Issues in Informing Science + Information Technology

An Official Publication of the Informing Science Institute
InformingScience.org

IISIT.org

Volume 16, 2019

BUSINESS PRIORITIES DRIVING BYOD ADOPTION: A CASE STUDY OF A SOUTH AFRICAN FINANCIAL SERVICES ORGANIZATION

Jacques Ophoff* — Department of Information Systems, University of Cape Town, Cape Town, South Africa — jacques.ophoff@uct.ac.za

Steve Miller — Department of Information Systems, University of Cape Town, Cape Town, South Africa — MLLSTE028@myuct.ac.za

* Corresponding author

ABSTRACT

Aim/Purpose Bring your own device (BYOD) provides opportunities for both the organization and employees, but the adoption of BYOD also introduces risks. This case study of an organization's BYOD program identifies key positive and negative influences on the adoption decision.

Background The consumerization of IT introduced the BYOD phenomenon into the enterprise environment. As mobile and Internet technologies improve employees are opting to use their personal devices to access organizational systems to perform their work tasks. Such devices include smartphones, tablets and laptop computers.

Methodology This research uses a case study approach to investigate how business priorities drive the adoption of BYOD and how resulting benefits and risks are realized and managed by the organization. Primary empirical data was collected using semi-structured interviews with 15 senior employees from a large South African financial services organization. Policy documents from the organization were analyzed as secondary data.

Contribution Thematic analysis of the data revealed six major themes: improving employee mobility; improving client service and experience; creating a competitive industry advantage; improving business processes; information security risks; and management best practices.

Accepting Editor: Eli Cohen | Received: December 8, 2019 | Revised: January 31, April 1, 2019 | Accepted: April 8, 2019

Cite as: Ophoff, J., & Miller, S. (2019). Business priorities driving BYOD adoption: A case study of a South African financial services organization. *Issues in Informing Science and Information Technology, 16,* 165-196. https://doi.org/10.28945/4303

Findings	The themes were analyzed using the Technology-Organization-Environment (TOE) framework, showing the key positive and negative influences on the adoption decision.
Recommendations for Practitioners	Organizations need to clearly understand the reasons they want to introduce BYOD in their organizations. The conceptual framework can be applied by practitioners in their organizations to achieve their BYOD business objectives.
Recommendations for Researchers	BYOD remains an important innovation for organizations with several aspects worthy of further study. The TOE framework presents a suitable lens for analysis, but other models should also be considered.
Impact on Society	The findings show that organizations can use BYOD to improve client service, gain competitive advantage, and improve their processes using their digital devices and backend systems. The BYOD trend is thus not likely to go away anytime soon.
Future Research	The applicability of findings should be validated across additional contexts. Additional models should also be used.
Keywords	Bring your own device (BYOD), IT management, benefits, risks, Technology-Organization-Environment framework, case study, financial services, South Africa

INTRODUCTION

BYOD is a phenomenon that emerged with the advent of smartphones and tablets and enables users to use their own mobile device in the business as well as the personal environment. Zielinski (2012) described BYOD as the concept where individuals were not reliant on company sponsored devices but chose to purchase and use their own mobile devices to connect and process organizational information. Gartner (2012) defined BYOD as "the strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data" (para. 2). BYOD was spurred on by the consumerization of IT where consumer devices made their way into the corporate world.

Many organizations allow their employees to connect to their wireless networks to access resources and stay connected in meetings and presentations. The variety of applications for business and personal use allows the mobile device owner to use the device for multiple functions. The advancement of these multifunctional mobile devices includes increased processing power that allows users to complete functions they previously were only able to undertake on their desktop computers (Couture, 2010). Businesses have come to realize that BYOD provides benefits that include increased employee productivity, work flexibility and the cost reduction for IT (Wood, 2012).

Although there are many benefits associated with BYOD there are also risks that need to be mitigated. Chen and Nath (2011) highlighted the risks that personal mobile devices introduce to the corporate network. If these devices are lost, stolen or the organization does not have the appropriate security controls in place the sensitive business data stored on the device will put the business at risk. These compromised devices could be used to gain unauthorized entry into the organizations network through exploitation of a direct connection. Loss of sensitive data leaves businesses vulnerable to financial losses, reputational damage and losing their competitive advantage (The Ponemon Institute, 2012).

In the past corporate information was stored within the organizational perimeter secured by firewalls and at a fixed location. In the digital age that businesses now operate in information is processed and sent to staff members and clients globally. This sensitive information is processed and resides on

personally owned mobile devices of employees that have chosen to have more flexible working tools (i.e., BYOD). The risk is that organizations have little control over BYOD in terms of where these devices move, and the potential loss of the data stored on them (Calder, 2013).

BYOD research frequently focuses on strategic analysis of expectations and capabilities. A smaller body of prior research covers strategy design, while very little is found in implementation and evaluation of BYOD (Brodin, Rose & Ahlfeldt, 2015). Organizations that do not understand the business objectives that drive BYOD adoption will not be able to effectively identify the appropriate requirements to build a BYOD strategy. These organizations will not be able to clearly justify the costs associated with the implementation of the BYOD strategy as well as the changes to business processes (Rose, 2013). Proper planning and management of the BYOD strategy would lead to limiting not only the costs of implementation, but also the security risks associated with the utilization of this facility. The objective of this research is to understand and examine the adoption of BYOD within a South African context. To achieve this objective the study is guided by the following primary research question: *How do business priorities drive the adoption of BYOD in the organization?*

This remainder of this paper is structured as follows. The next section provides a literature review as theoretical basis for enterprise mobility and the BYOD concept. Based on a systematic review approach it highlights the importance of the trend and how it can benefit organizations as well as employees. The risks and operational concerns of BYOD are then identified and the controls to effectively deal with BYOD risks are covered. Next the theoretical framework is discussed, which guides subsequent analysis of the results. Thereafter the research methodology is discussed. The findings are presented, analyzed and discussed next. Lastly conclusions are drawn, along with future research opportunities.

LITERATURE REVIEW

Employees often feel frustrated with issues related to traditional infrastructure in the organization. However, with consumerization of IT employees can experience IT in an enjoyable and efficient manner by also selecting a device with hardware and software specifications that meets their criteria (Baskerville, 2011; Weiß & Leimeister, 2012). This contrasts with the traditional infrastructure called Company-Issued Personally-Enabled (COPE) where employees had to accept the devices provided by the company. A middle ground is provided by Choose Your Own Device (CYOD) where employees have a choice between a small number of company-approved device options. The differences between CYOD and BYOD include ownership, user satisfaction, integration into business systems, etc. The models have their pros and cons and the suitability of the chosen model depends on the user or the organization's requirements.

ENTERPRISE MOBILITY

Ghoda (2009) has defined enterprise mobility as the ability for organizations to operate in both the traditional business sense based on fixed location and the new virtualized business where the location is irrelevant. Enterprise mobility allows employees to access organizational information, collaborate on projects with different teams and process information via wireless networks, broadband and satellite connections and services. Disabato (2016) has stated that enterprise mobility does not only relate to the technology within the organization but how technology is incorporated into the business strategy and business processes. According to Disabato (2016), enterprise mobility must be used to generate new business opportunities, improve client relationships and extend business processes to cater for mobile functionality. Basole (2007) has stated that enterprise mobility is the product of consumerization of mobile device technology within the organization and will change how business is conducted. Configuring the mobile technology within an organization does not mean that it is a mobile organization but determines how the organization operates.

Access to information from mobile devices reduces dependence on working from fixed locations and allows users to operate freely wherever they are. Typical mobile activities include accessing business emails and calendars, managing documentation and accessing customer relationship management systems and accessing intranet portals. Mobility cannot be achieved by infrastructure alone, but organizations must establish strategies to provide for access to the various internal systems that will allow employees to complete their daily tasks (Unhelkar & Murugesan, 2010).

Information and communication technology (ICT) advancements in the mobile space have opened new possibilities that can improve business processes and deliver more business value (Kornak, Teutloff, & Welin-Berger, 2004). Even though the benefits of mobile ICT are available not all organizations have adopted this strategy due to the risks that include security, privacy and other technology issues. Despite such risks, organizational competencies and strategies built around mobility can pave the way for an organization to access different markets and industries.

Benefits of BYOD

It is thought that BYOD brings several perceived benefits to the organization and its employees. Liljander and Strandvik (1992) have defined perceived benefits as the benefits the consumers perceive they will receive. In the context of BYOD, perceived benefits reflect the overall benefits employees and organizations expect this technology will provide. With BYOD programs direct benefits are tangible and immediately available, for example, cost savings to the organizations and increased productivity (Calder, 2013). Indirect benefits are less tangible and include employee satisfaction and using BYOD programs to attract and retain employees (Weeger, Wang, & Gewald, 2016). The benefits associated with BYOD are discussed in more detail below.

Employee satisfaction

In market research that has been conducted among the stakeholders of organizations, nearly 60% of the respondents indicated that job satisfaction among their staff was a factor in adopting the BYOD strategy (Citrix, 2011). This was found to be particularly true for the younger generation of employees who have grown up with technology and are generally more tech savvy than their older colleagues. The motivation of the organizations employees is strongly linked to the success of the business since high employee morale results in improved productivity. It has also been shown that organizations which have a BYOD program are more attractive to employees (Weeger et al., 2016).

Employee productivity and accessibility of data

One of the benefits that the BYOD concept provides to a business is that it allows corporate data to be readily available, via laptops, smartphones and tablets, to those employees who are travelling outside of the office. The accessibility of the corporate data by the employees allows businesses to provide better services to their clients. For example, a study of IT users that use laptop computers discovered that these users were, on average, 50 minutes more productive on a usual day, than those users that had desktop computers (Calder, 2013). Employees have indicated that being able to select their own mobile device and the technology that suits their individual requirements has enabled them to be more efficient. The increase in productivity has been due to the device, the operating system installed on it together with other mobile applications, and cloud services available on this device.

Cost savings for the organization

In a business that decides to follow the BYOD trend the employee purchases the mobile device themselves which translates into significant savings for the organization regarding procurement and training (Wood, 2012). Wood (2012) states that many organizations list cost savings as their number one reason for adopting a BYOD strategy. The annual cost of upgrading existing technology and purchasing new equipment for an organization is significant, and saving costs is vital for businesses to operate in this global economy. When employees provide their own tools, these costs are for their

own account. Having paid for a device themselves employees are more likely to take better care of these devices than the company issued assets. Support costs that would be borne by businesses are further reduced when employees support their own devices.

Even though organizations may save on the costs of the devices and support thereof, costs of security and compliance for BYOD will increase (Twentyman, 2012). As the risks associated with mobile devices are increasing, organizations need to ensure that their data, as well as the privacy of their employee's data, are secured. In the next section the importance of information security will be discussed as it relates to the risks associated with BYOD.

Risks Associated with BYOD

In the current information age organizations rely heavily on their information systems to operate successfully. Organizations need to manage the risks that accompany these connected systems and networks. A risk can be defined as the possibility that a threat could exploit a vulnerability and thus cause damage to the organization (Whitman & Mattord, 2013). Security threats are a major risk and information security is rated as a major business priority (Percy, 2018). Information security is the process of protecting information and ensuring that only authorized users (confidentiality) have access to accurate and complete information (integrity) when needed (availability) (ISACA, 2008). The three components are often referred to as the CIA triad (Whitman & Mattord, 2013). Confidentiality ensures that only the authorized users have access to the information. Integrity is the characteristic that is accurate, trustworthy information that has not been tampered with or modified unknowingly. Availability is having the information ready for the authorized users when required. Information security is vital when employees use their personal mobile devices to connect to their organization's network infrastructure that contains confidential corporate information. In addition, the mobile devices used by employees often have sensitive business information stored on them which, if lost or stolen, is a risk to the organization.

With the use of BYOD there also comes a certain level of risk. Bauer (1967) has introduced perceived risk in the perceived risk theory which analyzed how individuals consider the risks associated with their actions and the consequences thereof. Cunningham (1967) stated that the theory assumes the perceptions of risks have a bearing on an individual's intention to complete an action. Stone and Gronhaug (1993, p.42) define perceived risk as a "subjective expectation of a possible loss". Perceived risk theory could be used as a basis to explain employees' behaviour in adopting BYOD and their actions using the mobile devices when faced with decisions that could impact the privacy of their data and the security of the organizations systems, network, and data. Perceived risk has been a major factor in how users intended to use IT systems (Featherman & Pavlou, 2003; Liu, Yang, & Li, 2012)

Six types of perceived risks have been noted: financial, privacy, performance, social, physical and time-loss (Jacoby & Kaplan, 1972; Kaplan, Szybillo, & Jacoby, 1974; Roselius, 1971). Featherman and Palvou (2003) state that the dimensions of perceived risk may differ for product or service. Several risks that the BYOD concept has introduced into organizations are discussed next.

Data loss

Calder (2013) states that one of the main risks of BYOD is the loss of confidential data that has been stored on the mobile devices. The loss of the mobile device presents a criminal with an opportunity to exploit the organization's confidential information, creating a severe security risk for the organization. When devices are not configured with the basic security measures, such as locking the device with a strong pin, requiring a password to enter the device, or encryption of sensitive data, it is easy for a criminal to gain access to this information. Managing these issues using data loss prevention software is a difficult but important process (Dhingra, 2016).

Another issue with data loss is data leakage where the affected user is not aware that data is being misused and the user cannot minimize risk until it is too late. The Ponemon Institute (2012) reports that on average it costs an organization 7.2 million US dollars per data breach and on average 214 US dollars per compromised record. Organizations need to ensure that their internal controls are effective at protecting the sensitive information of their clients. Failing to safeguard this data could have the organization suffering financial losses, legal action and, depending on the severity of the breach, this could cause reputational damage to the business. This in turn could affect their ability to be competitive and conduct business in the future.

Malware

Malware which is short for malicious software is a piece of software code that infects computer systems, causes disruption to the services, gathers sensitive information without permission and causes damage to the device (Moir, 2009). Malware allows criminals to steal sensitive information from computers, like password and credit card information. In some severe cases malware can infect computer systems and mobile devices allowing hackers to control these devices and systems. Tzoumas (2013) explains that malware and viruses are usually accidentally downloaded to the mobile devices. These viruses can cause havoc when they spread onto the company networks. These malicious programs can easily find and open back door entry points to servers and databases allowing hackers to steal organizational data. This usually goes unnoticed before it is too late. As more businesses adopt the BYOD concept, the malware that affects mobile devices has also increasingly been targeting tablets and smartphone software (Drew, 2012; Kaspersky, 2012; Ponemon Institute LLC, 2012). Traditional security measures which organizations usually provide such as firewalls and antivirus software may no longer be effective at preventing malicious infections from entering the organization via mobile devices (Ponemon Institute LLC, 2012). The Cisco (2013) survey highlighted that 69% of BYOD users had personal applications on their devices that were potentially dangerous. If the appropriate control measures are not put in place sensitive corporate data, on the network and BYOD devices, could be at risk to malware attacks which could have a negative impact on the business.

Device misconfiguration

Unlike the traditional desktop computers that are situated on the premises of the organization and managed by the in-house IT department, BYOD devices are owned and managed by their users. This allows the owner of the device to configure the device to their own preferences, which could leave the device vulnerable to attack. The danger being that all mobile users will not have the knowledge required to secure their devices configuration settings appropriately. Landman (2010) believes a significant number of security incidents in the organization stem from BYOD devices that are not configured correctly with the appropriate security controls. Some employees that may not be aware of the BYOD and information security policies, or that deliberately violate the policies, can cause significant risks for the organization (Landman, 2010).

Software vulnerabilities

Whitman and Mattord (2013) define vulnerability from an information security viewpoint as an identified flaw within a system that can be exploited. The IT department does not have full control with BYOD making it difficult to monitor and control these devices. As the sales of smartphones and tablets are increasing cyber criminals are targeting these devices and exploiting vulnerability in the software installed and downloaded to them. Malicious applications are downloaded by employees who are often unaware of the dangers such software creates to the information stored on the device. The vulnerabilities allow viruses and malware into the device, which increases the chance of data leakage and data loss. To alleviate some of the known priority security issues the top vulnerabilities need to be patched to prevent exploitation by criminals.

Wireless connectivity weaknesses

The ease of connectivity to the World Wide Web, organizational systems and social networks is one of the reasons that mobile devices have become so popular. These devices that depend on the cellular network offer impressive internet connection speeds via 3/4G network technology. These devices offer wireless connectivity to access work resources at the office or at home, and the devices have Bluetooth connectivity for data sharing and to enable connections to various other devices. Anderson (2014) stated it could be possible for unauthorized users to gain access to organization data if they are tethered to an authorized device connected to the company network. The Bluetooth and wireless technology that these devices have built-in has been known to be exploited, without difficulty to infect the mobile devices with malware or intercept sensitive data being transmitted (IBM, 2011). When BYOD users are connected to insecure networks the data transferred by the device is susceptible to 'man in the middle' attacks, where the hacker can intercept the data being communicated.

When the Bluetooth option is set to discoverable on a mobile device, criminals can scan for vulnerable devices, and once connected to the device they are able to access stored personal information (Cisco, 2013). BYOD users who access these Bluetooth and wireless technology networks should be aware of the dangers that exist when connecting to untrusted connections and networks.

Applications downloaded from the web

Apps (short for applications) have become very popular in recent years as developers have been creating software for smartphones and tablets for a multitude of purposes and interests including but not limited to information retrieval, productivity, social networking, weather and games. There are 2.1 million apps in the Google Play Store and 2 million apps in the Apple App Store (Statista, 2019). Generally, it is safer to download applications from an app store than from web site links. However, malware can be planted within applications from these stores as well (Botha, Furnell, & Clarke, 2009). Smartphone and tablet owners must not accept that all apps within the App Stores are safe anymore and should rather do their own research first by reading reviews of the apps they are contemplating downloading first (Botha et al., 2009). IBM (2012) stated that with the number of applications being added to these App stores it is not be possible for App Store administrators and owners to conduct in-depth analysis of the software code for each application. This leaves the possibility that users who download from these App stores, may still download and be infected with malware and other viruses. Careful consideration needs to be taken before downloading applications, as infected BYOD devices can cause havoc with the network infrastructure of an organization.

Operational risks (support issues)

It has been shown that the availability of an IT support team has a positive impact, especially on employee's intention to comply with BYOD security policies (Hovav & Putri, 2016). Traditionally IT departments in a non-BYOD environment supported devices and systems that were all located at the premises of the organization. The IT department was responsible for installation, configuration and maintenance of the hardware and software owned by the organization. All infrastructure was standardized which made supporting such an environment relatively easy. Rose (2013) indicated that it was becoming increasingly difficult for IT departments to support a wide variety of mobile device models and software versions. The IT staff in such an organization would need a substantial amount of training and expertise to support all the different mobile devices. The nature of mobile devices allows the members of staff who own them to operate the BYOD device from any location if an internet connection is available. When employees have trouble operating their devices and need support away from the organization's offices this adds more difficulty since the IT team is expected to provide advice and support telephonically without being able to assist the user face to face. BYOD devices that have not been configured properly by the organization's IT team run the risk of becoming infected with malware that could cause problems for the device and affect sensitive corporate data (Moir, 2009). Enterprise mobility has altered the way IT teams now operate and IT teams that

adopt a BYOD strategy are expected to have the knowledge to support the various models of BYOD devices the organization allows on their corporate network. IT Teams that do not have the processes and procedures in place to support the organization's BYOD program will see an increase in operational risks.

Hidden BYOD expenses

Although benefits of mobility and BYOD include employee satisfaction, increases in productivity and cost saving for the organization there are also less obvious increased expenses that the organization will have to consider (Rose, 2013). With an influx of employees wanting to use their mobile devices within the office environment the organization will need to consider additional infrastructure including Wireless access points to allow these devices to connect to information systems. Depending on the agreement with the organization additional telecommunications charges, including voice and data, will be for the employee or the organizations account. The company will need to plan for the increased bandwidth required for mobile device communication, without it negatively impacting on the existing infrastructure that was in place prior to allowing BYOD on the network. Mobile Device Management (MDM) systems and other security controls that are used to manage mobile devices are expensive (Kaneshige, 2012). This includes setup costs of the MDM system, yearly license fees for the number of devices, and the infrastructure to host the MDM solution. According to industry research BYOD costs businesses 33% more than CYOD/COPE due to loss of bulk discounts, expense reimbursements, manual compliance checks, help desk support, and multi-platform support (Kaneshige, 2012).

Managing BYOD

In the past organizations relied solely on technical solutions to limit the risks to information loss and ensure information security (Ernst & Young 2008). These technical control measures do improve the information security for businesses, but this approach alone is not enough. Success can only be realized if both the technical and socio-organizational aspects are considered and addressed (Cavusoglu, Cavusoglu, Son, & Benbasat, 2009). The following sections examine policies, education and awareness, security culture, and mobility management.

Policies

The first step that an organization needs to take when preparing to allow BYOD, is to create an explicit policy outlining all the rules and regulations that employees must adhere to if they would like to use their own devices on the corporate network. The policy needs to include the appropriate level of detail and be very clear for the users, as this aspect affects the users' view of the security issues to which the organization is exposed. Purser (2002) recommends that the policies be written clearly and address the topics in a specific manner that is understandable to all users that need to comply with the policy. Once the policy has been finalized the policy needs to be distributed to all users who then need to familiarize themselves with the information within the document and sign off that they understand and will adhere to the acceptable use of the information systems described in the policy.

The policies need to be carefully designed to balance productivity as well as cater for the various risks associated with this technology. The security team and the business users need to agree on the design of the BYOD policy. Mansfield-Devine (2012) warns that if the IT security team does not involve the business users, then the users will find the BYOD policy restrictive and will be less likely to adhere to the policy. In some cases users will find ways to bypass these restrictions. Only devices that meet the requirements of the policy should be allowed to access the company network.

Education and awareness

Morrow (2012) believes most of mobile security incidents are because of employees not being aware of the dangers of cybercrime and recommends that organizations should invest in educating their

employees about the information security and compliance with the organization's policies. The most expensive and elaborate technical controls will be ineffective if the employees do not follow the best practices for using mobile devices and guarding information security. These steps will protect their personal information as well as the business data. As more individuals use their mobile devices within the organization, if cybercrime incidents continue to increase, management will need to ensure that their employees receive regular information security and awareness training. Mansfield-Devine (2012) stated that it is crucial that employees form part of the organization's overall security design. The organization's security is only as strong as its weakest link and technical controls alone are not enough. Organizations need to have a balance of both technical and non-technical controls to ensure the robustness of the information security posture of the organization. Albrechtsen (2007) highlighted that employees often do not follow information security policies and procedures and that other work-related tasks take preference over security. Post and Kagan's (2007) study indicated that an employee's perception of practicing security was a hindrance that kept them from doing their main duties and reduced their productivity. Siponen (2000) argues that employees need to be given all the facts of why information security was vital to the business and themselves, in a logical and rational manner, to improve their understanding. This approach will assist in the compliance of employees with policies and guidelines.

According to Albrechtsen and Hovden (2010) organizations that have users participate in regular information security discussions and group training have seen positive results in their employees' awareness and behavior towards risks. Workshops and training need to be used to provide the information in a concise and effective manner to hold an employee's attention. Kim and Homan (2012) established that computer-based information security training has been more effective than instructor-based training: those employees that had received computer training retained much more of the information provided to them after a 60-day period, than those employees who did not. However, after 90 days, the information retained from both types of training was similar, which should prompt organizations to have more frequent sessions, to remind users of the threats and of how to conduct safe digital behavior. Albrechtsen and Hovden (2010) believe workshops and training that were not found interesting or motivating by the employees were very unlikely to improve the secure behavior of users. Hagen, Albrechtsen, and Johnsen (2010) highlights the previous statement as they recommended building an entertaining aspect into information security education programs because it is a major factor that ensures employees and users are involved and motivated in the sessions. The training provided by the organization will assist the employees to make responsible decisions when downloading applications, to avoid connecting to insecure free public Wi-Fi networks and avoiding suspicious website links.

Thomson, von Solms, and Louw (2006) argued that employees that are well trained to appreciate the importance of securing the organization's information assets are the organization's strongest and most effective component of the information security program. These employees do not need to be experts in this field or have any technical certification, but they do need a basic understanding of the concepts, to minimize risk in their daily functions. Practical examples should be used when training staff members on the policies and procedures of the information security policies.

Information security culture

Every organization has its own specific culture, which consists of shared values, behaviors and beliefs that direct and shape members behaviors and attitudes in organizations (Smit & Cronje, 1992). The human side of information security deals directly with the corporate culture of the organization and how employees view the organization and their role within the business. The employees' individual values, beliefs and knowledge about the organization's information security create the Information Security Culture (ISC). Both internal and external security measures must be in place to ensure an organization's sensitive information is protected, and one side should not exist without the other.

Thomson, von Solms, and Louw (2006) states that even though it might not be easily recognized every business has its own corporate culture that can be used as a guide for the practices of its employees. The employees' attitudes and beliefs towards information security are largely determined by the corporate culture of the organization. It is vital that management places a high priority on improving the information security culture by driving awareness of the importance of information security as one of the organizations goals. Beach (1993) believes security culture in organizations guides the activities of employees and a clear distinction needs to be drawn between acceptable and unacceptable behavior. Schein (1999) stated that corporate culture changes are often painful exercises, resisted and challenged continuously until employees are persuaded by the management hierarchy to accept the changes. For the successful implementation of information security programs within the organization the message must come from the executive board all the way down the management hierarchy. Schlienger and Teufel (2003) suggested a four-staged strategy based on top management commitment, the effective communication throughout the organization, awareness and training programs for employees and buy-in from all staff. ISC still remains one of the top concerns of practitioners and academics alike (Kolkowska and Dhillon, 2013).

Enterprise mobility management

Enterprise mobility management (EMM) is a comprehensive platform for enabling the secure use of mobile devices including smartphones and tablets. EMM is the collection of people, processes and technology dedicated to managing these devices, the wireless networks they connect to and the other services that contribute to the use of the mobile devices for business purposes (Pinchot & Paullet, 2015). The need for EMM systems has increased with the number of privately-owned mobile devices (BYOD) that have been entering the corporate environment over the last few years and there is no sign of this need reducing. The EMM technical system typically has three main components which include mobile device management (MDM), mobile application management (MAM) and mobile information management (MIM).

MDM software tools assist organizations to manage the mobile devices that connect to their business' network infrastructure (Ghosh, Gajar & Rai, 2013). These MDM tools provide features that include device management, security configuration, and policy enforcement on the mobile devices, remote wipe of the data stored on the device and data encryption. These features allow the organization to securely manage, monitor and control each device to minimize threats to the employee's and the organization's data.

MAM provides organizations with mechanisms to deliver enterprise software applications to personally owned and corporate sponsored mobile devices and enables the organizations to improve the management of the business applications and data on these devices (Rouse, 2014). MAM functionality includes software deployment, software licensing, software configuration, maintenance, policy enforcement and usage tracking. IT administrators can also use MAM to remotely wipe application data and organizational data from mobile devices without affecting any of the users' personal data (Mathias, 2015).

MIM is a device-agnostic security strategy that focuses on protecting sensitive business information by separating it from personal data and containerizing it, then only allowing authorized users and applications to access it. This is accomplished using encryption (Mathias, 2015).

The preceding discussion has largely ignored the impact of organizational size. However, it's important to note that risks and benefits may be experienced differently in small- and medium-sized enterprises (Baillette & Barlette, 2018). Furthermore, demographic factors (such as gender, age, and education level) may also play a role in BYOD adoption (Cho & Ip, 2018). Despite the risks associated with BYOD organizations have continued to allow employees to use mobile devices because the benefits seem to outweigh the risks.

THEORETICAL FRAMEWORK

To explore the issues discussed in the literature review in the context of our case study organization we use the Technology-Organization-Environment (TOE) Framework. It is an organizational-level framework which explains that three key areas (namely technology, organization, and environment) affect the adoption and implementation of new technologies and innovations (DePietro, Wiarda, & Fleischer, 1990).

The technological context focuses on internal and external technologies relevant to the organization. This can include infrastructure as well as processes. Technologies can already be in use within the organization or available but not currently in use. Existing technologies may limit the change and innovation an organization can undertake (Collins, Hage, & Hull, 1988). Innovations can crate three forms of change, namely incremental, synthetic, or discontinuous (Tushman & Nadler, 1986). Depending on the organization's existing EMM strategy BYOD could be producing synthetic (moderate) change, but more like represents a radical innovation or discontinuous change. BYOD would likely be classified as competence-enhancing (Tushman & Anderson, 1986) as it allows the organization to find new efficiencies in processes.

The organizational context concerns the characteristics and resources of the organization, including size, human (and slack) resources, employee linkages, management structure, and internal communication processes. In this context linking agents (product champions) and mechanisms that span internal boundaries could promote innovation (Galbraith, 1973; Tushman & Nadler, 1986). Management also plays a key role in fostering an innovation-friendly environment (Tushman & Nadler, 1986).

The environmental context includes the industry context, competitors, presence or absence of technology service providers, macroeconomic context, and regulatory environment. Competition may stimulate the adoption of innovation (Mansfield, 1977). While organizations in rapidly growing industries tend to innovate it is not clear that this holds across the entire industry life cycle (Baker, 2012). In terms of support infrastructure, the cost of skilled labor could also influence labor-saving innovations (Levin, Levin, & Meisel, 1987). Finally, government regulation (such as privacy requirements) can either encourage or discourage innovation (Baker, 2012) and potentially have a significant effect when considering the risks associated with BYOD.

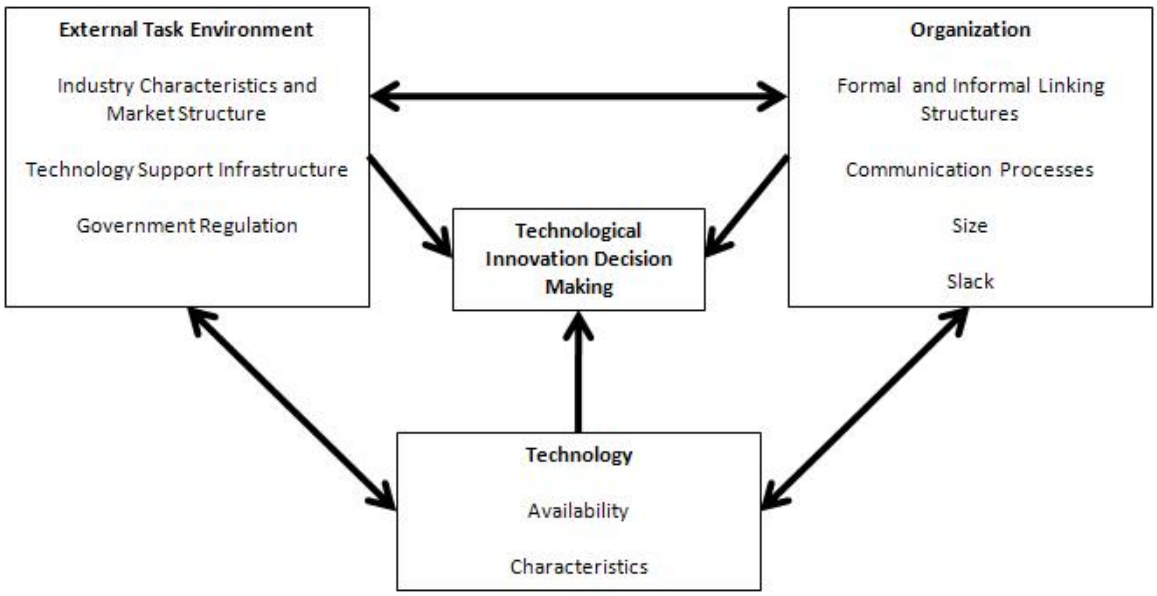

Figure 1. The Technology-Organization-Environment framework

Figure 1 provides a visual representation of the framework. The elements present "both constraints and opportunities for technological innovation" (DePietro et al., 1990, p. 154). A review of published research shows that the framework is applicable across a range of technologies, industries, and national contexts (Baker, 2012). In a study similar in context to the present, the framework was used to examine the adoption of cloud computing in the South African financial services sector, with good model fit (Abrahams, Ophoff, & Mwalemba, 2015). Taking the above into consideration we therefore argue that the framework also provides a suitable lens for this research.

This research does not adopt existing factors for the technological, organizational, and environmental contexts. Rather we use these contexts to frame the situation in an existing organization, using a case study strategy. The methodology that was used is described in the next section.

RESEARCH METHODOLOGY

The research followed an interpretivist approach to gain a deeper understanding of the phenomena by gaining the insights from IT and Business professionals involved in BYOD programs. According to Klein and Myers (1999, p.69) interpretivism proposes "that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meanings, documents, tools, and other artefacts". This research paradigm allowed the researchers to gain a better understanding of the phenomena being investigated. It allowed for deeper insights of the participants involved including their perception and experience of the BYOD in the organization.

An inductive approach to theory was used as the researchers observed the phenomena being studied. Cavana, Delahaye, and Sekaran (2001) defined the inductive approach as one that starts with data collection then analyzing of the data for themes to ultimately develop theory.

RESEARCH STRATEGY

Yin (2013) indicated that there are five research strategies namely survey, experiments, ethnographic, action research and case study. Selecting the research strategy depends on various factors like the research question, how the research will be conducted, and the environment being investigated. The case study approach was selected as the most appropriate strategy to conduct this qualitative study. The case study strategy allows the researcher to study the subject in detail within its real-life context, where the existing knowledge is limited, and phenomenon being studied is broad and complex (Darke, Shanks & Broadbent, 1988). A single case study was used to allow the research in-depth investigation and understanding of the situation being experienced in the organization.

Case site

The case study was conducted within a large financial organization. The organization referred to hereafter as Organization X is one of the largest financial institutions in South Africa with branches in the United Kingdom, United States of America and a few countries in Africa. The business offers financial solutions that include insurance, financial planning, retirement and investments products and services. The organization employs approximately 8,000 staff with the bulk of them situated at the company's head office in South Africa and the remainder at the branches and business units globally. The case site was their head office, located in the Western Cape region of South Africa.

One of the researchers has been employed at Organization X for several years and understands the company culture. Organization X is one of the biggest financial services companies in South Africa. The company comprises of many different business units that collectively form Organization X. As a financial organization that invests clients' savings, pension fund and other investments information security and privacy is of utmost importance to the organization and its clients. A core part of the business' revenue comes from the sale of financial products and the administration fees which the organization charges their clients for the administration of the clients' funds and investment portfolios. The organization has recently launched their BYOD program to allow their mobile sales staff to

stay connected to the organization systems when they operate outside the office. Other employees and executives within various other business units of the organization have also started using their own devices to connect to the various applications and systems. Approximately 14% of total staff at Organization X use mobile devices.

Participants

Non-probability (purposive) sampling was used to select participants. The participants all had extensive knowledge and experience in the fields of finance, mobility, and information security and are the key decision makers and advisors in these domains. The participants were chosen because they were either directly involved in the strategies and decision making for the mobility program and the introduction of BYOD or they were important users of the mobility program. Interviews were conducted over a period of two months during 2015 with 15 participants (abbreviated P1-P15 hereafter) in the following positions:

- Key role players responsible for the information security of the organization,
- Individuals involved with mobile technology decision making including business management.
- Employees that use mobile devices for work tasks.

All participants had more than three years' experience in their current position and overall experience ranged from 12-31years (average of 21.4 years).

Data Collection Techniques

The data was collected by means of interviews and organizational documents like policies, procedures and other artefacts. For the interviews an interview schedule that consisted of semi-structured interview questions was used (included as an Appendix). Myers (2013) defined a semi-structured interview schedule as a list of predefined questions that can be used as a guide during the interview with the participant. This type of interview schedule allows for further questions to be asked based on the response of the participant allowing for deeper information to be extracted. The questions in the interview schedule were designed to explore issues around the research objective and the research questions using existing literature on success and challenges of mobile devices. Organizational documents that included policy documents were also collected and analyzed to supplement interview data.

Data Analysis

Each interview was imported into a Computer Assisted/Aided Qualitative Data Analysis Software (CAQDAS) tool. CAQDAS are software packages which comprise of a set of tools that interprets the qualitative data into themes. The types of qualitative data included text, images, audio and video content (Lewins & Silver, 2009). The CAQDAS tool that was used in this research report was the NVivo 10 package (http://www.qsrinternational.com/). While similar tools exist, NVivo is widely used and has extensive qualitative analysis features (Leech & Onwuegbuzie, 2011). The CAQDAS package included a combination of the following tools: content searching tools, querying tools, coding tools, linking tools, mapping or networking tools, writing and annotation tools.

Thematic analysis was used to categorize, organize and code the data into themes to identify patterns and relationships (Braun & Clarke, 2006). Thematic analysis consists of the following stages: data familiarization, code generation, searching process for themes, reviewing process of themes, naming and defining themes and report production (Braun & Clarke, 2006). In the data familiarization stage, the interviews were read multiple times to understand the content before it was transcribed. During the second stage the research identified patterns that reoccurred in the data, called codes. The code generation process evolved over the period of data analysis to refine the final list of codes. The theme searching process involved using the codes to create themes within the data set. In the fourth

stage of this process themes were refined by ensuring that the coded data related to the themes and the researcher reviews patterns between themes by using a thematic map. The naming and defining themes stage involved an iterative process for reformulating the themes to represent the analysis.

FINDINGS AND ANALYSIS

The participants of the study listed numerous reasons for adopting BYOD as illustrated in Figure 2. The number one reason these participants participated in the mobile program were for communication purposes and to access schedule information. Besides listing communication as the main reason for the mobility usage, many also stated that mobile communication was the main reason staff in their respective business units wanted to have access to the mobility program. The second biggest reason the participants of the study wanted access to the mobility program was to gain access to the organization's Wi-Fi network for Internet access when they moved inside the company premises with their mobile devices e.g., attending workshops and meetings. If these users used a laptop those devices would by default be setup for Wi-Fi access but mobile devices including cellular phones and tablets needed special authorization from the individual staff members' direct manager to be granted Wi-Fi access on those devices. Of the participants only two used their mobile device to access the SAP ERP applications/sites to request and approve leave for staff that report to them. Two participants used the mobility program to access the financial approval systems for large approvals when out of the office. The mobile applications developed by the business to provide product information and that allowed financial advisors with functionality to provide financial advice and products to clients was also used by two participants. Only one participant used the calendar feature to keep track of his scheduling information and used this option only because he did not want to process work emails on his personal device. The other reasons included accessing SharePoint sites from mobile devices and reviewing large documents on mobile instead of printing the documents.

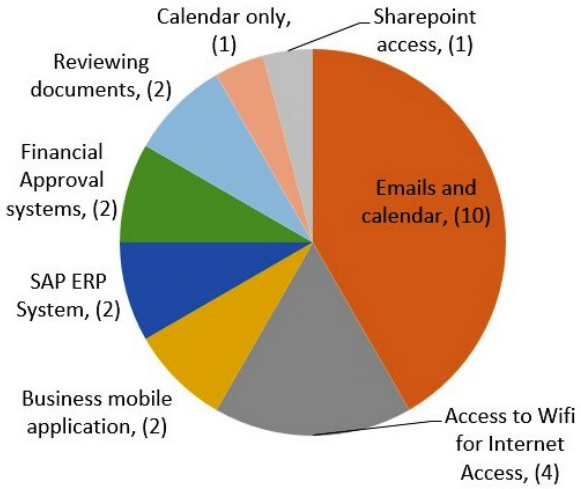

Figure 2. Reasons for BYOD participation

THEME 1 – MOBILITY BENEFITS

The first theme relates to the increased experience of mobility by employees. The literature shows that the main benefits provided by BYOD is the ability for users to connect to organizational systems irrespective of their physical location allowing them stay connected which provides production benefits for the organization (Calder, 2013). Subthemes include the importance of mobilizing the workforce, the resulting effects on productivity, and moving to a digital (paperless) environment.

Subtheme 1 – Mobilizing the workforce

Most of the participants agreed their organization's enterprise mobility strategies needed to align to the overall organizational objectives. When participants that were involved in the mobility decisions, especially around BYOD, were questioned about their businesses mobility requirements their responses varied and were all suited to their individual business needs, but all agreed on the importance of mobilizing the workforce. Most of the participants also agreed that going mobile was going to become standard in future and with employees bringing their own devices to work they needed to embrace the change.

All participants stated that the organization's mobility program allowed their mobile workforce to be more flexible by enabling them to stay connected when they were out of the office. Traveling executives were now able to stay connected with their teams by responding to important emails, completing large financial approvals on the financial system and gaining access to vital information while away from the office.

Most of the participants of the study agreed that BYOD and mobility is going to have a massive impact on the South African economy. The advances in technology allow businesses to get more work done in less time. Transactions can be completed by mobile workers faster than before. BYOD and mobility make collaboration of different individuals much easier by allowing them to communicate in real time irrespective of city, country or continent. Mobile devices allow employees to not be restricted by core working hours only so more production gets completed for the business which ultimately drives revenue.

All participants agreed that mobility was vital for the modern organization. The organization needs to allow its mobile staff to work with the tools and from any location user is comfortable with when they are not at the office. Mobility allows mobile workers to have access to corporate information quickly which enables them to make decisions faster.

Subtheme 2 – Productivity effects

P2 said that having the BYOD program they have seen their staff being more productive. *"This meant configuring their information systems to have online capability for quotations of their products and front office processes"*. These systems needed offline capability as well so that when the mobile worker did not have internet access they could capture information then as soon as they could establish a connection synchronize the data back to the organizations systems. P3 agreed stating that he believed enabling the organizations' workforce to be more mobile meant this allowed them to be efficient, so they could assist clients more effectively. P9 stated: "*As mobile devices and data become cheaper more users will be using mobile devices for business and personal reasons. BYOD allows the users to work with devices that they are more comfortable with which relates to more productive work being completed."*

Participants noted that they needed to capitalize on the BYOD phenomenon so that the company could make use of what the employees already had which were their personal mobile devices so that these could also be used for business purposes.

Mobile devices allow employees to increase their productivity by allowing them to access information and complete their daily tasks irrespective of where they are. P4 noted that these mobile users were much more productive because their mobile devices allowed them to communicate with clients and other employees wherever they were without the need to first come back to the office to respond to communication. The P4 also noticed an increase in productivity since BYOD and CYOD are allowed. The surprise finding that decision makers had not predicted was the amount of after-hours work that was being completed by staff. P2 noted: *"One of the facts that we did not envision before launching the mobility program was the amount of work staff are doing after hours in their personal time."* and P5 said: *"I find it easier to answer emails in the evening in the comfort of my own home which makes me more prepared for the days' work when I come back into the office the next day and I can get straight into working on my outstanding tasks."*

Smartphones have become the main means of communication for individuals and this is especially true for the African continent. One of the reasons for this is the lack of infrastructure in Africa in terms of roads, telephone and fixed line internet connectivity. *"In South Africa and the rest of Africa the number of mobile internet users is growing and has the greater penetration rate compared to fixed land line internet connections"* (P10). *"These smartphones are driving informal markets allowing consumers to gain access to information via these devices to make purchases and transfer money via these devices. South African businesses are now able to make contact with clients in rural areas via mobile networks and sell their products and services to clients from these regions that the business would otherwise not have access to"*. P12 and P11 stated that the organization's focus must be to make information more accessible and easier to consume on mobile devices, such as smartphones.

P1 stated that the Client Relations division's requirement prior to starting the mobile program was to enable their mobile workforce by providing them with the tools that could increase their productivity, allow for process improvement and save on costs. They wanted to operate in a virtual hub that allowed them to plug in their devices and work when they needed to be in the office and where there was no need for permanent office space.

Subtheme 3 – Facilitating a digital environment

Organization X executives in board meetings are now able to electronically view large board documents that are on the agenda for the meetings. These documents are usually more than 500 pages each so not printing these documents assists in costs savings for paper and printing. P3 noted that mobile devices including smartphones, tablets, and laptops are making it easier for employees to collaborate on projects and other milestones. These devices facilitate electronic conversations using tools like SMS, email and WhatsApp.

P1 mentioned that the business she represented needed to enable their staff to operate in a mobile manner. This participant was an advocate of the CYOD model. This participant did not want their business information stored on their personal devices. P1 stated: *"I prefer one company sponsored mobile device for all business-related tasks and wanted a mobile device that could offer a fully integrated solution. This solution needs to allow for a paperless environment and the mobile device functions have to have the following functions: email, Microsoft Lync messenger, WhatsApp, voice calling, Bluetooth for when driving, ability to sign documents digitally, uploading files to backend systems."* The research noted the amount of BYOD users far outweighed CYOD users in the organization but the amount of corporately sponsored devices (CYOD) was steadily increasing as managers saw the benefits of having standardized fully integrated mobile devices.

A paperless environment was also important to the Client Relations division that P1 represented where documents could be signed on their mobile devices and stored digitally on protected storage. The mobile devices they required needed to include and allow the following functionality:

1. Tablet/hybrid devices that would allow the users to touch, type documents, digitally sign documents, make voice calls and have video conferencing functions. (These hybrid devices are a tablet with a keyboard that can be plugged into it so that the device operates as a full laptop.)
2. Access emails, SharePoint and backend systems from their tablet/hybrid devices.

The findings in this theme indicate that the benefits listed in the literature are also experienced by Organization X in terms of productivity and accessibility of information. The other benefit listed in literature is BYOD cost saving on hardware, but this benefit did not come through strongly in the findings from participants.

Theme 2 – Client Service and Experience

Management guru Peter Drucker stated that *"to satisfy the customer is the mission and purpose of every business"* (as cited in Kandampully, Zhang, & Jaakkola, 2017). Customer satisfaction is one of the core objectives of any business irrespective of the product or service being offered to the market. Sub-

themes include the improved client responses times by employees and design considerations for mobile client-facing systems.

Subtheme 1 – Faster response time to client queries

At the organization where the data was collected there was a strong emphasis on doing business that focuses on their clients. It's vital for the business to understand their needs and fulfil their requirements while providing an excellent service experience. Employees using mobile devices can respond to client's queries and other business units quickly. There is no longer a reason to not be connected to company systems while traveling or in-between meetings. Customer relations consultants can assist clients with their queries and changes to their portfolios while visiting clients at their premises.

P1 agrees with the statement above: *"Mobility has improved our communication as Client Service Representatives respond much faster to emails on their tablets in-between meeting and while waiting at Clients premises"*.

An important benefit of mobile devices is that it allows employees to respond to clients queries very quickly and efficiently. More than half the participant mentioned this as a benefit in their business divisions. Mobile devices are an essential working tool as much of the working day includes traveling to and meeting with clients.

P6 noted that he and his fellow advisors are greatly benefiting from BYOD devices by way of the financial application that was developed by the organization for them to do business remotely on their devices. *"These mobile devices allow us as financial advisors to communicate via email with their clients and also meet with clients at different locations of the clients' preference"*. The application they use allows them to complete analysis of the clients' financial needs to enable them to make better financial choices in terms of retirement plans, investment choices and other financial plans. P6 explained that forms can be filled in on the tablet devices and signed electronically for a better client experience. Capturing these forms electronically helped with improving processes and moves the organization closer to a paperless environment.

Subtheme 2 – Client-friendly IT systems and applications

P2 reported that in his area of responsibility IT systems that are client-facing are also being developed for mobile devices and lot of thought is being put into the design of this and how information will be displayed on these devices. *"Information about the company's products and services must be made available on mobile devices so that this information can be easily accessible to current and potential clients"* (P2).

Summarizing this theme, for businesses to engage with their clients effectively they need to ensure their business strategies include the appropriate business models, technology and processes (Hollingworth & Harvey-Price, 2013). Technology has empowered consumers with the ability to access information about products and services in a manner to suits their preference. While the main communication channels for consumers are company websites then email and social media pages have become a popular channel for communication between businesses and their customers (The Economist, 2013). The latest addition to these communication channels has been mobile applications. Organization X has business strategies to cater to their clients for all communication channels about their products and services. These include the traditional company websites, emails, television, print media but they also cater for the social media pages and mobile applications for clients available for download in all major application stores. The organization has already developed their systems so that information can be rendered in a user-friendly design for mobile devices making it easier for clients to interact with the information and systems. The findings show that BYOD allows the employees of Organization X to provide a higher level of customer service whether it be face-to-face or electronically.

THEME 3 – COMPETITIVE ADVANTAGE

In a cross-nation industry survey of 2000 IT users (including senior managers) regarding their attitudes towards BYOD, more than 80% of the IT managers thought that BYOD provided a competitive advantage for organizations that could manage the risks associated with BYOD over organizations that did not offer a BYOD program (Singh, 2012). The subthemes include the need for innovation due to competition and presenting a professional image.

Subtheme 1 – Competitor pressure

For the organization to stay ahead of the competition the employees need to find innovative ways of doing business. This way of thinking is encouraged throughout all levels of the organization. Allowing employees to use their own devices that they are more comfortable with encourages this innovative behavior. *"If the business can't adapt and stay abreast with mobility the business will not be able to remain competitive in the financial industry"* (P12).

P11 has noted that shops with no or little online facilities are closing fast because they are not catering to the mobile internet user market. *"It is also important to keep abreast of what your competitors are doing so if they are offering consumers mobile internet information platforms your business also needs to do the same and better to avoid losing potential clients"* (P11). P11 and P12 believe that mobility allows the organization to save on costs of doing business with remote clients and if your competitor is conducting business at a cheaper rate than your business then your business will lose out and eventually get cut out of the market that they are competing in.

In addition, the organization can use BYOD and its mobility program as an incentive to attract and recruit younger talented professionals to the business. These younger professionals have grown up with the latest technology and use these tools to find innovative ways of solving problems. Allowing existing employees to use the mobility program assists the company with retaining their talented individuals.

Subtheme 2 – Presenting a professional image

In the sales portion of the business mobile devices have been an invaluable tool. When the financial advisors, client service and other sales professionals visit clients and use their mobile devices it creates a professional image of themselves and the business (P1).

P2 mentioned a mobile application developed for intermediaries and financial advisors: *"We also have an app now that allows them to access information and assist clients face-to-face."*

"The organization aims to have the best products and services in the industry and having the latest technology including IT systems and mobile devices allows the business to stay ahead of the competition in the industry." … *"Professional image – When staff meets with clients having the appropriate technology creates a good impression of the organizations systems and their ability to administer their business. Having outdated technology when presenting to potential clients can have disastrous effects on their perception of the organization."* (P11).

Some participants who were in support of the CYOD model felt that it was important that their staff that was visiting clients was equipped with the right technology to service the client's needs. This meant having devices that had enough processing capability but also assisted with creating a professional image of the staff member and the business. P7 believed that professional image of his staff was important for sales of the business products and services. The mobile devices were typically used in presentations to prospective clients and when servicing existing clients. P1 had the same comments regarding professional image and has also seen that when using cutting edge technology, the devices was often a conversation starter which helped in building rapport with clients. Most of the participants agreed that it was vitally important to use mobile devices in their business to remain competitive in the industry. If the competition was using mobile devices and they were not the competition would have the edge and do better in the market. Four of the participants were already

thinking of new and innovative methods to take mobile devices and the mobile applications to the next level to provide even more benefit to the customers and internal employees.

Summarizing this theme, the findings indicate that BYOD and mobility in terms of accessing important information and the ability to make importance decisions based on the information provides a competitive advantage for the organization. The literature on BYOD's competitive advantage and the information extracted from the participants is aligned.

Theme 4 – Process Improvement

Investment in the organizations IT systems aids in process improvement, which leads to higher company performance (McAfee & Brynjolfsson, 2008). Research has also shown that users' performance expectancies have a positive influence on their intention to adopt BYOD (Weeger et al., 2016). This theme focuses solely on the factor of process improvement.

P2 stated that their division had the utility benefits in mind for their mobility program that included providing their financial advisors and brokers with online capability for the business quotations systems, front office processes and the ability for the sales person to fill in the forms and process it online with the customer. These individuals who deal with customers need all the tools available to be able to service the customer at the place that is most convenient for them. Future systems need to be built that allow the company to communicate their product and services with customers of all ages, across multiple platforms including mobile. After the organization has their mobile program in place that allows employees to use their mobile devices to connect to organizational resources, the program can be used to attract young talented individuals to join the business. Businesses needed to capitalize on the latest mobile technology in the market and use this technology to forward their business goals.

Clients can complete and sign documents electronically on these mobile devices, with the assistance of the client-facing staff. Mobile devices also allow for the business to go paperless as all documentation is stored electronically at the business premises instead of in large filing cabinets. Finding customer information in filing cabinets is time consuming and these files take up lots of storage space that is expensive. P15 stated that *"Productivity is improved because access to the information and processes are much faster using mobile technology and the application."* P11 and P12 explained that the organizations mobile application allowed the intermediary to fill out the forms with the client on the broker's mobile device without the need for papers. This made it easier for intermediaries to do business with Organization X.

In summary, the findings for this theme align with previous literature to show that BYOD does assist with business process improvements. The BYOD program, applications specifically designed for BYOD, and the online capabilities are improving processes in the business.

Theme 5 – BYOD Risks

Mobile devices have a higher risk to an organization compared to desktop computers that are permanently fixed and located on the organization premises and protected by the security firewalls and other security measures. Mobile devices are constantly moving with the owner of the device and the problem is it can be easily lost or stolen. As the technology that these devices are built with has improved over the years the size of these devices has become smaller also making them more prone to be misplaced (Calder, 2013). Subthemes include various types of risk as well as concerns about regulatory privacy compliance.

Subtheme 1 – Information security risk

Of the many risks associated with the mobile devices information security of the organizations was the most common risk stated by participants. Sensitive information can include client information and strategic business information, new product development not yet in the market and sensitive

internal communication. Corporate data stored on the device is also moving outside the perimeter of the organization and is difficult to control. P1 stated that one of the main functions that they use their mobile devices for is to respond to emails which contains sensitive personal information of their clients as well as other important internal communication that should only be viewed by certain individuals. If that information got into the wrong hands and was used maliciously it could be detrimental to the organization. This participant emphasized the role the organization had in protecting their clients' personal information and loss of this information could lead to serious legal implications for the organization. If the organization was exposed and valuable information was compromised, it would affect the organizations reputation which would lead to loss in revenue (P3).

One of the concerns for P2 was the uncertainty of where the information was after it was stored on the mobile devices and what copies existed elsewhere. With the current tools available it made it impossible to have an accurate view of this. This risk was also mentioned by the information security officer that noted the dangers of synchronizing data to mobile devices and other IT services. Available cloud services like Dropbox allows the possibility for staff to synchronize business data to the cloud without the knowledge of the organization. These cloud services have been known to be vulnerable to attack by cyber criminals.

Two of the participants believed that in South Africa mobile devices were mainly stolen for the monetary value of the device and not the information stored on the device. They did say it is was vitally important that the organization and individuals tasked with information security responsibilities protect sensitive data though, but data theft and data leaks was not accounting for mobile device theft. Most of these thefts were from break-ins to staff vehicles where mobile devices including laptops and tablets were being stored when the employees were away from the vehicles.

Subtheme 2 – Financial risk

Other financial risks related to mobility and BYOD are the IT systems that are being developed to cater for mobile use. These development costs of these systems are usually high. When developing applications that clients and internal staff can use there is always the chance that the mobile system including apps will not be as successful as it was originally projected and the number of users that continually use these systems are lower than expected.

Subtheme 3 – Insecure mobile device risk

As with risks for the organization the mobile user also runs the risk of losing their personal information stored on their mobile device. Organizational information that was stored on mobile devices can be backed up on storage at the organization's premises but if the mobile device is lost/stolen or corrupted then often the users' personal information is lost. P8 stated that research showed that mobile devices are more vulnerable than laptops as the smaller devices are often misplaced and lost. One of the reasons for this could be that tablets and smartphones cannot be locked to the desk like laptops can with cable locks. The loss of these devices is for the users' own account. The insurance costs for their devices and the costs for replacement are their responsibility. Mobile devices are also damaged more easily than its laptop counterparts (P9).

P8 noted that other risks facing mobile users are connecting to insecure wireless access points that provide wireless networking and internet access. Cyber criminals use these insecure networks to intercept unencrypted communications sent and received by the mobile user. P8 also pointed out that there has been an increase in malware that has been developed to exploit and infect mobile devices. The purpose of this malware is usually to steal sensitive login information that includes credit card and banking login details. According to P8 there has not been an increase in malicious software like viruses since launching the mobile program.

P1 felt that the risks for laptops and tablets/smartphones were similar as all these devices moved with the mobile user compared to the traditional desktop computer that stayed at the office. This

participant who was an advocate of the company sponsored mobile device believed the less mobile devices the user carried with them the better. So instead of having a laptop, a business tablet, personal tablet and smartphone they were transporting to and from the office combine the functionality of certain devices then this reduces the risk to the organization and the user. Their division was using corporate sponsored hybrid devices that had the functionality of a laptop and the versatility of a tablet and smartphone that was also partially covered by the business. That enabled employees to only carry two devices compared to four.

Subtheme 4 – Regulatory privacy compliance

Most of the participants were concerned about how difficult it was to manage data on mobile devices and how this would affect compliance to the Protection of Personal Information Act (POPIA) (Government of South Africa, 2013). POPIA promotes the protection of personal information and guides how this information is processed was signed into law and once the commencement date is set companies will have one year to comply or face hefty financial penalties. It will force companies to report on lost data including customer records so having data stored on mobile devices will make it difficult to comply with this legislation (P3).

P4 stated that more focus should be placed on where sensitive data is stored to understand the risk exposure from a reputational risk point of view. This will enable the organization to be better prepared to protect sensitive data and ensure compliance to POPIA.

In summarizing this theme, BYOD risks included loss or misuse of sensitive information, financial risks, technical risks (like malware and insecure Wi-Fi), as well as privacy concerns. As found in the literature review, the number one concern for organizations using BYOD is information security (Calder, 2013). This was also the main concern for participants. In addition, the issue of regulatory privacy compliance also presented an environmental concern for BYOD innovation (Baker, 2012).

Theme 6 – Management of BYOD

Mansfield-Devine (2012) highlighted the importance of an information security policy and this should also cover the rules for safe BYOD usage. The policy should strike the right balance of security while also not being too restrictive to prevent the users from working. Organization X follows several best practices to manage its mobility risks. Subthemes include a range of security-related factors, e.g., policies, information security training and awareness, end-user behavior, as well as technical security considerations.

Subtheme 1 – Policies

When questioned about the management of BYOD risks most of the participants felt that to protect the organization's information and especially on mobile devices a combination of internal and external security controls was required. Using one type of security control alone was not adequate in protecting the organizations information assets. Nearly all the participants from the information technology side quoted policies as their first method of controlling mobile risks.

The organization had recently rolled out their digital behavior policy where a major component of this policy was dedicated to mobile device security. This policy and other information security policies in the organization prescribed the rules and regulations that all users of the organization network infrastructure and IT systems had to adhere to. This policy also advised users on how to use their devices, IT systems and the internet safely to minimize their chances of being exploited or having corporate information exploited by cybercriminals. All users from all the business units in the organization had to sign off on this policy. Prior to the signoff of the digital behavior policy all users were required to read regular email communication regarding this as well as complete a compulsory online training session that quizzed the users on their understanding of the policy. Another method to entice users to understand this policy was the creation of a series of animated videos covering various

information security topics. At the end of the videos staff was asked a few simple questions and if they answered correctly they could enter a competition where they stood a chance of winning prices that included tablet and smartphone devices.

Subtheme 2 – Information security training and awareness

P3 of one of the companies within organization stated that when new employees start their employment at the organization they are required to attend a compulsory information security training session. At different intervals throughout the year workshops are held to educate and familiarize the staff with important current information security topics. When there are new security protocols and practices or changes to existing one the organization runs internal advertising campaigns to raise awareness and understanding. The IT Security team also developed an internet website dedicated to information security practices that assisted people to use the internet in a safe and responsible manner (P4).

Subtheme 3 – Passwords

Only users that have received departmental management approval can use their mobile devices to access the organizations mobile network and internet connection. There is a monthly charge against the business department for this mobile connectivity. P10 said that when connecting to this mobility program users are forced to use a password on their devices with a minimum of four characters. Other employees not using this mobility program are also encouraged to do so for their own protection. To access services like email and IT systems the mobile user is required to use their network credentials. This network credentials need to be configured on the mobile devices of the user and updated by them each time their password changes on the network.

Subtheme 4 – Mobile device management

Many of the participants in this study were involved in the requirement analysis, evaluation of mobile device management (MDM) products on the market and were involved in the decision to purchase the MDM systems that the organization currently uses. P3, P8, and P4 emphasized the importance of the MDM solution that allows the organization to administer mobile devices including smartphones and tablets. Some of the functions that were mentioned by participants included containerization where corporate data including emails and corporate applications and data were stored in a separate encrypted container on the users' mobile device. The other important feature is remote wiping capability that cleans all corporate information and personal data on mobile devices. If a mobile device is lost or stolen the affected staff member needs to report this to their IT department immediately so that the information stored on it can be remotely wiped before sensitive data is leaked.

In BYOD literature MDM is listed as one of the best practices for BYOD management (Rouse, 2014; Mathias, 2015). This technology is implemented at Organization X as stated by the participants above, but this security technology is expensive.

Subtheme 5 – Secured communications

Encryption technologies are used for communication between the mobile device and the organization's network. This is accomplished via virtual private networking that allows all communication to be secured through the communication tunnel. All new laptops issued in the organization have built-in encryption which helps if the device gets into the wrong hands then the information can't be accessed (P4).

Subtheme 6 – Support challenges for mobility

P3 noted that with the addition of mobile devices in the organization the requests for support have increased. The IT Helpdesk team prepared for the additional influx of requests for assistance by add-

ing additional staff members. The team dealing with these requests needed specific mobile experience and additional training to support the needs of the organization's mobile workforce.

Subtheme 7 – Complexity and compatibility

The mobile devices used by the users come in different brands and types making complexity a big issue for the organization. Not all the software developed in house is compatible for all the types of devices. The P2 stated that it is very difficult to accommodate all the technology of the mobile devices within the business. For example, when certain web applications are developed they do so for certain browsers and mobile operating systems. He also mentioned that a lot of complexity issues arise when going from one version of the software to the next.

Subtheme 8 – Security controls on mobile devices

The IT team responsible for the security controls set these controls to provide an adequate level of security for the users and the business without being too restrictive. All the IT participants agreed that if the security controls were too restrictive the employees would either not use the mobile services or try and find ways around the security, so they needed to find the right balance.

When the user starts using the company's mobile program they are forced to use a four-digit pin. Most of the organization's users don't have any issues with this and other security controls. They understand that it is necessary to have this protection. There were a few participants that paid for their own mobile devices (BYOD) that felt entering the four-digit pin each time they wanted to use their device was restrictive. For example, when they needed to make a call quickly they needed to enter this pin code first (P1 and P11).

After the digital behavior policy that included mobile device usage was issued by the business there were several users and business divisions that refused to sign the policy. Some of the reasons for this included disagreeing with some of the security controls and not understanding these controls. Some users were concerned that the IT team could see their personal information on their devices. After communicating to these users that the technology did not allow the IT team to see the user's personal information the user's signed the digital behavior policy. Users that refused to sign and agree to the terms of the policy and mobile program simply would not be authorized to use the mobility program.

In summarizing this theme, the organization's best practices for BYOD management include policy creation and enforcement, information security training and awareness, and MDM which includes remote wipe facilities. It also advocates that password protection of devices should be compulsory.

CONCEPTUAL FRAMEWORK FOR BYOD ADOPTION

In this study we examined the business priorities driving the adoption of BYOD in a large South African financial services organization. To summarize the results of the thematic analysis this section analyzes the data in terms of the three contexts of the TOE framework. It discusses how each of the three contexts affect the adoption and implementation of BYOD in our case study, Organization X.

The conceptual framework in Figure 3 represents a summary of the themes and links found in this study. It illustrates the factors which have a positive effect (+) on the BYOD adoption decision, as well as the factors which are negative influencers (-). It should be noted that some factors could have both a positive as well as negative impact. The concept of BYOD started when consumerization of IT began. Employees started bringing their own devices into the workplace and wanted to use their devices for work purposes. Rather than resist the trend Organization X decided to develop strategies that would allow the organization to benefit from this.

Within the technological context the most significant positive factors include increased employee productivity, the transition to a digital (paperless) environment, faster client response time, more cli-

ent-friendly IT systems, and process improvements. For the organization's mobile workforce to be productive while they were seeing clients or traveling the organization needed to create systems and strategies to allow these users to connect to the corporate systems securely. The Organization X has seen significant increase in mobile workers productivity. A surprise finding was the amount of after-hours work that mobile users were completing. BYOD enabled the mobile workers to provide better service to their clients because they were able to respond to queries much faster.

The organization was able to use the digital capabilities of BYOD to improve certain processes which included allowing clients to fill in digital forms for faster processing and storage. Finding customer information was found to be much easier in the paperless environment compared to the old filing cabinets used in the past. When the clients have decided on a product or service they are able to digitally sign documents and/or contracts, and this is then processed in the organizations back office. The financial advisors are also able to track the clients request on the workflow systems via their mobile devices. Less printed paper copies aid in the organization's overall green strategy to limit its carbon footprint.

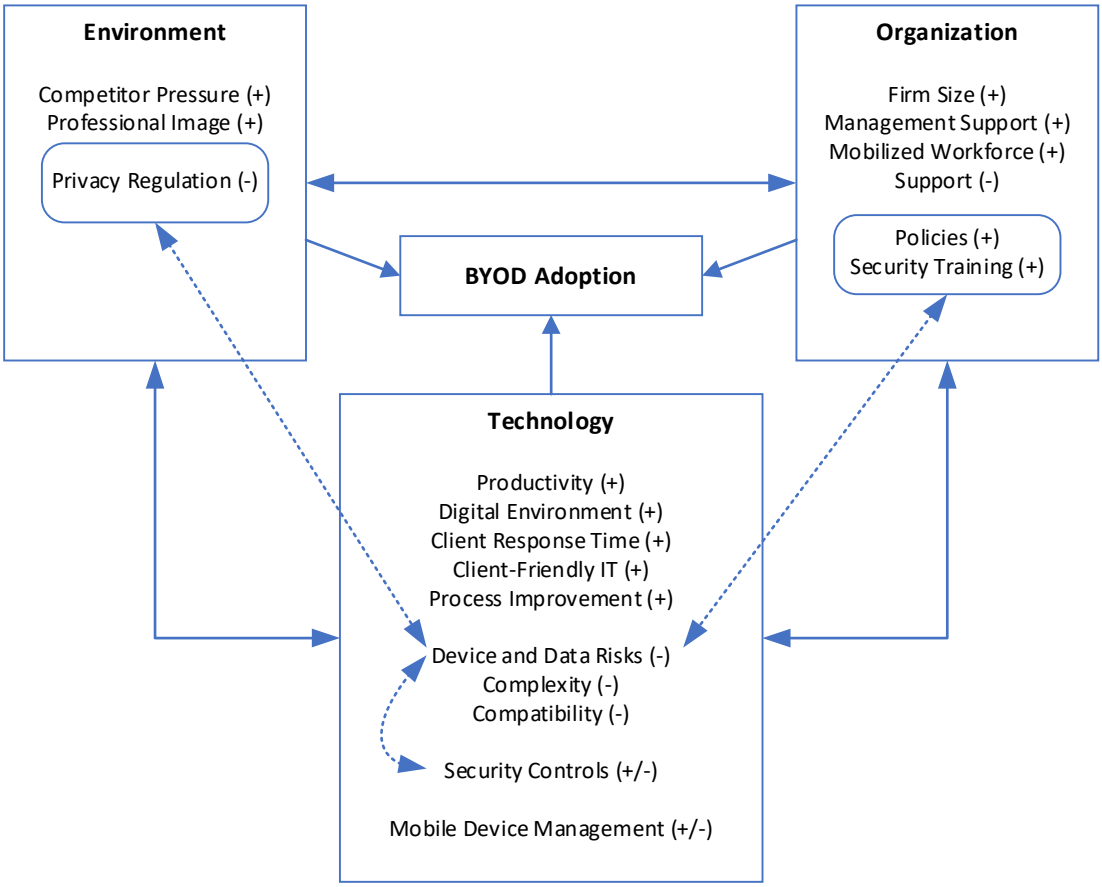

Figure 3. Conceptual framework for BYOD adoption

On the other hand, BYOD has introduced device and data risks for the organization. There is also increased IT complexity and issues with compatibility. The risks can be addressed with security controls (e.g., passwords, encryption, etc.), but if controls are too restrictive employees would either not use the mobile services or try and find ways around the security. Thus, achieving a balance within the context of the organization is of importance. Finally, MDM was a key part of the organization's BYOD strategy but is costly. Findings in the literature and in the empirical research suggest organizations incorporate enterprise mobility management solutions that include MDM (Ghosh et al., 2013;

Pinchot & Paullet, 2015). Here functions like remote wipe of the information stored on lost devices are some of the important functions.

In terms of the environmental context the organization adopted BYOD to create a competitive advantage over other companies in the market. This was driven by competitor pressure and the desire to present a professional image. However, a big concern was regulatory privacy compliance – having data stored on mobile devices will make it difficult to comply with legislation. Appropriate security controls would need to be implemented to comply with legislation.

Finally, within the organizational context it could be seen that the size of the organization – and resulting improvements affecting many employees – played a positive role in BYOD adoption. There was also suitable management support and the desire to create a mobilized workforce. It was seen that policies (mainly security-related) and information security training were an important part of the organization's BYOD strategy and helped to address the device and data risks.

A major concern that organizations have with BYOD is the possible loss of sensitive information located on the mobile devices (Calder, 2013) and protecting their information assets is a high priority. To ensure that these information assets are protected a combination of technical and human controls are a necessity. Firstly, the organization needs to create appropriate information security and BYOD policies that govern the use of mobile devices and the organizations IT systems and the appropriate use and processing of sensitive organizational data. It is important that the staff understand these policies, accept consequences of being in contravention of the policy and sign off that they agree with the terms. The organization needs to establish which security systems will be appropriate for the organization's needs.

On the other hand, technical support for BYOD proved challenging as a high number of requests needed to be serviced and support staff needed training in this area. As reported by the participants, setting up the IT infrastructure for BYOD can be costly for the organization. These costs, which are not often mentioned in literature, include the connectivity, security, IT support and development costs for mobile platforms. Having IT professionals with the right amount of skill and experience is key to a successful BYOD program.

In summary, we see the adoption of BYOD in Organization X as having produced discontinuous change, presenting a significant departure from current technologies and processes. At this point it cannot be determined with absolute certainty whether BYOD was purely competence-enhancing, but evidence of the firm building on this new expertise was encouraging.

CONCLUSION

The aim of this study was to provide insight into the business priorities that drive BYOD adoption and to investigate the how the case organization dealt with the challenges associated with BYOD. A conceptual framework (based on the TOE framework) contextualized the findings from the case study, highlighting the issues in each of the three TOE contexts. The findings show that organizations can use BYOD to improve client service, gain competitive advantage, and improve their processes using their digital devices and backend systems. Recommendations on how organizations could implement and manage their BYOD program was also suggested.

A practical contribution of this research is to show organizations considering adopting a BYOD program the benefits achieved by the case organization and how the risks are managed. Organizations need to clearly understand the reasons they want to introduce BYOD in their organizations. This information can be used to build a business case for the new BYOD program, gain top management support for the program and to receive buy in from the relevant stakeholders. The conceptual framework can be applied by practitioners in their organizations to achieve these business objectives.

In South Africa there has been a high mobile penetration rate and broadband usage has overtaken fixed line internet usage. The factors that affect BYOD usage in South African differ from the more developed North American and European countries. Barriers that affect Internet usage in Africa and specifically South Africa include poor fixed line infrastructure and high telecommunications fees. BYOD can be used by organizations to access clients living in rural parts of the country and the African continent. A caveat of the study is that it focused on a single case study, conducted within a large South African financial services organization, and the empirical data is from this organization's perspective. Research from other organizations in a different industry may yield different results. In addition, small to medium organizations might have different criteria for choosing BYOD leading to different findings.

Future research should be conducted across multiple case sites to determine if new factors can be identified and to highlight differences between sites. This research was conducted in a financial services organization, but other industries should also be observed to determine if this introduces contextual factors that did not emerge in this study. Future research can also examine in more depth how BYOD risk assessments are completed. Completing the risk assessment will enable the organization to identify possible risks, who or what might be affected, what level of risk will be acceptable, appropriate actions to limit the risks and who is responsible to carry out actions. This research could be extended to explore how to effectively manage the risks that were identified. Finally, an exploration of possible links between BYOD and the culture shift to smartphone use in the private sector presents another potential study.

ACKNOWLEDGEMENTS

This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

REFERENCES

Abrahams, O., Ophoff, J., & Mwalemba, G. (2015). Cloud computing adoption for business development: A TOE perspective. In J. Steyn, & J. P. Van Belle (Eds.), *Beyond development. Time for a new ICT4D paradigm? Proceedings of the 9th IDIA conference* (pp. 463–476). Nungwi, Zanzibar. Retrieved from http://www.developmentinformatics.org/conferences/2015/papers/33-abrahams-ophoff-mwalemba.pdf

Albrechtsen, E. (2007). A qualitative study of users' view of information security, *Computers & Security, 26*(4), 276-289. https://doi.org/10.1016/j.cose.2006.11.004

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445. https://doi.org/10.1016/j.cose.2009.12.005

Anderson, N. (2014). *Cisco bring your own device.* CISCO Systems, Inc. Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: The identification of a twofold security paradox. *Journal of Organizational Change Management, 31*(4), 839–851. https://doi.org/10.1108/JOCM-03-2017-0044

Baker, J. (2012). The technology–organization–environment framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information systems theory. Integrated Series in Information Systems, Vol 28* (pp. 231–245). New York, NY: Springer. https://doi.org/10.1007/978-1-4419-6108-2_12

Baskerville, R. (2011). Individual information systems as a research arena. *European Journal of Information Systems, 20*(3), 251-254. https://doi.org/10.1057/ejis.2011.8

Basole, R. C. (2007). The emergence of the mobile enterprise: A value-driven perspective. In *Proceedings of the International Conference on the Management of Mobile Business (ICMB 2007)* (pp. 41-48). IEEE. https://doi.org/10.1109/ICMB.2007.63

Bauer, R. A. (1967). *Consumer behaviour as risk taking*. In D. F. Cox (Ed.), *Risk taking and information handling in consumer behaviour* (pp. 23-33). Graduate School of Business Administration. Cambridge, USA: Harvard University Press.

Beach, L. R. (1993). *Making the right decision. Organizational culture, vision and planning*. Eaglewood Cliffs, New Jersey: Prentice Hall.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130–137. https://doi.org/10.1016/j.cose.2008.11.001

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brodin, M., Rose, J., & Ahlfeldt, R. M. (2015). Management issues for bring your own device. In *Proceedings of the 12th European, Mediterranean & Middle Eastern Conference on Information Systems 2015 (EMCIS 2015)*. Retrieved July 17, 2015, from http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-11004

Calder, A. (2013). Is the BYOD Movement Worth the Risks? *Credit Control Journal, 34*(3), 65-70. Retrieved from http://connection.ebscohost.com/c/articles/87627145/byod-movement-worth-risks

Cavana, R., Delahaye, B. L., & Sekaran, U. (2001). *Applied business research: Qualitative and quantitative methods*. Australia: John Wiley & Sons Inc.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2009). *Information security control resources in organizations: A multidimensional view and their key drivers*. Working paper. Sauder School of Business, University of British Columbia.

Chen, L., & Nath, R. (2011). Impediments to mobile work: An empirical study. *International Journal of Mobile Communications, 9*(5), 522-540. https://doi.org/10.1504/IJMC.2011.042457

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

Cisco. (2013). *Cisco connected world – International mobile security: Survey research highlights and considerations for enterprise IT*. White Paper. CISCO Systems, Inc. Retrieved from http://www.webtorials.com/main/resource/papers/cisco/paper240/International_Mobile_Security.pdf

Citrix (2011). *IT organizations embrace bring-your-own-devices: Global BYO index*. Fort Lauderdale: Citrix. Retrieved June 30, 2014, from http://s3.amazonaws.com/legacy.icmp/additional/citrix_byo_index_report.pdf

Collins, P. D., Hage, J., & Hull, F. M. (1988). Organizational and technological predictors of change in automaticity. *Academy of Management Journal, 31*(3), 512–543. https://doi.org/10.5465/256458

Couture, E. (2010). Mobile security: Current threats and emerging protective measures. *SANS Institute Information Security Reading Room*. Retrieved August 18, 2014, from http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548

Cunningham, S.M. (1967). The major dimensions of perceived risk. In D. F. Cox (Ed.), *Risk taking and information handling in consumer behavior* (pp. 82-108). Boston, MA: Graduate School of Business Administration, Harvard University Press.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigor, relevance and pragmatism. *Information Systems Journal, 8*(4), 273 – 289. https://doi.org/10.1046/j.1365-2575.1998.00040.x

DePietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. In L. Tornatsky, & M. Fleischer (Eds.) *The processes of technological innovation* (pp. 151–175).

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

Disabato, M. (2016, January 06). Solution path: How to create a mobile strategy. *Gartner Catalyst Conference*. San Diego. Retrieved from https://www.gartner.com/doc/3183319/solution-path-create-mobile-strategy

Drew, J. (2012). Managing cybersecurity risks. *Journal of Accountancy, 214*(2), 44-48. Retrieved from https://www.journalofaccountancy.com/issues/2012/aug/20125900.html

Ernst & Young (2008). *Moving beyond compliance: Ernst & Young's 2008 global information security survey*. Retrieved August 19, 2014 from http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/2008_E&YWhitePaper_GlobalInfoSecuritySurvey.pdf

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474. https://doi.org/10.1016/S1071-5819(03)00111-3

Galbraith, J. R. (1973). *Designing complex organizations (1st edition)*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Gartner. (2012). Gartner says bring your own device programs herald the most radical shift in enterprise client computing since the introduction of the PC. *Gartner Newsroom*. Retrieved January 24, 2019, from https://www.gartner.com/newsroom/id/2136615

Ghoda, A. (2009). *Pro Silverlight for the enterprise*. New York: Apress. https://doi.org/10.1007/978-1-4302-1868-5

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4*(4), 62-70. Retrieved from http://jgrcs.info/index.php/jgrcs/article/view/654

Government of South Africa (2013). *Protection of Personal Information Act, No.4 of 2013*. South African Government. Retrieved from https://www.gov.za/documents/protection-personal-information-act

Hagen, J., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*(3), 140-154. https://doi.org/10.1108/09685221111153537

Hollingworth, L., & Harvey-Price, A. (2013). *Technology and skills in the digital industries. Evidence Report 73*. UK Commission for Employment and Skills. Retrieved November 5, 2015, from www.gov.uk/government/uploads/system/uploads/attachment_data/file/305376/evidence-report-73-technology-skills-digital-industries.pdf

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

IBM, (2011). *The new workplace: Supporting "bring your own"*. White Paper. IBM.

IBM, (2012). *Securing end-user mobile devices in the enterprise*. White Paper. IBM.

ISACA. (2008). *Glossary of terms, 2008*. Retrieved 02 July 2014 from http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. In: M. Venkatesan (Ed.), In *Proceedings of the Third Annual Conference of the Association for Consumer Research: Advances in consumer research* (pp. 382-393). Chicago, IL: Association for Consumer Research. Retrieved from http://www.acrwebsite.org/search/view-conference-proceedings.aspx?Id=12016

Kandampully, J., Zhang, T., & Jaakkola, E. (2017). Customer experience management in hospitality: A literature synthesis, new understanding and research agenda. *International Journal of Contemporary Hospitality Management, 30*(1), 21–56. https://doi.org/10.1108/IJCHM-10-2015-0549

Kaneshige, T. (2012, April 07). *ComputerWorld UK BYOD - Five hidden costs to a bring-your-own-device program*. Retrieved January 26, 2019, from https://www.computerworlduk.com/it-vendors/byod-five-hidden-costs-bring-your-own-device-progamme-3349518/

Kaplan, L. B., Szybillo, G. J., & Jacoby, J. (1974). Components of perceived risk in product purchase: a cross validation. *Journal of Applied Psychology, 59*(3), 278–291. https://doi.org/10.1037/h0036657

Kaspersky, (2012). *Security technologies for mobile and BYOD*. White Paper. Retrieved from https://media.kaspersky.com/en/business-security/Kaspersky-Security-Technologies-Mobile-BYOD.pdf

Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: A comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems, 13*(1), 215-224.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67–94. https://doi.org/10.2307/249410

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*, 3-11. https://doi.org/10.1016/j.cose.2012.07.001

Kornak, A., Teutloff, J., & Welin-Berger, M. (2004). *Enterprise guide to gaining business value from mobile technologies*. New York: John Wiley & Sons.

Landman, M. (2010). Managing smartphones security risks. In *Proceedings of the 2010 Information Security Curriculum Development Conference, InfoSecCD '10* (pp. 145-155). New York, NY: ACM. https://doi.org/10.1145/1940941.1940971

Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School Psychology Quarterly, 26*(1), 70-84. https://doi.org/10.1037/a0022711

Levin, S., Levin, S. L., & Meisel, J. B. (1987). A dynamic analysis of the adoption of a new technology: The case of optical scanners. *The Review of Economics and Statistics, 69*(1), 12–17. https://doi.org/10.2307/1937895

Lewins, A., & Silver, C. (2009). Choosing a CAQDAS package. *CAQDAS Networking Project and Qualitative Innovations in CAQDAS Project. (QUIC)*. Retrieved November 03, 2015 from http://eprints.ncrm.ac.uk/791/1/2009ChoosingaCAQDASPackage.pdf

Liljander, V., & Strandvik, T. (1992). Estimating zones of tolerance in perceived service quality and perceived service value. *International Journal of Service Industry Management, 4*(2), 6-28. https://doi.org/10.1108/09564239310037909

Liu, Y., Yang, Y., & Li, H. (2012). A unified risk-benefit analysis framework for investigating mobile payment adoption. In *2012 International Conference on Mobile Business (ICMB)* (paper 20). Retrieved from http://aisel.aisnet.org/icmb2012/20

Mansfield, E. (1977). *The production and application of new industrial technology (1st edition)*. New York: W. W. Norton & Co Inc.

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security, 2012*(4), 14-17. https://doi.org/10.1016/S1361-3723(12)70031-3

Mathias, C. (2015). Enterprise mobility management options: MDM, MAM and MIM. *TechTarget*. Retrieved January 25, 2015 from http://searchmobilecomputing.techtarget.com/tip/Enterprise-mobility-management-options-MDM-MAM-and-MIM

McAfee, A., & Brynjolfsson, E. (2008). Investing in the IT that makes a competitive difference. *Harvard Business Review*, (July–August). Retrieved from https://hbr.org/2008/07/investing-in-the-it-that-makes-a-competitive-difference

Moir, R. (2009). Defining malware: FAQ. *Microsoft TechNet*. Retrieved July 5, 2014, from http://technet.microsoft.com/en-us/library/dd632948.aspx

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *12*, 5-8. https://doi.org/10.1016/s1353-4858(12)70111-3

Myers, M. D. (2013). *Qualitative Research in Business and Management* (2nd ed.). London: SAGE Publications Ltd.

Percy, S. (2018). The top three business priorities for leaders over the next three years. *Forbes*. Retrieved January 26, 2019, from https://www.forbes.com/sites/sallypercy/2018/11/27/the-top-three-business-priorities-for-leaders-over-the-next-three-years/

Pinchot, J., & Paullet, K. (2015). Bring your own device to work: Benefits, security risks and governance issues. *Issues in Information Systems, 16*(3), 238-244. Retrieved from http://www.iacis.org/iis/2015/3_iis_2015_238-244.pdf

The Ponemon Institute LLC. (2012). *Global Study on Mobility Risks Survey Results for: United States*. Research Report. Retrieved from https://www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229–237. https://doi.org/10.1016/j.cose.2006.10.004

Purser, S. (2002). Why access control is difficult. *Computers & Security, 21*(4), 303-309. https://doi.org/10.1016/S0167-4048(02)00403-0

Rose, C. (2013). BYOD: An examination of bring your own device in business. *Review of Business Information Systems, 17*(2), 65-70. https://doi.org/10.19030/rbis.v17i2.7846

Roselius T. (1971). Consumer rankings of risk reduction methods. *Journal of Marketing, 35*(1), 56–61. https://doi.org/10.1177/002224297103500110

Rouse, M. (2014). Mobile application management. *TechTarget*. Retrieved March 15, 2015, from http://searchmobilecomputing.techtarget.com/definition/mobile-application-management-MAM

Schein, E. H. (1999). *The corporate culture survival guide*. San Francisco, CA, USA: Jossey-Bass Inc.

Schlienger, T., & Teufel, S. (2003). Information security culture – from analysis to change. *South African Computer Journal, 2003*(31), 46-52. Retrieved from https://pdfs.semanticscholar.org/0ae6/a37940971c1dd0b9e462ea0598aebc087cbb.pdf

Singh, N. (2012). B.Y.O.D. Genie is out of the bottle – "Devil or angel." *Journal of Business Management & Social Sciences Research, 1*(3), 1–12.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness, *Information Management & Computer Security, 8*(1), 31-41. https://doi.org/10.1108/09685220010371394

Smit, P. J., & Cronje, G. J. (1992). *Management principles: A contemporary South African edition*. Claremont, Cape Town: Juta Publishers.

Statista. (2019). *Number of apps available in leading app stores as of 3rd quarter 2018*. Retrieved January 26, 2019, from https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Stone R. N., & Gronhaug K. (1993). Perceived risk: Further consideration for the marketing discipline. *European Journal of Marketing, 27*(3), 39- 50. https://doi.org/10.1108/03090569310026637

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11. https://doi.org/10.1016/S1361-3723(06)70430-4

Tushman, M. L., & Anderson, P. (1986). Technological discontinuities and organizational environments. *Administrative Science Quarterly, 31*(3), 439–465. https://doi.org/10.2307/2392832

Tushman, M., & Nadler, D. (1986). Organizing for innovation. *California Management Review, 28*(3), 74–92. https://doi.org/10.2307/41165203

Twentyman, J. (2012). "BYOD: OMG! Or A-OK?" *SC Magazine: For IT Security Professionals (UK Edition),* 18-23. London, UK: Haymarket Business Publications. Retrieved from http://connection.ebscohost.com/c/articles/80215216/byod-omg-a-ok

Tzoumas, C. (2013, June 04). The effect of 'bring your own device' on today's businesses. *BusinessWest: The BYOD world*. Retrieved from https://businesswest.com/blog/the-byod-world/

Unhelkar, B., & Murugesan, S. (2010). The enterprise mobile applications development framework, *IT Professional, 12*(3), 33-39. IEEE. https://doi.org/10.1109/MITP.2010.45

Weiß, F., & Leimeister, J. (2012). Consumerization - IT innovations from the consumer market as a challenge for corporate IT. *Business & Information Systems Engineering, 54*(6), 363-366. https://doi.org/10.1007/s12599-012-0234-4

Weeger, A., Wang, X., & Gewald, H. (2016). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems, 56*(1), 1–10. https://doi.org/10.1080/08874417.2015.11645795

Whitman, M. E., & Mattord, H. J. (2013). *Management of information security (4th edition)*. Boston, Massachusetts, USA: Cengage Learning.

Wood, A. (2012). 'BYOD: The pros and cons for end users and the business', *Credit Control, 33*(7/8), 68-70. Retrieved from http://connection.ebscohost.com/c/articles/87627331/byod-pros-cons-end-users-business

Yin, R. K. (2013). *Case study research: Design and methods (5th edition)*. Thousand Oaks, California: Sage Publications.

Zielinski, D. (2012). Bring your own device: More employers are allowing employees to use their own technology in the workplace. *Society for Human Resource Management (SHRM)*. Retrieved from https://www.shrm.org/hr-today/news/hr-magazine/pages/0212tech.aspx

APPENDIX

The following interview guide was used for data collection. The questions were designed to explore issues around the research questions, developed from existing literature on success and challenges of BYOD. Organizational documents that included policy documents were also collected and analyzed to supplement interview data.

Management

1. Before launching the BYOD program what utility benefits did the organization envision?
2. Now that the BYOD program is operational have these utility benefits been realized? If not, why?
3. What risks (costs) has the organization experienced since using the BYOD program?
4. How has the organization dealt with these risks?
5. What best practices for managing BYOD have emerged?

General Use/Utility benefits – Users

6. What were your reasons for wanting to participate in the BYOD program?
7. Which work aspects does BYOD assist with most?
8. Which other positive aspects has your participation in BYOD led to?

Risks and other challenges – Users

9. What are the risks that you experience with BYOD e.g., Financial, performance, reputational damage, security, privacy?
10. As a BYOD user how do you feel about your device being monitored in terms of the personal information that is stored on it?
11. How restrictive are the security controls set to your device by the organization, towards personal tasks that you use your device for?

Concluding questions for organization and users.

12. What factors beyond utility and risk affected the BYOD decision?
13. Can you make any recommendations on how to increase the utility while minimizing the risks of BYOD to the user and organization?
14. How important is BYOD within the modern organization?
15. What role does BYOD have in the South African economic environment?

BIOGRAPHIES

Jacques Ophoff is a Senior Lecturer in the Department of Information Systems at the University of Cape Town (UCT), South Africa. He obtained his doctorate in Information Technology from the Nelson Mandela Metropolitan University, South Africa. His research interests include behavioral information security, privacy, digital forensics, mobile technologies, and education. He is a regular reviewer for international journals and conferences. He is an active member of the Association of Information Systems and the IFIP WG8.11/WG11.13 Information Systems Security Research group.

Steve Miller is a Senior Information Security Analyst currently working for a leading South African retail organization and he previously worked for a large financial services provider. He obtained his BCom Honors Degree in Information Systems from the University of the Western Cape then he went on to complete his MCom (Masters) degree in Information Systems at the University of Cape Town. His research interests include information security, risk management and mobile technology.