29.8%	38.7%
The GPS of the mobile device used to track device location in the event of loss or theft	26.0%	36.5%	37.6%

The use of information security controls does not represent effectiveness against threats, so the information security controls were evaluated in the context of a security breach occurrence. Although many survey responses indicated that it was unknown if there was an information security breach due to BYOD, only 12.2% of organizations that allow BYOD acknowledged that the organization had experienced an information security breach. All of the information security controls that were identified during the literature review and included in the survey were identified as significantly related to the (lack of) occurrence of an information security breach in the organization due to BYOD.

This finding informs the information security controls that have been empirically tested as significantly related to the lack of occurrence of an information security breach at organizations that allow BYOD.

RQ5: What new information security risks are associated with BYOD programs?

This study sought to understand the new information security concerns and risks that were associated with BYOD. Information security concerns and risks presented by BYOD were identified through the literature review, and were presented on the survey for consideration. Organizations that allowed BYOD indicated when the information security concern or risk was newly introduced by BYOD adoption, and organizations that did not allow BYOD indicated when they perceived that the information security concern or risk was newly introduced by BYOD adoption.

Both organizations that allow BYOD and those that do not were consistent (not significantly different) in identifying two of the information security risks presented: 1) theft or loss of a BYOD device and (2) social engineering schemes to compromise a BYOD device. However, the remaining nine information security risks were identified as significantly related to the decision to not allow BYOD. Organizations that did not allow BYOD responded significantly more positively ("Yes") compared to organizations that allowed BYOD for eight of the nine remaining information security risks. Data availability when needed on a BYOD device was the only new information security concern that had a higher percentage of "Yes" responses from organizations that allow BYOD.

The study revealed that BYOD is associated with new information security concerns in the broad areas of device security, data security, and data availability. This study found that all of the information security concerns and risks presented, including access to data, compliance with policies, compromise of the device, protection of sensitive data, and control of the device did or was perceived to introduce new risks and affected a company's willingness to support BYOD.

Implications

This study has established the adoption rate of BYOD by an empirical test of organizations that were represented by internal control professionals. Further, the study investigated the categories of allowed BYOD and did not allow BYOD to establish effective approaches to making the BYOD decision. Identification of the significant approaches to making a BYOD decision can serve as a basis for future research that further develops the understanding and implication of each decision making approach. For example, this study established that following a formal decision making process is a critical part of evaluating BYOD, and future research could document and validate the specific steps in a formal process to evaluate BYOD.

This study also established that management support and the influence of cloud vendor solutions, such as Salesforce or Workday, to provide business capabilities via BYOD are critical factors that drive the decision to evaluate BYOD. Future research could develop a model and identify the specific constructs that result in a successful decision making process, based on the initial factors identified by this study.

This study also provided valuable information about monitoring and controlling BYOD for practitioners who are considering BYOD. Based on the current literature, 16 information security controls related to BYOD were identified and confirmed as significant in preventing information security breaches due to BYOD. This provides valuable insight for practitioners who must mitigate the threats of BYOD with proven information security controls. In addition, future research could target organizations that allow BYOD and study the relationship between information security controls and the frequency of information security breaches.

Finally, the study revealed that organizations that did not allow BYOD are significantly more cautious of the new information security risks presented by BYOD. This finding not only highlights the need for diligence in preparing for BYOD, but also provided insight that perhaps the risks are over-emphasized in organizations that were tending towards rejecting BYOD.

Recommendations

Future research should consider the significant approaches to making a BYOD decision and further develop the understanding and implication of each decision making approach. This study established the approaches that are a critical part of evaluating BYOD to establish a basic understanding. Future research should expand and validate the specific components of each approach to effectively consider and make a decision about BYOD.

Future research should develop a model and identify the specific constructs that are driving a BYOD decision making process, based on the significant factors identified

by this study. Future research should focus on scenarios where vendor cloud solutions inherently are accessible by BYOD, and identify the actual proliferation of BYOD throughout the organization. This future research could identify levels of BYOD adoption and the associated factors, information security controls, and new information security risks introduced by each level.

Finally, future research should focus on organizations that allow BYOD and establish the relationship between the presence of information security controls and the frequency of information security breaches.

Summary

Armando, Costa, Verdeme, and Merlo (2014) suggest that two primary factors are responsible for the rapid adoption of mobile devices: the powerful mobile operating systems that provide advanced device capabilities, and the millions of diverse apps available in the market place delivery model that cater to the user's needs. The BYOD phenomenon resulted from the expectation to use these smart devices and advanced capabilities in all aspects of a daily routine, including the workplace (Banham, 2013). BYOD could drive an IT evolution in organizations, providing powerful device capabilities and easy to use apps, but only if the information security concerns can be addressed.

BYOD is invading the business environment due to two primary factors. First, these advanced devices and applications that are readily available for personal use are finding their way into the workplace, causing significant information security challenges for organizations (Earley, Harmon, Lee, & Mithas, 2014). Second, enterprises are

adopting SaaS (Software-as-a-Service) cloud-based applications that leverage the features of mobile devices to provide a robust technology experience for employees. These new technology devices and advanced applications are challenging the traditional approach to information security controls, which include provisioning, controlling access to, and protecting equipment, systems, and data.

Despite the productivity opportunities, organizations must establish BYOD programs that include effective policies, appropriate access methods, compliance with applicable regulations, device security, data protection, and proper controls. Research and information security standards that identify appropriate controls to mitigate information security risk are plentiful. DaVeiga and Eloff (2007) suggest that effective information security is provided through a combination of technical controls, management processes, cultural elements, and governance. However, there was little understanding of the specific approach that led to successful adoption of a BYOD program. Research was needed to understand the adoption rate of BYOD, what approach was followed in the decision making process, and what specific factors affected a company's decision to adopt BYOD. In addition, specific information security risks associated with BYOD needed to be identified so that appropriate internal controls that lead to successful programs could be put in place to enable the high tech advantages that both employees and organizations seek (Harris, Kinkela, & Hayes, 2011).

The goal of this research was to explore how widely BYOD was permitted in organizations, the approaches that were used in the decision making process to allow the

use of BYOD, the factors that affected a company's willingness to support BYOD, and the specific information security risks that were associated with a BYOD program.

This study used exploratory research, which was appropriate since there was little existing literature available on the adoption of BYOD. Exploratory research was suitable to establish initial research in the problem area to use for future research (Singh, 2007). The exploratory research utilized available literature, data, and formal data collection methods. The research was carried out in three stages: instrument development and validation, data collection, and data analysis. The Chi-Square test of independence was used throughout the data analysis phase to establish significant relationships between the two categories of responses (BYOD allowed or not allowed) and the other variables in the survey.

Given the opportunities and challenges that BYOD presents to organizations, this study explored five research questions to understand how BYOD was securely adopted by organizations. The research questions included:

1. How widely was the use of BYOD permitted in organizations? The actual rate of acceptance of BYOD was established at 40.2%.
2. What approach was used to evaluate BYOD? The approaches that were found to be significantly important were conducting a formal risk assessment, involving management, utilizing a formal decision making process, and including a legal review.
3. What factors affected the decision to allow BYOD? Two factors were identified that were significantly related to the decision to allow BYOD: management support of the decision to allow BYOD and capability of cloud vendor solutions or apps, such as Salesforce or Workday.
4. How were BYOD programs monitored and controlled? The most common information security controls were having a formal BYOD policy in place and establishing a formal acceptable use policy with specific requirements for

BYOD. However, all of the information security controls that were presented were significantly related to the lack of occurrence of an information security breach in the organization due to BYOD.

5. What new information security risks were associated with BYOD programs? Two new information security concerns, theft or loss of a BYOD device and social engineering schemes to compromise a BYOD device, were consistent in importance to both organizations that allowed and organizations that did not allow BYOD.

The survey instrument was developed to communicate the questions clearly, while at the same time being concise and simple to ensure ease of response (Dolnicar, 2003). To determine what specific methods, factors, and controls were associated with the decision to permit BYOD, closed-end questions with a fixed set of answers (yes/no/unknown) were used.

This study was based on the opinions of experienced auditors and other internal control professionals to ensure the validity of the research. Working with the Institute for Internal Controls (IIC) ensured that this research was based on reputable and active internal control professionals, and allowed use of a trusted email channel to request participation in this effort. The IIC is an organization with a membership of internal control professionals, and most hold the Certified Internal Controls Auditor (CICA) credential.

To ensure validity and reliability, an expert panel of 10 members of the IIC was selected to evaluate the survey instrument, and to indicate if the survey covered the full breadth of content (sampling validity) and if each question measured what it intended to measure (item validity). The survey was updated to reflect the expert panel feedback,

and the final survey was published and disseminated to the IIC email channel for data collection.

This study established the actual rate of acceptance of BYOD at 40.2% for organizations that participated in the study. The research also established that the acceptance rate of BYOD is similar regardless of the primary business activity, size, or where the organization conducts business.

Data analysis results confirmed that conducting a risk assessment was a critical part of an organization's approach to adopting BYOD. Statistical analysis showed a significant relationship between allowing BYOD and conducting a formal risk assessment to prepare for BYOD. Further, the research determined that the involvement of management was significantly important in the decision making process, and is significantly more important to organizations that allowed BYOD. In addition, the study found that a formal decision making process and a legal review were significantly related to the decision to allow BYOD.

This study expected that the participation of internal control professionals was necessary in the decision making process to allow BYOD. However, the research found that the BYOD decision was made without significant involvement of internal control professionals in the decision making process or in the evaluation process. However, the results revealed that the majority of organizations were influenced by the support of internal control professionals for the BYOD decision. Further, the results revealed that the participation of internal control professionals is necessary to assess BYOD controls and policies on an ongoing basis to effectively monitor and control BYOD programs.

This study identified two factors that were significantly related to the decision to allow BYOD: 1) management support of the decision to allow BYOD and 2) capabilities of cloud vendor solutions or apps, such as Salesforce or Workday.

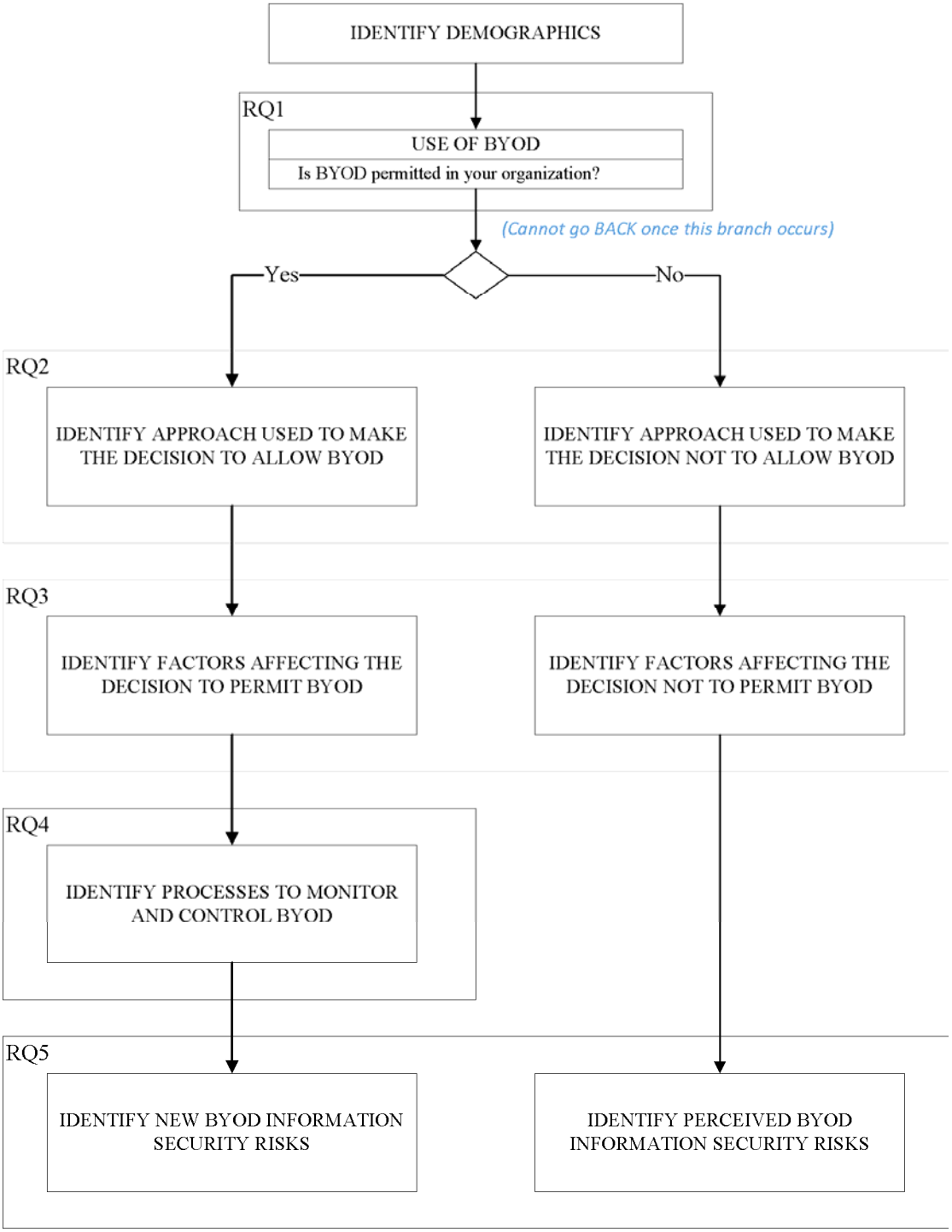
This study found that having a formal BYOD policy in place and establishing a formal acceptable use policy with specific requirements for BYOD were the most common information security controls in place for organizations that allow BYOD. The use of information security controls does not represent effectiveness against threats, so the information security controls were evaluated in the context of a security breach occurrence. Although many survey responses indicated that it was unknown if there was an information security breach due to BYOD, only 12.2% of organizations that allow BYOD acknowledged that the organization had experienced an information security breach. All of the information security controls that were identified during the literature review and included in the survey were identified as significantly related to the (lack of) occurrence of an information security breach in the organization due to BYOD, which provides valuable insight for practitioners that are looking to adopt BYOD. This finding identified the empirically tested information security controls that were significantly related to the lack of occurrence of an information security breach at organizations that allow BYOD.

The research identified the new information security concerns and risks that were associated with BYOD. Both organizations that allow BYOD and those that do not were consistent (not significantly different) in identifying two of the information security risks presented: 1) theft or loss of a BYOD device and (2) social engineering schemes to

compromise a BYOD device. However, eight of the remaining nine information security risks were identified as significantly related to the decision to not allow BYOD. Organizations that did not allow BYOD responded significantly more positively ("Yes") compared to organizations that allowed BYOD, indicating more apprehension with information security concerns relating to BYOD and resulting in the rejection of BYOD. Data availability when needed on a BYOD device was the only new information security concern that had a higher percentage of "Yes" responses from organizations that allow BYOD.

This study established the acceptance rate of BYOD and identified approaches that are a critical part of evaluating BYOD. This research provided initial knowledge in the area of BYOD adoption upon which future research should expand and validate the specific components of each approach to effectively consider and make a decision about BYOD. The research confirmed that there were several new information security risks in the areas of access, compliance, compromise, data protection, and control that affect a company's willingness to adopt BYOD and identified new elements of governance, risk management, and control systems that were necessary to ensure a secure BYOD program.

Appendix A
Survey Decision Tree



Appendix B

Preliminary Survey Instrument

This research proposes to leverage the expertise of experienced internal control professionals to determine the use of BYOD in organizations, the approach used in the decision making process, and the significant factors that led to the decision to adopt BYOD.

This survey seeks to understand your experience with the evaluation of BYOD and the final decision regarding the use of BYOD. This survey will take approximately 10-15 minutes. Responses are Anonymous. Personal information and contact association will NOT be recorded.

Demographics. Please provide the following basic information describing your role and organization characteristics.
What is your title/role in this organization? o Internal Auditor o External Auditor o Consultant o Accountant o Other If Other Is Selected: Please enter description of "other" title/role:
What is your organization's primary business activity? o Agriculture/Forestry o Business/Professional Services o Construction/Architecture o Consumer Products/Goods o Education o Entertainment/Recreation o Federal Government o Financial Services/Insurance o Healthcare o Manufacturing o Retail/Wholesale

- State/Local Government
- Technology
- Telecommunications
- Utilities
- Other:

If Other Is Selected:
Please enter description of "other" primary business activity:

How many employees (full- and part-time) are employed at your organization?
- Under 100
- 100 to 499
- 500 to 1500
- Over 1500

Where does your organization conduct its business?
- Domestically
- Globally

RQ1 - Use of BYOD.

Does your organization currently allow the use of BYOD?
- Yes
- No

YES: RQ2 – Approach used to make the decision to allow BYOD.
Each organization has a unique approach to decision-making, and this question seeks to identify the approaches that were significant to your organization during the process of evaluating BYOD.

Please indicate for each approach if it was used in the decision-making process to permit BYOD.

	Yes	No	Unknown
Was a formal risk assessment conducted to prepare for BYOD?	❍	❍	❍
Was management involved in the decision-making process for BYOD?	❍	❍	❍
Were auditors/internal audit involved in the decision-making process for BYOD?	❍	❍	❍
Was a formal decision making process followed?	❍	❍	❍
Was there any other significant approach used in the process of evaluating BYOD?	❍	❍	❍

If Other Is Selected:
Please describe other significant approach used:

YES: RQ3 - Factors affecting the decision to allow BYOD.

Following are significant factors that could contribute to the decision to permit BYOD. For the following specific factors, please indicate if they were important in the decision making process to allow BYOD.

	Yes	No	Unknown
Did a risk assessment indicate that BYOD would not increase the vulnerability of the organization?	❍	❍	❍
Did management support the decision to allow BYOD?	❍	❍	❍
Did the auditors/internal audit support the decision to allow BYOD?	❍	❍	❍
Was the decision to permit BYOD influenced by the advanced capabilities of mobile devices?	❍	❍	❍
Was the decision to permit BYOD influenced by the capabilities of cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	❍	❍	❍
Was there any other significant factor that affected the decision to allow BYOD?	❍	❍	❍

If Other Is Selected:
Please describe other significant factor that affected decision making:

YES: RQ4 - Monitoring and Controlling BYOD Programs.
The following security controls may be in use in your organization to mitigate information security threats. Indicate if the following controls are being used to monitor and control BYOD at your organization.

	Yes	No	Unknown
Is a formal BYOD policy in place?	❍	❍	❍
Is a formal data governance process or policy in effect for BYOD?	❍	❍	❍
Does a formal acceptable use policy exist with specific requirements for BYOD?	❍	❍	❍
Are regular risk assessments conducted to monitor BYOD?	❍	❍	❍
Is there internal control oversight of BYOD controls and policies?	❍	❍	❍
Are there new internal controls for data protection (on the device and in transmission) for BYOD?	❍	❍	❍
Are there new internal controls for passwords or lock codes on BYOD devices?	❍	❍	❍
Have there been any information security breaches	❍	❍	❍

at your organization due to BYOD?			
Have service restrictions (i.e. public wireless networks, collaborative apps, data sharing services, file sharing services) been enforced for BYOD?	❍	❍	❍
Are data usage alerts in place to notify when corporate data is accessed?	❍	❍	❍
Is mobile security software mandatory?	❍	❍	❍
Is software that detects viruses or malware required for BYOD?	❍	❍	❍
Is policy enforcement (permission to erase data) required for BYOD?	❍	❍	❍
Is segregation of personal and organizational data mandatory for BYOD?	❍	❍	❍
Is geotracking (device locating services) used to track devices for BYOD?	❍	❍	❍
Are sensitive data/privacy filters in use for BYOD?	❍	❍	❍
Is compliance with device (operating system) upgrades enforced for BYOD through automatic updates or notifications?	❍	❍	❍
Are there any other new internal controls implemented to monitor the use of BYOD?	❍	❍	❍

If Other Is Selected:
Please describe other new internal controls:

YES: RQ5 - New BYOD Information Security Risks.
Many of the information security concerns associated with BYOD may be similar to general concerns established in information security standards such as ISO/IEC 27000.

For the following list of information security concerns, indicate if you believe that BYOD presents NEW information security concerns and risks:

	Yes	No	Unknown
Theft or loss of a BYOD device			
Organization control of BYOD device activity	❍	❍	❍
Unauthorized access to business systems and data	❍	❍	❍
Access controls based on business need to know	❍	❍	❍
BYOD device compliance with policies and regulations	❍	❍	❍
Protection of sensitive information at all times	❍	❍	❍
Data is available when needed on a BYOD device	❍	❍	❍

Social engineering schemes to compromise a BYOD device	❍	❍	❍
Loss or theft of data on a BYOD device	❍	❍	❍
Loss or theft of data in transmission to a BYOD device	❍	❍	❍
Viruses or malicious software that target a BYOD device	❍	❍	❍
Other:	❍	❍	❍

If Other Is Selected:
Please describe:

NO: RQ2 - Approach used to make the decision not to allow BYOD.
Each organization has a unique approach to decision-making, and this question seeks to identify the approaches that were significant to your organization during the process of evaluating BYOD.

Who made the decision to reject BYOD?

Please indicate for each approach if it was used in the decision-making process to reject BYOD.

	Yes	No	Unknown
Was management involved in the decision making process to reject BYOD?	❍	❍	❍
Were auditors/internal audit involved in the decision making process to reject BYOD?	❍	❍	❍
Was a formal decision making process followed?	❍	❍	❍
Was a formal risk assessment conducted to assess the risks of BYOD?	❍	❍	❍
Was there any other significant approach used in the process of evaluating BYOD?	❍	❍	❍

If Other Is Selected:
Please describe other significant approach used:

NO: RQ3 - Factors affecting the decision not to allow BYOD.
Following are significant factors that could contribute to the decision to permit BYOD. For the following specific factors, please indicate if they were important in the decision making process to allow BYOD.

	Yes	No	Unknown
Did a risk assessment indicate that BYOD would increase the vulnerability of the organization?	❍	❍	❍
Did management support the decision to reject BYOD?	❍	❍	❍

Did the auditors/internal audit support the decision to reject BYOD?	❍	❍	❍
Was the decision to reject BYOD influenced by information/data security concerns?	❍	❍	❍
Was the decision to reject BYOD influenced by security concerns about cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	❍	❍	❍
Was the decision to reject BYOD influenced by concerns about securing and managing mobile devices?	❍	❍	❍
Was there any other significant factor that affected the decision to reject BYOD?	❍	❍	❍

If Other Is Selected:
Please describe other significant factor that affected decision making:

NO: RQ4 – Perceived New BYOD Information Security Risks.
Many of the information security concerns associated with BYOD may be similar to general concerns established in information security standards such as ISO/IEC 27000.

For the following list of information security concerns, indicate if you perceive that BYOD presents NEW information security concerns and risks:

	Yes	No	Unknown
Theft or loss of a BYOD device			
Organization control of BYOD device activity	❍	❍	❍
Unauthorized access to business systems and data	❍	❍	❍
Access controls based on business need to know	❍	❍	❍
BYOD device compliance with policies and regulations	❍	❍	❍
Protection of sensitive information at all times	❍	❍	❍
Data is available when needed on a BYOD device	❍	❍	❍
Social engineering schemes to compromise a BYOD device	❍	❍	❍
Loss or theft of data on a BYOD device	❍	❍	❍
Loss or theft of data in transmission to a BYOD device	❍	❍	❍
Viruses or malicious software that target a BYOD device	❍	❍	❍
Other:	❍	❍	❍

If Other Is Selected: Please describe:

Appendix C

Final Survey Instrument

This research proposes to leverage the expertise of experienced internal control professionals to determine the use of BYOD in organizations, the approach used in the decision making process, and the significant factors that led to the decision to adopt BYOD.

This survey seeks to understand your experience with the evaluation of BYOD and the final decision regarding the use of BYOD. This survey will take approximately 10-15 minutes. Responses are Anonymous. Personal information and contact association will NOT be recorded.

Demographics. Please provide the following basic information describing your role and organization characteristics.
What is your title/role in this organization? o Internal Auditor o External Auditor o Consultant o Accountant o Other If Other Is Selected: Please enter description of "other" title/role:
What is your organization's primary business activity? o Agriculture/Forestry o Business/Professional Services o Construction/Architecture o Consumer Products/Goods o Education o Entertainment/Recreation o Federal Government o Financial Services/Insurance o Healthcare o Manufacturing o Retail/Wholesale

- State/Local Government
- Technology
- Telecommunications
- Utilities
- Other:

If Other Is Selected:
Please enter description of "other" primary business activity:

How many employees (full- and part-time) are employed at your organization?
- Under 100
- 100 to 499
- 500 to 1500
- Over 1500

Where does your organization conduct its business?
- Domestically
- Globally

RQ1 - Use of BYOD.

Does your organization currently allow the use of BYOD?
- Yes
- No

YES: RQ2 – Approach used to make the decision to allow BYOD.
Each organization has a unique approach to decision-making, and this question seeks to identify the approaches that were significant to your organization during the process of evaluating BYOD.

Please indicate for each approach if it was used in the decision-making process to permit BYOD.

	Yes	No	Unknown
Was a formal risk assessment conducted to prepare for BYOD?	❍	❍	❍
Was management involved in the decision-making process for BYOD?	❍	❍	❍
Were auditors/internal audit involved in the evaluation process for BYOD?	❍	❍	❍
Were auditors/internal audit involved in the decision-making process for BYOD?	❍	❍	❍
Was a legal review part of the decision-making process for BYOD?	❍	❍	❍
Was a formal decision making process followed?	❍	❍	❍

Was there any other significant approach used in the process of evaluating BYOD?

If a formal risk assessment was conducted to prepare for BYOD:

Did the risk assessment indicate that BYOD would not increase the vulnerability of the organization?

- o Yes
- o No
- o Unknown

YES: RQ3 - Factors affecting the decision to allow BYOD.
Following are significant factors that could contribute to the decision to permit BYOD. For the following specific factors, please indicate if they were important in the decision making process to allow BYOD.

	Yes	No	Unknown
Did management support the decision to allow BYOD?	❍	❍	❍
Did the auditors/internal audit support the decision to allow BYOD?	❍	❍	❍
Was the decision to permit BYOD influenced by the advanced capabilities of mobile devices?	❍	❍	❍
Was the decision to permit BYOD influenced by the capabilities of cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	❍	❍	❍

Was there any other significant factor that affected the decision to allow BYOD?

YES: RQ4 - Monitoring and Controlling BYOD Programs.
The following information security controls may be in use in your organization to mitigate information security threats. Indicate if the following controls are being used to monitor and control BYOD at your organization.

If a control effectiveness audit has not been performed on BYOD or the information is not known, please select "Unknown".

	Yes	No	Unknown
Is a formal BYOD policy in place?	❍	❍	❍
Is a formal data governance process or policy in effect for BYOD?	❍	❍	❍
Does a formal acceptable use policy exist with specific requirements for BYOD?	❍	❍	❍
Are regular risk assessments conducted to monitor BYOD?	❍	❍	❍
Is there internal control oversight of BYOD controls and policies?	❍	❍	❍

Are there new internal controls for data protection (on the device and in transmission between the company and the device) for BYOD?	❍	❍	❍
Are there new internal controls for passwords or lock codes on BYOD devices?	❍	❍	❍
Have there been any information security breaches at your organization due to BYOD?	❍	❍	❍
Have service restrictions (i.e. public wireless networks, collaborative apps, data sharing services, file sharing services) been enforced for BYOD?	❍	❍	❍
Are data usage alerts in place to notify when corporate data is accessed by a personal mobile device?	❍	❍	❍
Is mobile security software mandatory for personal mobile devices?	❍	❍	❍
Is software that detects viruses or malware required for BYOD?	❍	❍	❍
Is policy enforcement (i.e. permission to erase data in the event of loss or theft of a device) required for BYOD?	❍	❍	❍
Is segregation of personal and organizational data mandatory for BYOD, to ensure corporate data isn't accidentally shared via personal contacts or apps?	❍	❍	❍
Is the GPS of the mobile device (device locating services) used to track device location in the event of loss or theft?	❍	❍	❍
Are sensitive data/privacy filters in use to limit the data that can be accessed with BYOD?	❍	❍	❍
Is compliance with device upgrades, such as staying current with operating system and security patches, enforced for BYOD through automatic updates or notifications?	❍	❍	❍
Are there any other new internal controls implemented to monitor the use of BYOD?			

YES: RQ5 - New BYOD Information Security Risks.
Many of the information security concerns associated with BYOD may be similar to general concerns established in information security standards such as ISO/IEC 27000.

For the following list of information security concerns, indicate if you believe that BYOD presents NEW information security concerns and risks:

	Yes	No	Unknown

Theft or loss of a BYOD device			
Organization control of BYOD device activity	❍	❍	❍
Unauthorized access to business systems and data	❍	❍	❍
Access controls based on business need to know	❍	❍	❍
BYOD device compliance with policies and regulations	❍	❍	❍
Protection of sensitive information at all times	❍	❍	❍
Data is available when needed on a BYOD device	❍	❍	❍
Social engineering schemes to compromise a BYOD device	❍	❍	❍
Loss or theft of data on a BYOD device	❍	❍	❍
Loss or theft of data in transmission to a BYOD device	❍	❍	❍
Viruses or malicious software that target a BYOD device	❍	❍	❍

Are there any other new information security concerns presented by BYOD?

NO: RQ2 - Approach used to make the decision not to allow BYOD.
Each organization has a unique approach to decision-making, and this question seeks to identify the approaches that were significant to your organization during the process of evaluating BYOD.

Please indicate for each approach if it was used in the decision-making process to reject BYOD.

Who made the decision to reject BYOD?

- o CEO/President
- o CIO
- o Consultant
- o External Auditor
- o Internal Auditor
- o Legal Counsel
- o Management Team
- o Other

If Other Is Selected:
Please enter description of "other" title/role::

	Yes	No	Unknown
Was management involved in the decision making process to reject BYOD?	❍	❍	❍
Were auditors/internal audit involved in the evaluation process for BYOD?	❍	❍	❍

Were auditors/internal audit involved in the decision making process to reject BYOD?	❍	❍	❍
Was a legal review part of the decision-making process to reject BYOD?	❍	❍	❍
Was a formal decision making process followed?	❍	❍	❍
Was a formal risk assessment conducted to assess the risks of BYOD?	❍	❍	❍

Was there any other significant approach used in the process of evaluating BYOD?

If a formal risk assessment was conducted to assess the risks of BYOD:
Did the risk assessment indicate that BYOD would increase the vulnerability of the organization?

- o Yes
- o No
- o Unknown

NO: RQ3 - Factors affecting the decision not to allow BYOD.
Following are significant factors that could contribute to the decision to permit BYOD. For the following specific factors, please indicate if they were important in the decision making process to reject BYOD.

	Yes	No	Unknown
Did management support the decision to reject BYOD?	❍	❍	❍
Did the auditors/internal audit support the decision to reject BYOD?	❍	❍	❍
Was the decision to reject BYOD influenced by information/data security concerns?	❍	❍	❍
Was the decision to reject BYOD influenced by security concerns about cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	❍	❍	❍
Was the decision to reject BYOD influenced by concerns about securing and managing mobile devices?	❍	❍	❍

Was there any other significant factor that affected the decision to reject BYOD?

NO: RQ4 – Perceived New BYOD Information Security Risks.
Many of the information security concerns associated with BYOD may be similar to general concerns established in information security standards such as ISO/IEC 27000.

For the following list of information security concerns, indicate if you perceive that BYOD presents NEW information security concerns and risks:

	Yes	No	Unknown
Theft or loss of a BYOD device	❍	❍	❍
Organization control of BYOD device activity	❍	❍	❍
Unauthorized access to business systems and data	❍	❍	❍
Access controls based on business need to know	❍	❍	❍
BYOD device compliance with policies and regulations	❍	❍	❍
Protection of sensitive information at all times	❍	❍	❍
Data is available when needed on a BYOD device	❍	❍	❍
Social engineering schemes to compromise a BYOD device	❍	❍	❍
Loss or theft of data on a BYOD device	❍	❍	❍
Loss or theft of data in transmission to a BYOD device	❍	❍	❍
Viruses or malicious software that target a BYOD device	❍	❍	❍
Are there any other new information security concerns presented by BYOD?			

Appendix D

Sample Invitation to Participate in Dissertation Study

[From chairman@theiic.org to TheIIC Membership Email system]

Dear IIC member,

Coleen D. Santee, a doctoral student at Nova Southeastern University seeking a Doctor of Information Systems (Ph.D.) degree, is conducting a study to determine the use of Bring Your Own Devices (BYOD) in organizations, the approach used in the decision making process regarding the use of BYOD, and the significant factors that led to the decision to adopt BYOD, including internal controls issues. She is requesting participation of TheIIC and its members, since input from experienced internal control professionals is needed to understand involvement in the evaluation of BYOD and the final decision regarding the use of BYOD. This survey will take approximately 10-15 minutes to complete. It should be noted that the survey should be completed whether or not your organization is allowing the use of BYOD since this is a factor in the study. If your organization is not using BYOD the survey will involve only a few questions and take only minutes. I suggest that all members of TheIIC complete the survey immediately.

Note that summarized findings will be made available to TheIIC at the conclusion of the study and will be published in a subsequent issue of TheIIC e-Magazine and made available for consideration for publication in the new Journal of Internal Controls.

Responses to the survey will be anonymous and submitted directly to the researcher. Personal information will NOT be recorded and only aggregate data will be used in reports and publications. Confidentiality will be strictly maintained.

To participate in the study, please access the survey at:
http://kentstate.az1.qualtrics.com/SE/?SID=SV_0TXFVJx7D52qsct

Participation in this study is voluntary; however, I encourage you to complete the survey. Please contact me directly at chairman@theiic.org for more information or with questions about this study.

Dr. Frank

Frank Nasuti, Ph.D., CPA, CICA, CFE, CGMA
Chairman

Appendix E

IRB Approval

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Coleen Santee**
College of Engineering and Computing

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **September 26, 2016**

Re: **IRB #: 2016-429; Title, "An Exploratory Study of the Approach to Bring Your Own Device (BYOD) in Assuring Information Security"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: **FRANK NASUTI**

Appendix F

Demographics for BYOD Participants – Descriptive Data

Title/Role	**BYOD Permitted**	**BYOD Not Permitted**
Internal Auditor	45.9%	50.2%
External Auditor	7.2%	8.6%
Consultant	13.3%	7.8%
Accountant	9.4%	11.2%
Other	24.3%	22.3%
Primary Business Activity	**BYOD Permitted**	**BYOD Not Permitted**
Agriculture/Forestry	0.6%	0.7%
Business/Professional Services	13.3%	9.7%
Construction/Architecture	1.7%	1.5%
Consumer Products/Goods	1.1%	1.1%
Education	11.6%	4.5%
Entertainment/Recreation	0.6%	0.4%
Federal Government	6.6%	14.5%
Financial Services/Insurance	29.3%	26.8%
Healthcare	5.5%	4.8%
Manufacturing	3.3%	5.6%
Retail/Wholesale	2.8%	3.0%
State/Local Government	11.0%	14.1%
Technology	2.8%	0.7%
Telecommunications	1.1%	1.1%
Utilities	3.3%	5.6%
Other	5.5%	5.9%
Number of Employees	**BYOD Permitted**	**BYOD Not Permitted**
Under 100	16.0%	15.6%
100 to 499	19.9%	18.2%
500 to 1500	11.0%	19.3%
Over 1500	53.0%	46.8%
Conduct Business	**BYOD Permitted**	**BYOD Not Permitted**
Domestically	60.8%	65.1%
Globally	39.2%	34.6%
Missing	0.0%	0.4%

Appendix G

Approach Used in Decision Making Process for BYOD – Descriptive Data

BYOD Currently Permitted	Yes	No	Unknown
Was a formal risk assessment conducted to prepare for BYOD?	52.5%	26.0%	21.5%
Was management involved in the decision-making process for BYOD?	75.1%	11.0%	13.8%
Were auditors/internal audit involved in the evaluation process for BYOD?	32.6%	40.9%	26.5%
Were auditors/internal audit involved in the decision-making process for BYOD?	23.8%	49.7%	26.5%
Was a formal decision making process followed?	58.0%	18.2%	23.8%
Was a legal review part of the decision-making process for BYOD?	39.8%	29.8%	30.4%
Did the risk assessment indicate that BYOD would not increase the vulnerability of the organization?	24.3%	13.8%	14.4%
BYOD Currently Not Permitted	**Yes**	**No**	**Unknown**
Was a formal risk assessment conducted to assess the risks of BYOD?	39.0%	17.5%	43.5%
Was management involved in the decision making process to reject BYOD?	66.2%	7.4%	26.4%
Were auditors/internal audit involved in the evaluation process for BYOD?	26.0%	48.0%	26.0%
Were auditors/internal audit involved in the decision making process to reject BYOD?	18.2%	51.3%	30.5%
Was a formal decision making process followed?	42.0%	16.7%	41.3%
Was a legal review part of the decision-making process to reject BYOD?	33.5%	23.4%	43.1%
Did the risk assessment indicate that BYOD would increase the vulnerability of the organization?	34.6%	1.5%	3.0%

Appendix H

Significant Factors for BYOD Decision – Descriptive Data

BYOD Currently Permitted	**Yes**	**No**	**Unknown**
Did management support the decision to allow BYOD?	80.7%	4.4%	14.9%
Did the auditors/internal audit support the decision to allow BYOD?	37.6%	18.8%	43.6%
Was the decision to permit BYOD influenced by the advanced capabilities of mobile devices?	64.1%	11.0%	24.9%
Was the decision to permit BYOD influenced by the capabilities of cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	37.6%	27.1%	35.4%
BYOD Currently Not Permitted	**Yes**	**No**	**Unknown**
Did management support the decision to reject BYOD?	68.8%	4.5%	26.8%
Did the auditors/internal audit support the decision to reject BYOD?	40.5%	14.9%	44.6%
Was the decision to reject BYOD influenced by security concerns about cloud vendor solutions or apps available to the organization, such as Salesforce or Workday?	38.7%	14.1%	47.2%
Was the decision to reject BYOD influenced by information/data security concerns?	65.4%	5.6%	29.0%
Was the decision to reject BYOD influenced by concerns about securing and managing mobile devices?	57.6%	9.7%	32.7%

Appendix I

Information Security Controls in Use for BYOD - Descriptive Data

BYOD Currently Permitted	Yes	No	Unknown
Is a formal BYOD policy in place?	61.3%	27.1%	11.6%
Is a formal data governance process or policy in effect for BYOD?	55.8%	25.4%	18.8%
Does a formal acceptable use policy exist with specific requirements for BYOD?	60.8%	23.8%	15.5%
Are regular risk assessments conducted to monitor BYOD?	41.4%	28.7%	29.8%
Is there internal control oversight of BYOD controls and policies?	50.8%	26.5%	22.7%
Are there new internal controls for data protection (on the device and in transmission between the company and the device) for BYOD?	53.6%	20.4%	26.0%
Are there new internal controls for passwords or lock codes on BYOD devices?	58.6%	22.1%	19.3%
Have there been any information security breaches at your organization due to BYOD?	12.2%	42.5%	45.3%
Have service restrictions (i.e. public wireless networks, collaborative apps, data sharing services, file sharing services) been enforced for BYOD?	51.4%	26.5%	22.1%
Are data usage alerts in place to notify when corporate data is accessed by a personal mobile device?	31.5%	29.8%	38.7%
Is mobile security software mandatory for personal mobile devices?	50.3%	29.8%	19.9%
Is software that detects viruses or malware required for BYOD?	50.8%	23.8%	25.4%
Is policy enforcement (i.e. permission to erase data in the event of loss or theft of a device) required for BYOD?	44.8%	21.5%	33.7%
Is segregation of personal and organizational data mandatory for BYOD, to ensure corporate data isn't accidentally shared via personal contacts or apps?	40.9%	29.3%	29.8%

BYOD Currently Permitted	Yes	No	Unknown
Is the GPS of the mobile device (device locating services) used to track device location in the event of loss or theft?	26.0%	36.5%	37.6%
Are sensitive data/privacy filters in use to limit the data that can be accessed with BYOD?	41.4%	24.9%	33.7%
Is compliance with device upgrades, such as staying current with operating system and security patches, enforced for BYOD through automatic updates or notifications?	42.5%	28.7%	28.7%

Appendix J

Information Security Controls Effectiveness for BYOD

Item	Pearson Chi-Square	Critical Value	df
Is a formal BYOD policy in place?	14.244	9.488	4
Is a formal data governance process or policy in effect for BYOD?	30.104	9.488	4
Does a formal acceptable use policy exist with specific requirements for BYOD?	25.271	9.488	4
Are regular risk assessments conducted to monitor BYOD?	25.356	9.488	4
Is there internal control oversight of BYOD controls and policies?	21.390	9.488	4
Are there new internal controls for data protection (on the device and in transmission between the company and the device) for BYOD?	26.707	9.488	4
Are there new internal controls for passwords or lock codes on BYOD devices?	25.857	9.488	4
Have service restrictions (i.e. public wireless networks, collaborative apps, data sharing services, file sharing services) been enforced for BYOD?	42.397	9.488	4
Are data usage alerts in place to notify when corporate data is accessed by a personal mobile device?	70.501	9.488	4
Is mobile security software mandatory for personal mobile devices?	32.259	9.488	4
Is software that detects viruses or malware required for BYOD?	18.603	9.488	4
Is policy enforcement (i.e. permission to erase data in the event of loss or theft of a device) required for BYOD?	26.764	9.488	4
Is segregation of personal and organizational data mandatory for BYOD, to ensure corporate data isn’t accidentally shared via personal contacts or apps?	30.476	9.488	4

Item	Pearson Chi-Square	Critical Value	df
Is the GPS of the mobile device (device locating services) used to track device location in the event of loss or theft?	29.461	9.488	4
Are sensitive data/privacy filters in use to limit the data that can be accessed with BYOD?	31.810	9.488	4
Is compliance with device upgrades, such as staying current with operating system and security patches, enforced for BYOD through automatic updates or notifications?	36.207	9.488	4

Appendix K

New Information Security Risks for BYOD – Descriptive Data

BYOD Currently Permitted	Yes	No	Unknown
Theft or loss of a BYOD device	68.5%	21.5%	9.9%
Organization control of BYOD device activity	64.1%	26.0%	9.9%
Unauthorized access to business systems and data	64.1%	26.5%	9.4%
Access controls based on business need to know	64.6%	23.8%	11.6%
BYOD device compliance with policies and regulations	68.0%	24.3%	7.7%
Protection of sensitive information at all times	75.7%	16.0%	8.3%
Data is available when needed on a BYOD device	66.9%	21.5%	11.6%
Social engineering schemes to compromise a BYOD device	60.8%	20.4%	18.8%
Loss or theft of data on a BYOD device	66.3%	19.3%	14.4%
Loss or theft of data in transmission to a BYOD device	64.6%	20.4%	14.9%
Viruses or malicious software that target a BYOD device	71.8%	14.9%	13.3%
BYOD Currently Not Permitted	**Yes**	**No**	**Unknown**
Theft or loss of a BYOD device	73.2%	14.9%	11.9%
Organization control of BYOD device activity	79.6%	8.2%	12.3%
Unauthorized access to business systems and data	81.0%	10.4%	8.6%
Access controls based on business need to know	73.6%	13.4%	13.0%
BYOD device compliance with policies and regulations	79.2%	10.0%	10.8%
Protection of sensitive information at all times	88.5%	4.8%	6.7%
Data is available when needed on a BYOD device	55.0%	24.2%	20.8%
Social engineering schemes to compromise a BYOD device	63.9%	14.9%	21.2%
Loss or theft of data on a BYOD device	82.9%	7.1%	10.0%
Loss or theft of data in transmission to a BYOD device	78.8%	10.8%	10.4%
Viruses or malicious software that target a BYOD device	83.6%	6.7%	9.7%

References

Adler, M.P. (2006). A unified approach to information security compliance. *Educause Review, 41*(5), 46-61.

Allen, V. (2008). ERP security tools. *The Internal Auditor, 65*(1), 25-27.

Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Armando, A., Costa, G., Merlo, A., & Verderame, L. (2015). Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security*, *14*(2), 123-140.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the "Bring Your Own Device" paradigm. *Computer, 47*(6), 48-56.

Banham, R. (2013). The shadow knows. *Risk Management, 60*(6), 10-11.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Beeler, J., George W., & Gardner, D. (2006). A requirements primer. *Queue, 4*(7), 22-26.

Castro-Leon, E. (2014). Consumerization in the IT service ecosystem. *IT Professional, 16*(5), 20-27.

Churchill, G. A., Jr. (1979). A paradigm for developing better measures of marketing constructs. Journal of Marketing Research, 16(1), 64-73.

Clark, T. L. (2009). Securing institutional data: Let's make it everyone's business. *ECAR Research Bulletin, 2009*(9), 1-11.

Coggrave, F. (2012). How to tackle digital investigations. *Waters,* 44-45.

Corporate Governance Task Force (2004). Information security governance: A call to action. Retrieved from http://www.cyberpartnership.org/InfoSecGov4_04.pdf.

COSO (2013). Internal Control – Integrated Framework, COSO, San Jose, CA.

Da Veiga, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

Difilipo, S. (2013). The Policy of BYOD: Considerations for higher education. *EDUCAUSE Review March/April*, 60-61.

Dolnicar, S. (2003) *Simplifying Three-way Questionnaires - Do the Advantages of Binary Answer Categories Compensate for the Loss of Information?* Australia and New Zealand Marketing Academy (ANZMAC) CD Proceedings.

Dolnicar, S., Grün, B., & Leisch, F. (2011). Quick, simple and reliable: Forced binary survey questions. *International Journal of Market Research, 53*(2), 231.

Drew, J. (2012). Managing cybersecurity risks. *Journal of Accountancy, 214*(2), 44-48.

Drugescu, C., & Etges, R. (2006). Maximizing the return on investment on information security programs: Program governance and metrics. *Information Systems Security, 15*(6), 30-40.

Dutta, A. & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Dutton, W. H. (2014). Putting things to work: social and policy challenges for the Internet of things. *info*, 16(3), 1-21.

Earley, S., Harmon, R., Lee, M. R., & Mithas, S. (2014). From BYOD to BYOA, phishing, and botnets. *IT Professional, 16*(5), 16-18.

Eisenberg, V., Kallner, S., & Ben-Harrush, I. (2014). *Mobile enablement of business process management suites*. Paper presented at the Proceedings of the 1st International Conference on Mobile Software Engineering and Systems.

Foley, S. N. (2009). *Security risk management using internal controls.* Paper presented at the Proceedings of the First ACM Workshop on Information Security Governance, Chicago, IL, USA.

Fox, R. J., Crask, M. R., & Kim, J. (1989). Mail survey response rate: A meta-analysis of selected techniques for inducing response. Public Opinion Quarterly, 52(4), 467-491.

Girard J. (2013). Top seven failures in mobile device security. Retrieved from http://Gartner.com.

Grassi, M., Nucera, A., Zanolin, E., Omenaas, E., Anto, J. M., & Leynaert, B. (2007). Performance Comparison of Likert and Binary Formats of SF-36 Version 1.6 Across ECRHS II Adults Populations. *Value in Health, 10*(6), 478-488.

Greengard, S. (2014). Missing in Action: BYOD Security. Retrieved from http://www.cioinsight.com/blogs/missing-in-action-byod-security.html.

Gudivada, V. N., & Nandigam, J. (2009). Corporate compliance and its implications to IT professionals. *Proceedings of the 2009 Sixth International Conference on Information Technology*, 725-729.

Harris, P., Kinkela, K., & Hayes, N. T. (2011). Internal auditing developments: COSO studies key risk assessment as a component of enterprise risk management. *Internal Auditing, 26*(5), 11-15.

iPass Inc. (2013). iPass Mobile Enterprise Report. Retrieved from http://www.ipass.com/wp-content/uploads/2013/01/iPass_Mobile_Enterprise_Report_2013.pdf.

Johnson, K., & DeLaGrange, T. (2012). SANS Survey on Mobility/BYOD Security Policies and Practices. Retrieved from http://www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf.

Kamsin, A. (2004). Management of Information Technology: The study on strategy, planning and policies. *Proceedings of the 2004 International Symposium on Information and Communication Technologies ISICT '04*, 152-157.

Kaneshige, T. (2014). What is going wrong with BYOD? Retrieved from http://www.cio.com/article/2375498/byod/what-is-going-wrong-with-byod-.html.

Khoo, B., Harris, P., & Hartman, S. (2010). Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management and Information Systems, 14*(3), 49-55.

Korac-Kakabadse, N., & Kakabadse, A. (2001). IS/IT governance: Need for an integrated model. *Corporate Governance: The International Journal of Business in Society, 1*(4), 9-11.

Kotulic, A.G., & Clark, J.G. (2004). Why there aren't more information security research studies. *Information & Management, 41*, 597-607.

Kumar, R., & Singh, H. (2015). A Proactive Procedure to Mitigate the BYOD Risks on the Security of an Information System. *ACM SIGSOFT Software Engineering Notes, 40*(1), 1-4.

Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28, 563–575.

Lewis, B.R., Templeton, G.F., & Byrd, T.A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems, 14*, 388–400.

Malhotra, N. K. and Grover, V. (1998). An assessment of survey research in POM: From constructs to theory. *Journal of Operations Management, 16*(4), 403–423.

McFadzean, E., Ezingeard, J., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. *Journal of Information System Security, 2*(3), 3-48.

Mertler, C. A., & Vannatta, R. A. (2013). Advanced and multivariate statistical methods (5th ed.): Practical application and interpretation. Glendale, CA: Pyrczak Publishing.

Moon, A. (2013). Press release: BYOD trend drives number of consumer owned mobile devices used at work. Retrieved from http://www.juniperresearch.com/viewpressrelease.php?pr=413.

Nielsen Company (2015). So many apps, so much more time for entertainment. Retrieved from http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html.

Nolan, J. (2005). Best practices for establishing an effective workplace policy for acceptable computer usage. *Information Systems Control Journal, 6*, 32-34.

Nunnally, J.C., & Bernstein, I.H. (1994). Psychometric theory. New York: McGraw Hill.

Oltsik, J. (2012). A multitude of mobile security issues. Retrieved from http://www.esg-global.com/blogs/a-multitude-of-mobile-security-issues/.

Porter, S. R., & Whitcomb, M. E. (2007). Mixed-mode contacts in web surveys: Paper is not necessarily better. Public Opinion Quarterly, 71(4), 635-648.

Posthumus, S., & Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Rainer, Jr., R. K. & Harrison, A. W. (1993) Toward development of the end user computing construct in a university setting. Decision Sciences, 24(6), 1187–1202.

Rhodes, R. & Kaplan, E. (2012). Dictate the mobile device or let the user decide? *Network World, 29*(12), 24-25.

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security, 2014*(1), 13-15.

Rosario, T., Pereira, R., & da Silva, M. M. (2012). Formalization of the IT audit management process. *2012 IEEE 16th International Enterprise Distributed Object Computing Conference Workshops*, Beijing, 1-10.

Sanchez, L. E., Villafranca, D., Fernandez-Medina, E., & Piattini, M. (2006). *Practical Approach of a Secure Management System based on ISO/IEC 17799*. Paper presented at the Proceedings of the First International Conference on Availability, Reliability and Security.

Schaefer, D. R., & Dillman, D. A. (1998). Development of a standard e-mail methodology: Results of an experiment. Public Opinion Quarterly, 62(3), 378-397.

Schuldt, B. A., & Totten, J. W. (1994). Electronic mail vs. mail survey response rates. *Marketing Research*, *6*(1), 3-7.

Semer, L. (2013). Auditing the BYOD program: the growing business use of personal smartphones and other devices raises new security risks. *Internal Auditor*, *70*(1), 23-26.

Singh, K. (2007). *Quantitative Social Research Methods*. SAGE Publications.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment (ROSI) -- A Practical Quantitative Model. *Journal of Research & Practice in Information Technology, 38*(1), 45-56.

Stephens, H. (2012). Keeping data safe. *Business Credit*, *114*(8), 24, 26.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Swibel, M. (2004). Software security wars. Retrieved from http://www.forbes.com/business/businesstech/2004/06/02/cz_ms_0602beltway.html.

Taylor, B. (2013). Use the Key Levers of Process to Ensure BYOD Success. Retrieved from http://www.gartner.com/document/2453015.

Tech Pro Research (2013). BYOD business strategies: Adoption plans, deployment, options, IT concerns, and cost savings. Retrieved from http://www.techproresearch.com/downloads/byod-business-strategies-adoption-plans-deployment-options-it-concerns-and-cost-savings/.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, Processes and Relational mechanisms for Information Technology Governance: Theories and Practices *Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.

Vignesh, U., & Asha, S. (2015). Modifying Security Policies Towards BYOD. *Procedia Computer Science*, *50*, 511-516.

Whitman, M.E. (2003) Enemy at the gate: Threats to information security. *Communications of the ACM*, 46(8), 91-95.

Whitman, M. E., Mattord, H. J. (2013). *Management of Information Security*. Boston, MA: Thomson Course Technology.

Yates, S. (2013). Embrace mobile engagement as a catalyst to drive process change. Retrieved from http://blogs.forrester.com/simon_yates/13-02-05-embrace_mobile_engagement_as_a_catalyst_to_drive_process_change.