2014

Supporting and Securing Personal Mobile Devices Within an Existing Information Technology Environment

George Allen Patton
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

George Patton

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. David Gould, Committee Chairperson, Management Faculty
Dr. Mohammad Sharifzadeh, Committee Member, Management Faculty
Dr. Jeffrey Prinster, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2014

Abstract

Supporting and Securing Personal Mobile Devices Within

an Existing Information Technology Environment

by

George Allen Patton

MBA, Strayer University, 2006

BS, California Coast University, 1989

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

September 2014

Abstract

Personal mobile devices are becoming integrated into the daily operations of business. Managers are realizing that employees who are allowed to use personal mobile devices to access corporate information systems may reduce costs as users buy their own devices. The problem was that managers have a limited understanding of the need to secure or support personal mobile devices. The purpose of this survey study was to examine the relationship between employees' desire to use personal mobile devices and corporation needs for security and support. Hypotheses were tested by examining the relationships between the requirement to support and secure personal mobile devices as the independent variables and the desire to use personal mobile devices as the dependent variable. The theoretical framework for the study included the IT product life-cycle management theory, IT security-management theory, and IT strategic-management theory. Survey data were collected from a convenience sample of 108 employees at the study-site organization from an estimated population of 170. Basic linear regression analyses performed found a correlation coefficient of 0.905 indicating the variables are highly correlated. This finding indicates that if personal mobile devices are given access to corporate information systems, then support and security will be necessary for successful operations. If the relationship between internal factors and operational success is clearly documented, organizations may be able to use the data to justify incorporating personal mobile devices within their own corporate information system to reduce costs, improve productivity, and increase employee satisfaction thereby making a positive contribution to society.

Supporting and Securing Personal Mobile Devices Within an Existing Information Technology Environment

by

George Allen Patton

MBA, Strayer University, 2006

BS, California Coast University, 1989

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

September 2014

Dedication

This work is dedicated to my wife, son and daughter; their faith in me has given me the determination to succeed at everything in life.

Acknowledgments

Colin Powell wrote “There are no secrets to success. It is the result of preparation, hard work, and learning from failure.” However, if I may be so bold I would add to this statement that people help to achieve success. Therefore, I would like to acknowledge the chairman of my committee, Dr. David Gould, who took countless hours in reviewing my work and demanding a high level of expectations. Dr. Mohammad Sharifzadeh, his knowledge of research methods and statistical analysis was superb. Dr. Jeffrey Prinster, who’s help with the review and approval process for the URR was splendid. There are so many others that have given their time and efforts to help me achieve my goals and I do thank everyone for their support.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

As mobile devices become more sophisticated, demands for this technology in business environments are rapidly increasing. Employees are no longer dependent on desktop computers and can now perform business transactions practically anywhere at any time (Brans, 2003). However, several business decisions related to security, support, stability, and cost must be considered before allowing personal devices access to corporate information systems. The study used two strategies—the security and support of personal mobile devices.

This chapter covers the following: background on the influx of personal mobile devices being allowed access to the corporate information systems and the problems that may result, the problem statement, purpose of the study, research questions and hypotheses theoretical framework, nature of the study, significance, definition of terms, assumptions, limitations, and scope and delimitations.

Background

There are several motives surrounding the influx of personal mobile devices within business organizations. These include delivering access to applications and data in real-time or as close to real-time as possible. By supplying real-time access, employers and employees benefit by efficiently achieving their goals to swiftly respond to market opportunities that could otherwise result in business loss or reduce a competitive edge (James, 2011). Companies are much more likely to achieve competitive advantage and earn above-average profits if managers are able to find unique ways of delivering superior value to customers (Ziolkowski, 2011). Electronic mobility is emerging as a

potentially strategic benefit to establishing such advantage. Mobility can boost worker productivity with its added flexibility and efficiency (Sanni, Hashim, Anwar, Naji, & Ahmed, 2011). However, complications are introduced for technology teams as they work to manage the infrastructure while maintaining support and security (Gray, 2009). Consequently, managers of information technology (IT) departments are cautious about opening networks to mobile device users and allowing full access unless the devices are owned and controlled by the organization.

Redefining the Work Environment

To increased productivity and rapidly resolve problems regardless of location, requires instant access to data on an ongoing basis. Therefore, the need for wireless technology and mobile-enabled application strategies are concurrently increasing. Mobilization holds potential for enhanced performance metrics with the access to information anywhere and anytime; however, the challenges are immensely complex and require significant knowledge of the network infrastructure as well as the mobile devices (Brans, 2003). This process, if performed correctly, can assist management in the design of a framework conducive to overcoming the various transition barriers (Masli, Richardson, Sanchez, & Smith, 2011). While employees continue to use their company issued laptops to remotely connect with their primary computer system, a greater number of employees are requesting that their companies allow the use of personal mobile devices to be used exclusively when working in the field (see Figure 1). This is due to the improvements in mobile technology, including handheld devices and wireless networks. Employees have increasingly found that they can be as productive with their mobile

devices in the field as they could be in a office (Smith & Forman, 2014). Consequently, organizational managers are beginning to investigate the IT infrastructure to assess whether it can support these devices or integrate additional equipment to ensure a consistent and reliable response for growing support expectations (Morabito, Sack, Stohr, & Bhate, 2009).

Several infrastructure factors must be considered prior to the transition from a traditional office to an *anytime, anywhere office*. These factors include designing, establishing, and executing an effective mobile strategy that can support a wide variety of handheld mobile devices. Such a design would need to provide a comprehensive and unified mobile experience, which includes rich functionality for mobile-device applications (Payne, 2006). But several risks are introduced with the implementation of mobile devices into an enterprise computer system. The Business Performance Management Forum (as cited in Frolick & Ariyachandra, 2008) found that most companies have not created policies to ensure security compliance, and those with such policies in place are typically unable to enforce their requirements. Improper levels of protection against lost or stolen devices has resulted in the loss of valuable data that could jeopardize the entire business (Frolick & Ariyachandra, 2008).

When businesses embark on projects to develop an advanced mobile-service system, the risks are high. Problems often emerge with content management, device limitations, and the creation of formats that are compatible with the ever-increasing number of devices. This can cause project failure because of associated complexity in the design and cost. The majority of business managers struggle with analyzing the various

mobile devices on the market to determine the best methods to maintain their current level of service (Fitzgerald, 2009). Inaccurate analysis on the type of devices and methods can result in cost overruns and, ultimately, an ineffective business model. Therefore, for mobile-device projects to be successful, proper metrics and governance must first be in place (Saravani & Haddow, 2011).

Figure 1. Relationships between various electronic devices. Each device can be used independently or collectively by an independent user with the IT computer system. From *Making Business Intelligence Easy* (p. 7), by Lachlan James, 2011. Copyright 2011 by Lachlan James. Reprinted with permission.

Technology Innovation

Innovation in technology is a key to business success. The challenge is to merge new technology with fiscal and technological constraints while maintaining existing infrastructure investments. An open-technology system that is always connected via mobile devices is such an approach. This type of environment facilitates an efficient integration that may reduce costs and encourage efforts toward an integrated operational

readiness with standards and protocols across the enterprise. The benefits of mobile technology, including the constant connection and accessibility, enable workers to adapt their work lifestyle for efficiency. In the process, they remove the boundaries between work and personal life (Peters & Allouch, 2005), which gives mobile users the desire to use their personal devices for both business and social purposes.

Investing in mobile operation can introduce several risks to the corporate information system through external components, which corporate stakeholders must proactively minimize. The adoption of an enterprise mobility process can be a key business activity and its success will depend upon how closely it is aligned with both the business and management intentions for IT. A successful mobility plan focuses on the business process and is incorporated in a multiple-phase approach, allowing significant time for discovery, development, and deployment. This, the business can gain valuable insight during each phase on how to build an effective mobilization force and determine the order that various business processes can be most efficiently implemented (Brown & Sikes, 2011).

The existing literature on supporting and securing mobile devices indicates that minimal research has been done on the internal factors affecting the corporate success of personal mobility. Most studies point to external factors, such as application downloads or the type of available devices (Ahmad, 2009). Although, factors such as functionality, workforce productivity, physical constraints, time-zone differences, resources, and geographic location affect the success of personal mobility, little data is available to substantiate this claim. As noted by Oren (2009), easily defined variables such as cost,

scope, and schedule are factors concentrated on rather than how to secure or support personal mobile devices.

Problem Statement

Companies are having to address significant number of employees using personal mobile devices to connect to company computer systems with or without approval (Signorini & Hochmuth, 2010). But there is a lack of research on the security and support issues. Researchers have noted how mobile devices are transforming the workplace into a transparent landscape. Mobile devices are limiting reliance on physical location and increasing business productivity. Workers increasingly rely upon mobile devices to research their competition products and conduct business transactions across mobile networks (Swaroop, Kumar, & Shanker, 2011). However, IT personnel have limited understanding of the factors that would make connecting personal mobile devices with the appropriate support and security to the corporate information computer systems a success. Nevertheless, IT does know that there are several factors that would affect the success of this integration: management, individual, and organization, along with factors such as personal data loss, privacy, device seizure resulting in legal matters and, transaction processing.

The literature review notes that some companies are ready to allow use of mobile-device applications to deliver increased customer satisfaction and productivity but lack the ability to enforce acceptable use policies (Bellavista, Xie, & Tugcu, 2009). Furthermore, there is also a concern about the changing nature of how work is performed by employees using their own personal mobile devices for business and personal use

during and after established working hours as it pertains to human resource regulations policies (Viscusi, 2006).

Purpose of the Study

The purpose of this quantitative survey study was to examine the relationship between employees desire to use personal mobile devices and a corporation's needs for security by ensuring regulatory compliance to guard against unauthorized access to a communications network and support procedures to maintain the operating functionality of the mobile device. The quantitative approach produced the statistical data needed to understand the relationships among the independent variables of support and security and the dependent variable of personal mobile devices (see Figure 2). A survey was administered with questions based on factors identified in the literature review.

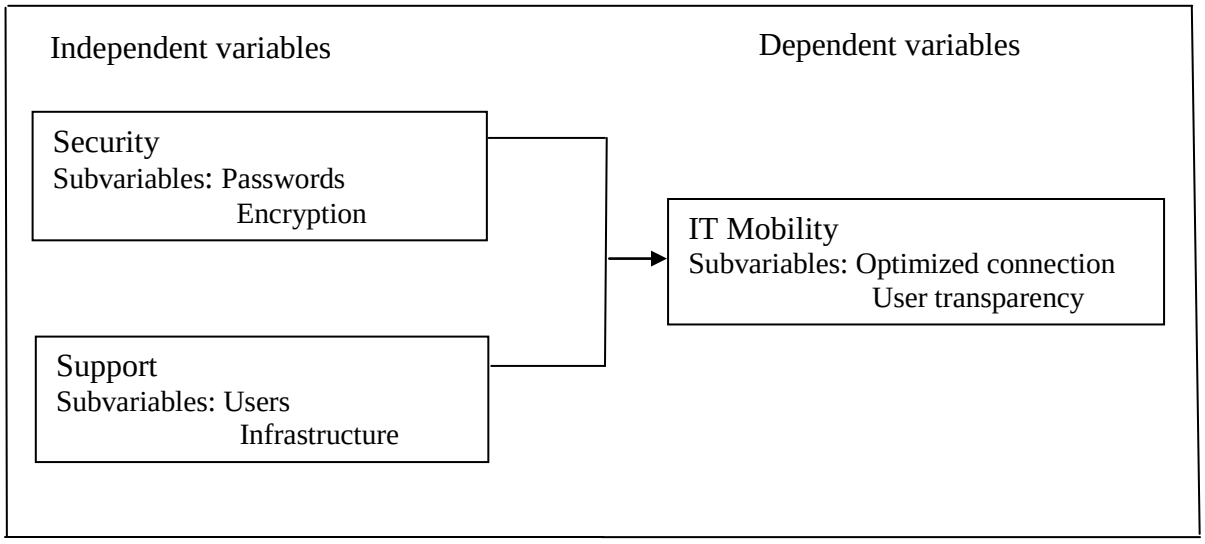


Figure 2. Relationship between variables and subvariable models.

Research Questions and Hypotheses

Descriptive and inferential statistics were used to test the relationships with the

research question and hypotheses . Descriptive statistics help to describe and summarize the data in a meaningful way. They can be used to produce various charts and graphs about variance, standard deviation, and statistics used in analyzing data. They allow the researcher to show the mean, median, and mode from the collected data.

While descriptive statistics are useful in summarizing raw data, they cannot help draw conclusions about the population from which the samples were taken. Therefore, inferential statistics tests were used to examine the hypotheses, for example, mobile use score, standardized regression analysis, and chi-square among others. The statistic draws conclusions about the population to infer what its members may be thinking. Inferential statistics are based on probability values or *p-values*, which were used to accept or reject the null hypothesis. A low p-value indicates a low probability that the null hypothesis is correct, thus providing evidence that the alternative hypothesis is correct (Byrne, 2007).

The following research question and corresponding hypotheses were used to guide the study:

Does security and support affect the successful integration of personal mobile devices? Integration is the ability to successfully connect electronic components without error for transaction purposes.

To test the following hypotheses, the study compared survey questions 11 – 15 with the independent variable, Support, and dependent variable, Personal Mobile Devices (see Appendix B).

H_{01}*:* There is no relationship between the use of personal mobile devices and corporate support.

H_{A1}: There is a relationship between the use of personal mobile devices and corporate support.

To test the following hypotheses, the study compared Survey Questions 16–20 with the independent variable, Security, and the dependent variable, Personal Mobile Devices (see Appendix B).

H_{02}:There is no relationship between the use of personal mobile devices and corporate security.

H_{A2}: There is a relationship between the use of personal mobile devices and corporate security.

Theoretical Framework

The theoretical framework for the study was derived from IT product life-cycle management theory, IT security-management theory, and IT strategic-management theory. Mobile contexts that address the personal preferences of users can strongly affect the operations method via the user interface. The quantity and quality of the service content that users need to access through their mobile devices, and the interconnection to other devices or services within the user environment, must be considered. User-interface design for mobile communication devices has not been a major research topic. Therefore, it is necessary to design research to lay the foundation for what is considered a good user interface for the various types of mobile devices. The goal is to understand the characteristics of the environments within which mobile devices can fit, both in the present and in the future, as well as to elaborate on the consequences of the user-interface design for future communication devices.

The product life cycle is the period of time a product remains on the market (Drejer, 2004). However, there are multiple descriptions of product life-cycle based on the product, the perceptions of customers, and the enterprise. The enterprise view may include when the product ceases to be produced or supported. The customer view is based on when the product is no longer used and is discarded. The product analysis of the life cycle is when the type of product, market segment, or single product is no longer used (Lo Storto, 2010).

Product life-cycle management is an administrative model and tactical approach to creating and managing the product-related capital of a business. This process is used to follow a product from introduction to retirement. As an IT undertaking, support of product life-cycle management involves modeling, capturing, exchanging, and using information during the entire decision-making process (Terzi, 2005). As a business continues to grow, it grows in complexity and encounters more challenges. Inevitably, these challenges lead to the addition of new tools and technology to continue improving on the process that leads to new complexities that business managers must begin to consider with the integration of mobile technology. With the increase of employee-purchased mobile devices, managers are considering the effect of incorporating the technology into daily work routines (Flisi, 2000). Organization management has been slower to adopt and use these devices as part of its business and IT strategy. To persuade them to invest in mobile technologies, they must be convinced that it is important to the achievement of corporate goals. While it is equally important to evaluate the potential life-cycle of these products to understand which will withstand the abuse of real-world

settings (Terzi, 2005).

IT Security-Management Theory

This theory mainly addresses the detection and prevention of unauthorized acts of computer users (Chenoweth, Minch, & Tabor, 2010). However, its broader objectives are to enforce company policy with regard to ensuring data confidentiality, integrity, and availability. The full scope of IT security management covers a mix of security policies, risk analysis, risk management, contingency planning, and disaster recovery (Schultz, 2002).

Securing IT network systems, a crucial business need, is now common practice due mainly to the increase of new technology that is playing an important role in transmitting information across various network systems. Two converging trends are causing security concerns among IT professionals. The first is the proliferation of smart mobile devices that have as much processing capacity and application performance as most desktop computers. The second is based upon open operating systems for mobile devices that are creating targets appealing to those with malicious intentions (Garretson, 2007). Over 228 million smartphones were deployed in 2007 compared to the 233 million personal computers sold in 2006. As mobile-device use increases, threats to their security concurrently increase, causing these devices to lose their immunity to the common threats that have plagued desktops and laptops. Consequently, a comprehensive and effective mobile security strategy is required. This strategy must include device management, either preinstalled on the device or downloaded by the user, which will protect against threats to the operating system and application. The strategy must also include protection

and preservation of user data if the device is lost or stolen (Smith, 2010).

Strategic Management Theory

Strategic management is a comparatively new theory within the field of managerial practice and is closely related to the realm of organizational structure. The approach emphasizes the complex challenges of managing diverse practices, regardless of their structure (Miller & Tsang, 2011). Strategic management also involves aligning an organization with changing trends, which may include environmental change or shifts in competition, regulation, customer preferences, political will, the availability of technology, and/or economic conditions. For any given organization, these changes may serve as either threats or opportunities and can occur at the market, industry, or societal level.

Within IT strategic-management theory, there is an understanding of various capabilities within a business, including technology management; this is crucial because of the critical role technology plays when generating and executing company strategies (Burgelman, Maidique, & Wheelwright, 2001). Technology management has been studied by scholars as an independent discipline. Yet Brent and Pretorius (2008) found that there are no commonly accepted theoretical and practical frameworks for this type of management. They claim that, due to the nature of technology, positioning strategic technology management is difficult to interlock. While other multiple theoretical frameworks try to help describe elements of IT strategic management, the overall concepts are blurred. Regardless, technology aspects must be properly considered because they are involved in all activities of business (Jang, 2009). Business and product

strategy must ensure that technological matters are aligned with business needs for optimal performance and competitiveness (Momaya & Ajitabh, 2005). However, developing an IT strategy is a challenge because of the abstract dimension of future planning. Uncertainty is inherent in technological developments, because of the complexity and uncertainty of human intervention which is a concern for strategy configuration, implementation, and sustainable development (Paap & Katz, 2004).

Nature of the Study

The study used a quantitative approach with a survey; the findings were statistically analyzed. Numerical data were collected and analyzed using mathematical methods to determine the results. This type of research necessitates a clear understanding of the dependent and independent variables (Sukamolson, n.d.). These variables were determined by investigating the relationship between security and support and deployment of personal mobile electronic devices to an existing computer network environment. Four types of quantitative designs are common to contemporary research of this nature—descriptive, correlational, quasi-experimental, and experimental. The choice of design is dependent upon the level of knowledge about the research problem or the objective of the study.

A large amount of research on intergrating IT equipment and mobile devices is descriptive in nature. Thus, the next logical approach would be a correlational study to examine any relationships between the variables. Once these two designs were performed, the path would lead to quasi-experimental and experimental research. Very few studies have been conducted using a correlational approach that focused on the

impact of personal mobiilty devices to interacting with current IT systems and measuring the degree of dependency due to the lack of existing system guidelines. Thus, to determine the relationship between the independent and dependent variables, a quantitative design was the appropriate choice (Creswell, 2003).

A survey was ideal for collecting data- for the study (Neuman, 2006). Participants were asked to complete an electronic survey. Simon and Francis (2006) stated, "If a significant relationship exists between the two variables, it does not necessarily mean than one causes the other" (p. 45). The data is collected and values are determined, which in turn, facilitates determination of the strength of the relationship between the variables. The quantitative method is optimal avenue accepting or rejecting hypotheses and thus establishing a relationship between dependent (i.e., personal mobile electronic devices within an existing IT environment) and independent variables (i.e., support or security). As noted by Creswell (2009), qualitative methodology is unsuitable for this research because it requires extensive time with In-depth interviews, time in the field, effort, and cost.

Definition of Terms

Electronic applications: A computer program enabling users to accomplish specific tasks (List of programming and computer science terms, 2011).

Enterprise: A company, firm, or business endeavor (List of programming and computer science terms, 2011).

Information technology (IT): A computer-based tool used to manipulate, store, or communicate information supporting the IT needs of an organization (Haag, Cummings,

& McCubbrey, 2005).

Mobile electronic device: A pocket-sized computing device, typically with a display screen and miniature keyboard (*Mobile Electronics Glossary,* 2011).

Mobile operating system: The software platform upon which other application programs run on mobile devices (Frese, 2003).

Project failure: A project that is not delivered on time nor within budget and does not meet the original expectations (Frese, 2003).

Project success: Determined when a project is completed on time, within budget, and with all features and functionality specified within the project agreement (Frese, 2003).

Secure: discipline governing the framework for the continuous cycle of safeguarding information and ensuring related regulatory compliance (Pfaffenberger, 2009).

Support: The maintenance and service associated with the software or hardware of a computer device (Mobile Electronics Glossary, 2011).

Assumptions

Assumptions are things that are taken for granted and are out of the researcher's control, but need to be identified; "they are so basic that, without them, the research problem itself could not exist" (Leedy & Ormrod, 2005, p. 62). Assumptions are in reference to participants answering truthfully to the survey questions; another is that the sample is a correct representative of the population for the study and that they are willing to participate in the study without bias. One assumption is that because participants work

within IT, they are experienced in working on IT projects. Another assumption is that the participants understand the security and support issues with various mobile devices. The third assumption is that the participants answered the survey truthfully and without bias because of confidentiality that was provided.

Scope and Delimitations

The scope of the study was to examine the relationships between supporting, securing or both, personal mobile devices that are allowed access to an existing corporate information systems. A delimitation of the study was that the sample was comprised only of personnel working at the study site. The results may differ with a sample derived from another organization. Allowing personal mobile devices within the workplace is a new practice. The survey was an online questionnaire via an online survey service. The survey was conducted only once prior to data analysis. The time to complete the survey following distribution was limited to 30 days.

Limitations

All studies have limitations. They need to be identified and taken into account because (a) they can affect the quality of the research and (b) some could be seen as fruitful avenues for future research under the same theme. This study presented several limitations. The sample consisted of IT personnel working for a large, multinational company, which will not provide generalizability. Participants may not report accurate numbers and there is no way to verify their reports. IT personnel may not wish to provide answers to sensitive questions such as the types of devices used, security barriers, and geographic locations. Furthermore, there was a concern with biases that could threaten

the validity of the study. Not all biases can be eliminated; therefore, the researcher will need to acknowledge their presence within the study and state what impact they may have on the results.

Significance of the Study

The study was significant because it holds the potential of verifying the statistical relationship between (a) internal organizational factors and (b) the success of integrating personal mobile devices into an existing corporate information system. The findings may help business management develop strategies that could leading to reduced costs and reinvestment in future mobile environments. Factors such as project management, productivity, cost benefits, and efficiency will be considered with strategic mobile planning. An IT system is a single unified system that integrates all data and business processes to fulfill essential organizational goals. This system is comprised of a set of different modules such as supply-chain management, customer-relationship management, human-resource management, and data warehousing. These modules can be further categorized into different submodules, which indicates the importance and complexity of enterprise systems within the corporate world.

Significance to Theory

Mobile technologies are gaining momentum within the business market, not only as a consumer product, but also as an extension tool for the mobile workforce. These products are to increase business strategies on a global scale by supporting organizational processes, particularly when integrated with Internet-based technologies (Varshney & Vetter, 2001). However, with the influx of demand for various personal mobile devices to

connect and interface with enterprise perimeters, IT personnel are facing an extremely difficult task with supporting or securing these devices. Mobile game plans and updated enterprise architectures are required to handle both daily and long-term challenges. The use of mobility as an effective tool will only be as good as the connection it has to any back-end system.

Organizations desiring to mobilize enterprise applications must thoroughly evaluate several high-level considerations well ahead of extending such applications to personal devices. Examples would include

- What mobile operating system is recommended by the IT department?
- Is this operating-system preference consistent with the majority of mobile devices currently installed among the employee population?
- Should the organization deploy individual mobile enterprise applications or provide enterprise access through a mobile browser?
- Will the company impose corporate policy relative to the employee-owned personal devices?
- Does the operating system meet the criteria of the corporate security policy?

Once these considerations have been addressed, the respective company managers can determine whether the implementation of personal mobile devices can be conducted with confidence.

As company management considers the influx of personal mobile devices into the workplace, security will not be the sole concern. Wireless bandwidth issues and privacy and compliance-related concerns will also need to be addressed to protect against

employees circumventing policies to get their personal devices connected. This could force IT teams into security breaches that could, in turn, compromise security for the entire enterprise. IT teams must be able to accurately measure security versus access with each emerging situation. Consequently, a successful implementation plan is crucial for mobile-device IT projects. Such plans can lead to strategic maneuvers, strategic transformations, significant improvements, cost reduction, greater efficiency, higher quality end products, a more significant competitive advantage, and breakthrough innovation.

Managers of IT organizations must be able to identify which devices are connecting to the network. This can be accomplished by defining metrics with the capabilities of identifying devices trying to connect to the system. Once this information is known, access policies can be created to help control who and what is making that connection and differentiate that access based upon established criteria and new-device guidelines (Grant, 2008). Upon conclusion of the research, managers may be able to provide valuable network visibility while also pinpointing potential security vulnerability. Such insight will enable organizations to take a proactive stance with tracking, logging, and managing every mobile device connected to their networks, eliminating the guesswork.

Significance to Practice

As with most investment decisions, there must always be a justifiable and observable return on investment. This is the most prevalent criteria to adopt (Mukherjee, 2008), particularly with the strategical planning for the introduction of mobile devices.

However, most businesses fail to place a value on the incorporation of mobile devices because the related return on investment is not always clearly identified, and in many instances, that value is a complete unknown (Bulearca & Bulearca, 2009). One of the intriguing values enterprise mobility solutions offer with the investment of technology is the ability to access network resources at all times. This is clearly beneficial and a key driver of business performance (Alkazemi, 2012).

Remote workers are no longer dependent upon their desktop computers to check critical data transmissions. With the use of mobile devices, workers are able to receive timely information, which in turn, can lead to timely decision making to achieve potentially significant cost savings. With less expensive handheld devices, remote workers can have immediate access to all business sources, thereby replacing older processes with newer mobilized applications. This alleviates the potential for data error when transferring information back to the IT system. By using mobile technology accuracy and integrity can increase, which in turn, can be harvested for overall business intelligence use. Data can be collected in real time and transmitted to the business system far faster than the traditional order-shipping and collections processes. The downstream benefits include lower inventory, efficient routing of multidrop deliveries, and greater customer satisfaction (Rouse, 2005).

Significance to Social Change

Success with mobile implementation would allow organizations the ability to use personal mobile devices within their own enterprise IT system to reduce cost, improve productivity, and increase employee satisfaction. However, mature business processes,

workflows, and data modeling are key success drivers for mobile projects. The implications for social change are as mobile devices become more sophisticated, the demands for this technology within business environments can rapidly increased. Thereby, being able to supply real-time access to employer's corporate information systems, employees will benefit by efficiently achieving their goals to swiftly respond to market opportunities that would otherwise result in business loss or losing a competitive edge (James, 2011). Companies are much more likely to achieve competitive advantage and earn above average profits if managers are able to find unique ways of delivering superior value to customers (Ziolkowski, 2011). Once businesses realize the benefits associated with personal mobile devices the demand will increase.

While mobile devices are becoming prevalent in private, public and government sectors, the significant implications on integrations to existing information technology environments remains unknown. By using mobile technology, accuracy and integrity can increase, which in turn, can be harvested for overall business intelligence use. Data can be collected by the employee in real time and transmitted to the business system faster than the traditional order shipping and collection processes. The downstream benefits include lower inventory, efficient routing of multidrop deliveries, and greater customer satisfaction (Rouse, 2005). This leads to workers increasingly relying upon mobile devices regardless of location to research products and conduct transactions across mobile networks which require instant access to data on an ongoing basis. (Swaroop, Kumar, & Shanker, 2011). By allowing employees the advantages of moving beyond the standard office environment and start using mobility to conduct transactions it is a win

for all parities.

Summary and Transition

There is a clear need for all workers to perform with greater efficiency. This is achieved by companies that provide their employees with secure, consistent access to information, which in turn, allows workers to develop an advantage over larger competitors. Employees who can react quickly to business or market changes are better equipped to successfully handle customer complaints and any major changes in organizational strategies. Allowing workers to move beyond the standard office with greater mobility and innovative means of connectivity includes allowing the use of personal mobile devices.

Mobile communication plays a central role in the transition of business within the global marketplace. Adoption rates surpass even those of Internet usage. The widespread use of mobile devices is creating a shift toward a personal-communication society. This is evidenced by several key factors including teams able to work together with far greater efficiency, sharing data and assessing the efficacy of their programs while working remotely. IT has traditionally discouraged the use of personal devices by locking down access to resources to ensure data, application, and network security. However, contemporary IT leaders are abandoning this rigid approach to security and adopting new policy that supports popular mobile operating systems and enables user-owned devices to connect to corporate resources.

The indication is there are areas for improvement among those working with personal mobile devices, which, if addressed, could improve the success rate of corporate

projects and office functions. The findings may lead to new methods of working and greater collaboration toward higher corporate profits. Businesses are learning more about the ways mobile technology can be used to increase productivity and subsequent profitability. Sharing information through mobile devices allows businesses to collect immediate feedback on products and services from customers. The speed and accessibility can lead to faster research and development, an important facet of market competitiveness. This also can lead to product upgrades moving at a faster rate, allowing both employees and clients to sense a more direct role in the development plans of the enterprise.

This can also facilitate improved IT governance, budgets, and efficiency within both the public and private sectors. New data and academic thought processes can enhance technology adoption and implementation within various types of organizations. Through the successful implementation of personal IT mobile devices, organizations can deliver services with greater efficiency and fewer errors, resulting in a healthier, safer, and more prosperous society.

Chapter 2 provides a literature review of relevant research on various factors concerning mobile IT success. Chapter 3 describes the research design, role of the researcher, methodology, survey method, sample size, data collection details, data analysis and reliability and validity . Chapter 4 will provide the results of the study, data collections and analysis of the hypothesis. Chapter 5 will give the findings, recommendations and implications.

Chapter 2: Literature Review

The purpose of this quantitative study was to examine the relationship between employees desire to use personal mobile devices and a corporation's need for security by ensuring physical regulatory compliance to guard against unauthorized access to a communications network and support procedures to maintain the operating functionality of the mobile device. Mobile-device technologies can uniquely contribute to the communications revolution by eliminating the need for physical, land-based connectivity between people, processes, and entities. Businesses that adopt a mobile, wireless connectivity solution may have a significant effect on productivity, irrespective of the size and location of the organization. Another effect would be to change the respective organizational structures both internal and external business processes by allowing these devices access to corporate information systems.

This review of literature indicates a direct positive relationship between employee confidence level and perception of their job performance while using mobile devices. However, there is a lack of data identifying the type of devices used as personally-owned, as well as a void in any conclusions about the ability of the participating companies to secure and support these devices.

The use of mobile devices may affect relationships with customers, employees, partners, and stakeholders (Kahn & Urie, 2011). The need for technological innovation is continually increasing to provide a source of competitive advantage (Perdomo-Ortiz, Gonzalez-Benito, & Galende, 2009). The challenge is to institute a standard process that will allow the integration of new technology as with mobile devices into existing systems

that address current and future fiscal and technological constraints. One approach is to allow mobile devices to connect seamlessly by adopting an open-architecture operating-system model, while ensuring that security is maintained (Peters & Allouch, 2005).

Open architecture is also known as open system, is a construction that is designed with precisely defined modules and interfaces. These interfaces allow independent suppliers the ability to provide new modules with the capabilities interacting with the existing systems without unlimited and unrestricted third-party development. This exists when industry standard communication architecture allows hardware to be interchangeable under common protocols, thereby, standardizing the communications between devices throughout the industry. This means that a company can purchase components from various vendors and install them together to form a cohesive system that is secure. Thereby, conforming to an open architecture stops the need for massive system replacements just to use the latest new technology. With the use of common standard communication this allows newer equipment the capability of interfacing with older hardware thereby expanding the life of the facility system (Indulska, Loke, Rakotonirainy, Witana, & Zaslavsky, 2002).

One of the primary benefits of open architecture is that it allows combinations of proprietary and nonproprietary strategies to reside on a single system. These benefits includes the company being able to shop around with various manufactures to gain a competitive price for new equipment. As a system continues to expands, new individual components can be added one by one to prevent a massive overhaul of the IT environment facility's system every few years because as new software and hardware

components becomes available, the open architecture standard ensures that these products will interface with the older products plus can offer the important features and capabilities with security and support (Jacobides, & Billinger, 2006) .

Literature Search Strategy

In searching the literature for peer-reviewed articles and dissertations, the following databases were used: EBSCOhost, Emerald, ProQuest, and Thomson Gale Info Trac. Keywords or phrases used in the search were *IT, electronic mobile devices, connectivity communication,* and *the effect of external factors on mobile devices.*

The following topics were discussed in this review :

- mobile electronic-device management
- mobile-device project-success model
- interface and mobile middleware and application
- innovation and future planning
- implementing change and social strategy
- methods

Theoretical Foundation

May (2010) noted that the most important technology product was no longer sitting on a desk, but rather, fits in the hand. Mobile phones have become the most prevalent tool for media consumption and communication worldwide. The International Telecommunication Union estimated that 4.6 billion mobile-phone subscriptions are active, compared to the 1.2 billion personal computers in use (Hennig, 2010). Of the 83% of American adults who own a mobile phone, 93% are adults between 18 and 29 years of

age (Lenhart, Ling, Campbell, & Purcell, 2010). As the development of mobile phones continues to advance, they are divided into two categories—feature phones and smartphones. Feature phones are basic mobile phones that can run simple applications, but typically do not connect to the Internet, while smartphones are mobile phones that have advanced computing abilities such as a complete operating system and Internet capabilities (Entner, 2010).

According to Daesung et al(2010), smartphones have become a widespread communications tool for employees, serving as a mobile extension to their desktop computers. These phones allow employees to access their corporate information systems while out of the office, providing the freedom to read e-mail, answer urgent messages, store presentations, and access business reports while on the go. Some companies are allowing their employees to use their smartphones to connect to the company computer system so they can be productive from any location. However, allowing such access to primary systems can result in problems with security and support (Daesung, Byungkwan, Yongwha, & Jin-Won, 2010).

Enterprise IT service providers are encountering challenges in delivering secure remote-network access, while concurrently limiting resource access based upon authentication, authorization, and user identity. The provision of such service introduces a complex security problem because, if a personal mobile device is left unprotected, it can lead to loss, theft, and the compromise of valuable confidential data for both the corporation and employee. Smartphones are not equipped with security measures of equivalent strength to those typically embedded within other mobile IT equipment such

as laptops. Therefore, it is not surprising that smartphones are often targeted by criminal organizations. Absolutely, it is crucial that any business planning to allow personal mobile devices consider carefully whether use of the device for such purposes is appropriate and cost effective (Fang-Yie, Ilsun, Feilong, Palmieri, Fiore, & Castiglione, 2011).

While reducing costs and increasing employee morale are popular arguments for allowing mobile devices, organizations also have to consider any hidden costs with this initiative. The ability to allow employees to use their devices at work may help increase productivity and raise confidence levels; however there are other considerations companies will have to be on guard for when developing their mobile use plans. One consideration is any new expenses borne by employees. These new expenses may eliminate any goodwill associated with allowing employee owned devices allowed to connect to the company IT system. To offset this some organizations are offering their employees a fixed monthly stipend to help with their monthly voice and data bill. This approach results in predictable mobile expenses for the employees while they continue to be responsible for the costs of their mobile devices and data plans (Berl & de Meer, 2011).

Other costs may come with security measures required to mitigate the risks associated with employees own devices and the applications installed on the device. These security risks could expose corporate data or contaminate other devices within the company's network. Thereby, causing additional security related costs to the company to support mobility platforms. Another area of cost may come from resource allocations;

with the introduction of a wider variety of devices. Support costs may increase as more and higher-skilled help desk personnel may be required to handle the overload. Other concerns outside of the IT department may be raised by human resources, finance, and corporate legal. To mitigate liability risks to the organization, legal and human resources may implement an employee agreement document to address topics that include acceptable use of personal devices and corporate access. Corporate finance will have to address any expenditures occurred to determine if the origination is responsible for reimbursement to employees. Corporate legal will carefully consider any record keeping requirements or logs made from mobile devices to evaluate any potential legal consequences while using employee owned devices (Guerrero, Ochoa, Pino, & Collazos, 2006).

Governance over BYOD

Personal mobile device programs also known as bring your own device (BYOD), allows access to company emails and internal network computers. Companies are finding that by allowing employees to use their BYOD, it introduces potential risks requiring assessment and evaluation by internal auditors. Audit reviews are being used to identify the existence and operating effectiveness of security controls over mobile devices that are designed to protect company data, plus to assess the adequacy of mobile computing security policies, risk assessment, and governance. Most companies have little or no process in place for managing access or storage methods with mobile devices, this lacking can put their data at risk. Therefore, it is critical that organization create governance over mobile device security and use, including roles and responsibilities for

data accessed by mobile device users (Thomas, 2012).

Governance in IT organizations as it relates to BYOD means creating policies which users are free to use whichever device they feel comfortable and have access to company applications and data. Systems, applications, data also fit in to these frameworks to enforce the policies in the organization while allowing freedom of device, location, ownership. A good enterprise mobile governance strategy should help an organization incorporate new business processes, optimize costs, define a clear mobility vision with a roadmap for the future and minimize risk. Governance over mobility framework cannot exist in a silo and must take into consideration business demands and IT requirements by including a plan for managing not only devices but also enterprise applications that run on those devices. A good first step is for the company to participate in a mobile assessment so it can identify the best use cases for allowing mobile technology and develop a long term strategy to solve specific challenges. This will enable an organization to roll out features and solutions based on high-priority needs, as well as avoid engaging in unnecessary and time-consuming mistakes. Determining how to manage and support mobile devices is the cornerstone of a sound governance strategy. It must begin with defining a technical policy based on business inputs and must seek to support and manage multiple devices across platforms and operating systems (Semer, 2013).

Mobile Electronic-Device Management

The requirements of business dynamics demands increasingly faster response from personnel and greater flexibility from the technology upon which they rely. To meet

these challenges, businesses now recognize that mobile devices can offer an excellent solution with both functionality and popularity by enabling remote data accessibility. Increased utilization of the Internet, coupled with advances in wireless communication and powerful mobile devices, have enabled greater business connectivity and a prevailing mobile workforce. The downside to the improved productivity is that the mobile devices may force the relinquishment of technology control by the centralized IT support infrastructure, thereby increasing the challenges of systems management, risk management, and maintaining configuration and compliance initiatives (Tarasewich, 2008).

Once businesses have engaged the mobile-device technology, IT must manage and support the devices with the same rigor and discipline as they manage and support any other critical business resources. This requires effective management of all mobile devices—either personal or business owned—across the full spectrum of IT disciplines. However, simply the mobile nature of the devices renders them considerably difficult to manage and support compared to office-based desktop and laptop computers. Managers of organizations that have enabled mobile users have found that their service desks experience a substantial increase in user support calls. Mobile devices require higher maintenance than desktops and laptops because they are more susceptible to damage, loss, and theft. As a result, they must be replaced with greater frequency. They also introduce an additional layer of complexity to the IT infrastructure because they connect through external wireless networks, while the vast majority of computers connect to the data center either through a private network or the Internet. Therefore, as mobile-device

users move through the world, the networks through which they are connected may change many times (Davis, Schiller, & Wheeler, 2007).

As noted earlier, mobile devices are susceptible to loss and theft, thereby rendering the protection of any sensitive information stored on the devices important. This increases the need to ensure consistent security-policy enforcement across the mobile infrastructure including the devices themselves. The dilemma is that the IT staff within most organizations does not have the necessary visibility or control over the devices. There are solutions available that can help provide better visibility and control; however, these are typically used in other segments of the IT infrastructure and not generally implemented separately for mobile-service management. As a result, IT personnel have been forced to manage mobile devices separately from the balance of the IT infrastructure, employing different tools and different skill sets. This hampers incident and problem handling by making it difficult for IT to understand the relationships between mobile devices and the balance of the IT infrastructure. This separation also creates a barrier to smooth process flow across IT groups, thus increasing the risk of error (Jansen, Daniellou, & Cilleros, 2006). However, IT managers are starting to work close with the mobile manufacturer to identify gaps in security, and understand support problems. By taking this approach IT personnel are better able to handle incident problems because they have a better understanding of the relationships between mobile devices and the IT infrastructure (Vacca, 2009).

Supporting and Securing Mobile Devices

A significant amount of security risk to the enterprise configuration is present

with the deployment of mobile devices. The organization and users are susceptible to numerous vulnerabilities, threats, and malicious attacks both internal and external. This includes the networks the mobile devices are using and the threat of data loss. Many of the risks associated with mobile devices exist because of portability. Mobile devices communicate via wireless networks that are typically less secure than wired networks and subject to data loss through interception. Additional problems are that many of these mobile devices have the capability to store data; consequently, loss of the device can result in the compromise of sensitive and proprietary information (Malik, 2011).

As an increasing number of business operations begin to accept mobile devices as a prominent tool, it is imperative that security managers consider how to manage the associated risk. With the introduction of new mobile devices and platforms, IT professionals must update existing, or create new, mobile-device strategies. A strategy must consist of both physical and data elements. This will help ensure that risks are accounted for and managed appropriately. Protecting and enhancing the value of needed information and IT systems have become a central strategic objective in most businesses, second only to making profits. Information security managers will need to address these additional issues such as organizational culture, technology, and governance when creating the strategy (Washburn, 2010). Creating a stringent security strategy that defines guidelines and policies will help lay the foundation for identifying security risk when incorporating mobile devices. This strategy should focus on several key areas including access, data, platform support, management methodology, and devices types allowed. Initially, the organization will need to identify which business data allowed to be

accessed, stored, and processed on the mobile device. Additional consideration will have to be given on the type of protection and to what degree because there are different degrees of access that will require different levels of security controls. Companies will need to determine which mobile device platforms allowed in the business environment and make plans for supporting the device. Various mobile platforms have different native security mechanisms that will need to be outlined and understood for security controls (Farahmand, Navathe, Sharp, & Enslow, 2005).

Literature Review Related to Key Variables

A qualitative research method will not be used in the study based upon the findings of previous research with similar participants and the extensive time necessary in the field to collect and analyze data. Various forms of qualitative study have been implemented such as narrative, phenomenological, based in grounded theory, ethnographical, and case study; however, these designs are not suitable for establishing a relationship between dependent and independent variables. Similar studies to that proposed have applied mixed theory, but this is time consuming and resource intensive, in addition to involving interviews to develop a grounded theory along with a survey to test the theory (Creswell, 2009).

This study collected the perspectives of participants via a set of survey questions. Previous studies have investigated other types of methodology and found that a quantitative design is the optimal selection for a topic such as that proposed (Ahmad, 2009; Basole, 2008; Hu, 2010; Peslak & Stanton, 2007; Standing, Guilfoyle, Lin, & Love, 2006; Weiling & Ping, 2009). Quantitative study can be performed via a number of

methods such as one-on-one interviews, telephone interviews, self-administered questionnaires, or electronic surveys. However, existing literature has found that face-to-face or telephone interviews can be time consuming and expensive (Anderson, Wright, & Wheeler, 2011). Studies have also indicated that the survey method is economical and has been consistently used in past research similar to the type proposed. The sample in the study was comprised of IT professionals previously exposed to electronic surveys. Therefore, use of this type of survey is expected to draw a higher response rate.

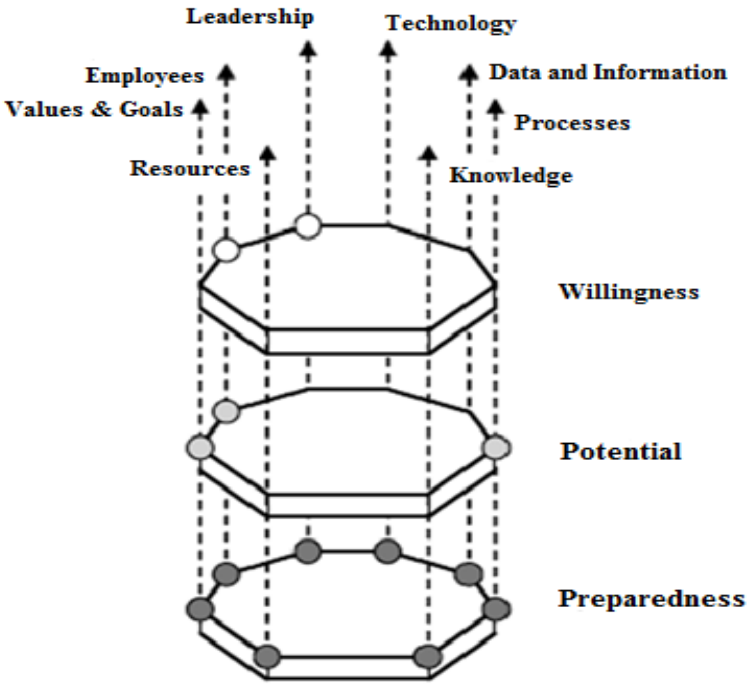


Figure 4. Components to achieve a successful enterprise mobility project. They minimize the associated risks and maximize the potential benefits of enterprise mobility solutions. From *Strategic Planning for Enterprise Mobility: A Readiness-Centric Approach* (p. 3), by R. C. Basole, 2004, Atlanta, GA: Tennenbaum Institute, Georgia Institute of Technology. Copyright 2004 by IFAC. Reprinted with permission.

The review of literature related to the proposed topic of study indicates that, with

the growth of the Internet and the expanded use of electronic mail, electronic surveys are becoming a widely used method of data collection for research analysis. The review further shows that participants with in-depth computer knowledge are more willing to respond to these types of surveys than hard-copy questions (Ward et al., 2005). Adequate consideration must be given to the survey design to ensure it collects the data intended and needed. If the survey is difficult or cumbersome, respondents will not participate. If the questions are in the wrong order, the results could be biased (Yin, 2003).

Company managers are recognizing the advantages of mobile devices to the overall welfare of their enterprises; however, they are struggling with the uncertainty of supporting and securing these devices if they are personally owned. The time is now for businesses to begin planning strategies incorporating standard solutions to the support and deployment of organizational mobilization that will control the cost of these business objectives with successful models. As technology advances continue, mobile-device capabilities increase proportionately. No longer are these devices limited to voice and e-mail components. Current devices present a full range of applications and services including video and voice with data speed that equals or surpasses the desktop computer. This equates to little distinction between the functionality of the desktop computer and mobile devices (Nah, Siau, & Sheng, 2005).

Mobile-Device Project-Success Model

Doherty (2010) noted that project success is derived from two separate components—(a) project-management success, which focuses on the management process; and (b) successful project execution, which entails cost and time effectiveness

along with end-product quality (p. 25). Although product success (i.e., product end quality) is distinguishable from project-management success, the successful outcomes of both are inseparably linked (p. 100). Various project models must be considered when businesses mobilize; identifying the correct model is imperative.

Project teams must consider mobile applications and infrastructures that meet the IT requirements of the enterprise for enabling security, device manageability, and application lifecycle management while maintaining control over development cost and ownership of the devices. Conversely, mobile devices are intrinsically different from any traditional systems previously managed by IT departments and may not fit within routine project norms. End users desire to use the mobile devices and applications they choose due to the expectations surrounding ease of use. To combat this complexity, companies need a flexible, open, and consistent development model that is designed to balance the unique nature of mobility while allowing IT to fulfill its usual requirements (Canali, Colajanni, & Lancellotti, 2010). Any mobile solution will be complex, consisting of various components. Important components that must be considered integral to the mobile project model are interface to back-end systems, mobile middleware, mobile application, network synchronization, and mobile-device strategy (Canali, Colajanni, & Lancellotti, 2010).

Interface and Mobile Middleware and Application

Mobile access to the business computer system is beneficial for mobile workers responsible for resource planning, supply-chain management, and customer-relationship management. Mobile devices can interoperate with these modules from anywhere and at

any time. However, with the implementation of mobile devices, consideration and preparation is needed with regard to how the data content is targeted to various devices. This is a complex task requiring special content adaptation methods or, at a minimum, design principles addressing the characteristics of the mobile devices, mobile environment, mobile networks and data-transfer rates, and the input and output capabilities of a mobile handset (Hussain & Kutar, 2012).

Middleware is a layer of software and hardware that resides between the business applications and the network layer to control various platforms and protocols. This process decouples dependencies within the operating systems, hardware platforms, and communication protocols from the business applications and allows mobile connectivity. Middleware has been used for years by market-application developers and is now a critical element in all aspects of the enterprise-software markets orchestrating the business-process flows. (Gajmez, Cubo, Fuentes, & Pimentel, 2012).

Essentially the approach that application developers take toward incorporating mobile devices will dictate the success or failure of a project. If developers consider mobile devices parallel to laptops or desktops, this approach can cause serious problems. Various development tools exist that render it possible to create an application for a desktop computer that can be ported to a mobile device; however, the resulting wireless application is not likely to be effective unless care is taken to customize it to the targeted device. Applications can present substantial risk to security, privacy, and service cost, depending upon the service provider. Application developers can prevent such vulnerability by creating applications that ensure users are notified when a function will

access sensitive information and provide a means of controlling the function. These functions includes access to personal information, contact lists, videos, and photos stored on mobile devices (Kafaie, Kashefi, & Sharifi, 2011).

Mobile-device applications developed for use with an enterprise system are more complex than those developed for the traditional desktop computer or interface systems. Multiple platforms must be supported while managing connectivity to the delivering systems. Therefore, developers will need to employ considerable ingenuity and skill when building interfaces for mobile devices, this is because of the financial impact that is absorbed by the business along with application-development costs that will secure the integrity and help maintain the effectiveness of the enterprise system (Kwong, Chen, & Chan, 2011).

Types of Security

Physical. There are numerous types of security that have to be addressed before the implementation of personal mobile devices. The two main types of security is network and information security. Network security involves methods used to protect the total computer network from unauthorized accesses. Information security is concerned with network security as well as cryptography, access control, physical security, and more. It covers everything from encryption codes, to how computers are locked down and is the intent of this type of security when reference within this study. Mobile-device users trust that their devices will have the capability to keep confidential information truly confidential, thereby limiting access to only the authorized user. Physically securing office and home personal computers have proven to be easier than providing security for

mobile devices. This is because of the small size and portability of these devices, making them a much more attractive theft target. Most devices are carried and can hence be easily misplaced, making them vulnerable to theft and data exposure. Therefore, securing mobile devices must go beyond the traditional physical-security methods to protection after loss or theft. The underlying processes that protect information on computer systems have been well documented. However, applying these same security measures to mobile devices is not as straightforward because security typically depends upon authentication and the ability to distinguish a legitimate from an illegitimate user (Goth, 2012).

Computer systems can and must verify the identity of users prior to granting access to information. Providing such authentication within the mobile domain presents very different challenges. Mobile devices are unique; they are often used by mobile individuals in public places, in short sessions, and often using less robust user interfaces. The problem is that, when a device is physically lost or stolen, the data on the device is also at risk of theft. Therefore, businesses need ways of restricting access to the data residing on the mobile device. This can be accomplished by erasing or encrypting the data. IT departments need to study the type of devices used to determine if remote commands can be signaled to automatically erase data from the devices or lock a device in the event of a security violation. However, the remote erase command may not always be effective because the command will never be triggered if the device is not connected to the Internet or a wireless carrier network. Encryption is another approach that may provide the best protection of data on mobile devices (Daniellou & Cilleros, 2006).

Data. Keeping mobile-device data secure is both a challenge and a critical

requirement. Unfortunately, most users are unaware of how effortless it is to lose data and fail to take the necessary precautions to protect data stored on their mobile devices. Loss of a mobile device could mean the loss and exposure of sensitive information, and this information may be much more valuable than the device itself, placing a corporation at risk. A laptop theft in 2006 involving the Veterans Affairs Department resulted in the exposure of personal information on millions of veterans and cost the Department $20 million in legal settlements (Frieden, 2006). Few mobile devices are sold with data protection; however, those that include such software also have limitations because basic security mechanisms, such as a password requirement or data encryption, are not utilized by the users. Consequently, data is still vulnerable to unauthorized viewing (Solanas, 2010).

As mobile devices continue to evolve with the ability to download programs, share software applications, and store data, these capabilities will create new vulnerabilities. Viruses are one area of vulnerability that affects these devices in various ways. Private data can be transmitted from a phone without owner knowledge or automatically send expensive messages to run up charges. The malware virus is a malicious software program that can affect device performance and functionality. Smartphones are susceptible to such viruses. They run on open operating systems and have capabilities such as Web browsing, e-mail, flash memory-card readers, and short-range Bluetooth. Each of these features offers a conduit through which Malware can propagate (Jamaluddin, Zotou, Edwards, & Coulton, 2004).

Bluetooth technology can receive and transmit data with another device by sheer

proximity, exemplifying the ease by which viruses can spread among vulnerable phones. A Bluetooth-equipped Smartphone can identify and exchange files with other Bluetooth devices from a distance of 10 meters or more. Consequently, as victims move from place to place, they can infect other devices with no knowledge of the transmission. Another type of virus is the Cabir, which spread so rapidly through an audience at the 2005 world track and field championships in Helsinki that stadium operators flashed warnings on the big screen. However, there are simple means of protecting against such an attack by using the security features on the phone; yet, few users take advantage of these features (Davis, Bodmer, & LeMasters, 2010).

Authentication. As mobile devices continue to grow in popularity and functionality, the ability to ensure and maintain unique user verification is imperative. The dilemma is that, when considering the different types of authentication mechanisms currently available, none satisfy the requirements for all users across all mobile devices. This is complicated by the dynamic and varied environment within which mobile devices operate. Functionality, processing, and memory capabilities vary, and differing network-access technologies exist along with the number of stakeholders interested in the device (Nixon, Tan, & Chellapppa, 2006).

The topology of an authentication mechanism is an important factor to consider at the onset of any security design process. Several groups depend upon identity-verification security to maintain their privacy because of the operational effect of mobile devices. These groups include network operators, corporate IT administrators, and end users. However, because of the various levels of security that can be established, it can be

difficult to maintain security and privacy for all stakeholders, and there are trade-offs depending upon what the system is attempting to optimally achieve. A number of trends have been identified with the planned use of authentication security within various industries. For example, applications are being created to strengthen existing single-factor authentication solutions. This trend can be observed in the financial-services arena with the introduction of additional security questions in combination with the logon ID and password as part of the authentication process. Another trend is use of a personal identification number (PIN) with credit-card purchases, which requires the user to enter a PIN in addition to the credit-card number for online purchases (Aloul, Zahidi, & El-Hajj, 2009).

Two-factor authentications use a token, which is a security device issued to authorized users along with a PIN. This type of authentication is used primarily within the financial-services industry and government applications. A new attempt at authentication is the chip card coupled with PINs, which has been implemented across corporations for financial transactions. However, this method is used primarily by international companies; it is unclear how it can be utilized within the online environment (Burr, Dodson, & Polk, 2008).

Other trends of authentication include continued use by e-commerce applications of single-factor authentication. This is an application used for information browsing through an online catalogue (Yan, Blackwell, Anderson, & Grant, 2004). Enterprise-wide authentication solutions eliminate single verification across different business units of an organization (Eliasson, Fiedler, & Jorstad, 2009). The latest solution, which is in its early

stages of development is the federations of authentication, with which enterprises adopt interoperability to form a federation of e-businesses. This leads to standards that are both industry specific and relevant across industries (Thanh, Jorstad, Jonvik, & Thuan, 2009).

Organizations have identified three key component challenges they must attempt to balance with an authentication solution—cost effectiveness, authentication strength, and ease of use. However, by increasing the strength of one requirement, it is often at the expense of another component. For example, by increasing the strength of the authentication technology, ease of use is typically affected, as well as cost effectiveness. Conversely, a solution with increased user friendliness (i.e., simplicity) is often at the expense of authentication strength. Therefore, organizations are reluctant to implement authentication solutions that interrupt, lengthen, or complicate a transaction process due to the potential for user dissatisfaction (Eliasson et al., 2009).

Mobile-Device Strategy

A mobility strategy must be designed with consideration to the business as a whole, rather than merely a reaction to the latest trend or popular device. To remain competitive, companies need to have a mobile strategy and reiterate it often. The greatest chance for success is to have the mobile strategy aligned with the IT technology goals, the usage patterns of the target audience, and the budget. The strategy will need a phased mobile roadmap, and leverage as much as possible any existing technology to maximize the budget, and extend any consistent experience in transformation. This strategy starts with defining the mobile goals for the company. Once this has been accomplished the company will have a better understanding of the target audience, budget and internal

efforts. A synergy among users is a goal, with the primary focus on those actively using their mobile devices to increase business success. The strategy must meet the requirements of various types of mobile devices because there is no single technology or service plan that can be expected to meet the entire set of enterprise-mobility requirements. As individuals within an organization begin to rely upon their mobile devices, they will have different communication needs, depending upon their work roles and responsibilities (Crumlish & Malone, 2009).

Once the development of a strategy plan is underway, the IT team needs to consider how, and at what cost, the mobile devices will interact with the balance of their complex systems. Incorporating a cost-management plan to ensure that existing networks and solutions are effectively leveraged to keep capital and operating expenditures under control is one avenue. Approaching integration from a strategic perspective to determine how mobile devices will operate with existing infrastructures and tools may open innovative opportunities with existing and new business processes that could potentially strengthen the competitive stance of the enterprise (see Figure 3). Thus, organization managers can maintain mobility costs and support users. The core of the mobility strategy must be the users, determining their needs and working efficiently and effectively to meet them on behalf of the organization as a whole (Yoo, 2011).

However, mobile strategy success isn't just implementing the right technology but also requires smart policies and clear communication with employees. This is due to the fact that the insertion of employee-owned devices within an IT environment is a very new experience and will require considerations and agreements from a variety of

different views. The right combination can contribute a wealth of insight and experience into the formulation of a company's mobile policies. An example would be if employees lost their mobile device and the company needed to immediately delete all information both personal and professional from the device. There are also legal agreements concerning company functions with mobile devices after hours that may affect labor unions, rules, contracts, and overtime. Therefore, management and employees will need to be aware of this policy and agree to it in advance. Other considerations are that mobile device users have support needs that go well beyond that of the normal desktop users. This will result in companies investigating a number of questions as they prepare to incorporate mobile devices by determining if the company will fully support the mobile user's devices, or provide just a secure connection. If the company elects to provide support it will have to determine which issues will be addressed by the organization's help desk, and if any investments must be made to train the help desk staff so that issues can be resolved. There will need to be a policies as to when support questions should be referred to the device manufacturers, carriers, application vendors or other third parties. Depending on the policy set forth with support, this may result in the company requiring their employees to purchase a maintenance support contract and if so the company may or may not reimburse the cost to the employees. With so many different possibilities for incorporating mobile strategies , companies may wish to consult with an experienced business partner that has implemented a mobile strategy to offer their perspective. By having a knowledgeable business partner, who has experienced incorporating mobile devices they can help the company craft a plan that appropriately prioritizes which

services and capabilities that are needed in an efficient and logical sequence (Porter, 2007).

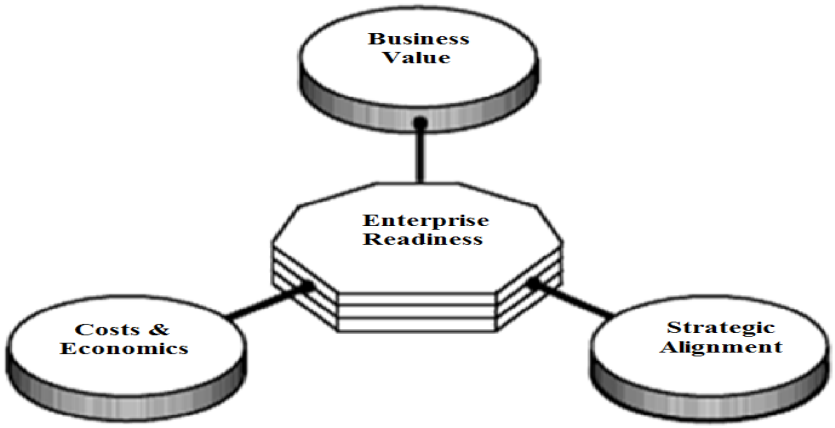


Figure 3. Planning approach with enterprise mobility projects. These factors can strengthen or weaken the core of a project. They must be considered because they build upon the notion of strategic planning requiring an understanding of the internal and external drivers necessary for successful adoption and implementation. From *Strategic Planning for Enterprise Mobility: A Readiness-Centric Approach* (p. 3), by R. C. Basole, 2004, Atlanta, GA: Tennenbaum Institute, Georgia Institute of Technology. Copyright 2004 by IFAC. Reprinted with permission.

Resource Planning

Effective use of theories such as defining the value of mobile devices within the enterprise, profiles of mobile enterprise users, mobile enablement, support work processes, and mobile resource-planning management, can facilitate planning and executing successful mobile IT projects for IT management teams. The theories should be analyzed to understand the internal factors associated with mobile-device projects. When considering technology-investment decisions, businesses must adopt a justifiable value for their return on investment (Ward, Bridges, & Chitty, 2005). This is particularly

important when considering emerging mobile devices because the business value of these devices has not been clearly identified (Ming-Shian, Sun-Jen, & Li-Wei, 2011). For most enterprises, mobility solutions are offering several intriguing value propositions such as access to corporate information systems anywhere and anytime, which is clearly a key driver to the adoption of a mobile-device strategy (Alkazemi, 2012).

Employees working remotely are no longer tied to desktop computers for checking task status or receiving substantial information. Mobile devices allow employees to receive timely information leading to timely decisions. This can, in turn, lead to cost savings and profits for the enterprise. Another benefit is replacing the cost of expensive computer equipment with less expensive and smaller, portable handheld devices. Furthermore, by replacing outdated current processes with new, faster mobilized processes, the potential for error in transferring information from older manual processes is reduced. Thus, a higher degree of data accuracy and reliability is gained, which in turn, increases business intelligence (Fonner & Roloff, 2010).

One of the advantages of mobile processing is the ability to collect data in real time and transfer it back to the office system, thereby improving many processes such as order processing and advance shipping notification to customers. These benefits can also be realized in many other areas by lowering inventory that carry overhead costs and improving efficiency with the routing of deliveries with multiple drop points. These advantages are multipurpose and generally improved customer satisfaction leading to overall business-process improvement. The instant access to corporate information system allows employees to naturally progress to a higher level of productivity. Mobile

workers are able to view data instantly that allows them to respond and execute their processes faster within continuously changing market conditions. Mobile devices allow companies the ability to provide greater insight and visibility through resources and assets, thereby creating a mechanized enterprise (Nevo & Wade, 2010). Organizations can create and use these advantages to affect core proficiencies that will influence business models, strategies, and markets (Basole & Rouse, 2007).

As with most mobility-implementation projects, the associated economics are an important aspect for consideration. Both tangible and intangible benefits must be considered. Organizations planning on adopting mobile devices must not only consider these factors, but also justify the costs associated with successful implementation (Otim, Dow, Grover, & Wong, 2012). Depending upon the scope and scale of the mobile projects, additional resources may be needed, thereby leading to higher costs. A problem is underestimating the true costs of mobile-device adoption and implementation. Management often includes solely the costs associated with the installation and configuration of hardware and software; however, significant indirect costs must also be considered. These expenditures can arise with employee training that must be provided on the basic functions of the mobile devices once they are in place. This transformation can cause a temporary loss in productivity due to the lack of experience with mobile-device equipment and any resistance to the change (Sharples, 2000).

Organizational managers must also calculate the potential loss for not implementing new mobile technology. Those foregoing the adoption of mobile devices may soon realize severe consequences potentially adversely affecting business profits. As

competition continues to strengthen their competitive edge, these organizations may begin to lose loyal customers and find their supply chains becoming inefficient. Corporate images can be damaged when employees do not view the enterprise as a technological leader. Properly evaluating all the costs and benefits associated with mobile-device implementation can lead to successful adoption so cannot be ignored as part of the overall strategic business-planning process (Tripathi, 2012). This process must be designed to obtain *buy-in* from management during the enterprise mobility-solutions initiative. Therefore, the careful assessment of the costs and benefits linked to several mobile models must be performed to determine the optimal investment (Teral, 2009).

Mobilizing the business workforce can present complex decision points with benefits, considerations, and challenges that can reach beyond mobility planning. Corporations typically only support devices they own so they can maintain control over the equipment and its use. These devices are only distributed to a select group of employees to manage support costs and maintain telecom expenses. Companies also maintain control over their owned mobile devices to minimize security risk and data loss through policy prohibiting unauthorized access to company computer systems and not allowing enterprise data to be stored on a personally own device. However, regardless of these policies, employees owning smartphones are making inroads into the company computer system (Lopez, 2010).

Integration and Related Policy

There are various reasons for employees desiring to use their personal mobile devices while at work. In some cases, employees who travel may have a corporate device

and personal mobile device. There are difficulties in maintaining two pieces of equipment, especially when one could be used to perform all needed functions. In other cases, employees may wish to access their mobile device for personal functions, but the corporation will not fund it. Therefore, they find other ways of gaining access that may be against corporate policy. Businesses are diligently attempting to secure computer systems by locking access to e-mail and other business applications; however, employees continue to find ways of breaching these measures, forcing management action. Measures can be put into place that either restrict the use of mobile devices, which necessitates policy related to security breaches, or that controls the use of mobile devices and allows employees to use their own devices (Cervone, 2010).

Businesses considering the enactment of policy related to mobile devices will need to define various criteria regarding who can access the enterprise network and the type of applications that can be accessed. Examples of such criteria are job title, function, and the number of hours employees work. However, businesses may create a policy that allows employee-owned devices to access only e-mail while corporate-owned devices are given access to all business applications. Typically it is within the purview of the IT department to select which applications can be accessed within the enterprise network. One of the problems the department can expect is that users will want to use other applications on their devices; hence, flexibility while maintaining a secure environment will be necessary. If the IT department embraces security solutions that limit the resources applications can access, and consider adding content filtering for mobile devices, this may be a viable solution. Once it is determined who can access the

enterprise network, and what applications can perform that access, the IT team can begin defining the process of user access and the use of business applications (Dearman & Pierce, 2008).

As users are defined, their mobile computing and communication will need support for the availability of services through wireless networks and mobile computing devices. This support is considered to be an extension of existing wireless services to make it possible to work at different locales while using mobile devices. The support will differ from user to user and activity to activity. Needs are based upon the process or context within which information is available or required by the user, and under which conditions an activity is to be performed. The conditions are influenced by the behavior of the users and the environment that constitutes the mobile workplace (Priestnall, 2009).

Therefore, it is important to understand the various categories and profiles of mobile users to successfully pursue a mobile-enterprise initiative. A critical step is to identify the enterprise functions and processes that are valuable and necessary to enterprise users. Earlier studies have shown that tasks and processes constrained by time and location tend to be prime candidates for mobilization. Previous mobile-enterprise solutions were simply revised applications of existing corporate data for use on mobile devices (Sejong, 2010). Current mobile-enterprise solutions consider the user, task, device, and context (Kauffman, Ting, & Heck, 2010). This leads to mobile-enterprise resource planning and is becoming important when enabling mobility due to the technological revolution.

Mobility relates to how businesses can provide an improved infrastructure

through mobile applications and services. While enterprise resource planning is an important step, the provision of services through mobile technologies is inevitable (see Figure 4). Coupled with other trends that are changing the enterprise applications landscape, resource-planning systems must support the mobile behavior of their users with the correct mobile-application landscape and an architecture model for mobile services with the necessary functionality to ensure the promotion and use of services (Tama, 2012).

Network Synchronization

The synchronization process maintains device alignment with business computer systems. The process uses the network to propagate any changes to files or folders between the destination and source computer systems. For synchronization to occur, the hard disk of a portable computer must be powered up so files can be copied from the network to the local cache, and files within the local cache can be copied to the network. The protocols for mobile-device synchronization must be carefully designed because the resources available for these devices are often constrained.

Mobile devices typically communicate over a low bandwidth or have limited memory and power resources because they are unable to quickly process or transfer large amounts of data (Cho, Kim, & Baek, 2011). However, this does not affect all mobile devices because, depending upon the application architecture, some devices are embedded with a process known as always available or occasionally connected, which allows synchronization throughout the day. These applications are capable of data storage so they can be synchronized once a network connection to the back-end system is

established. A key aspect of these business applications are that the information stored is not an isolated set of data, but data shared across many users. The data residing on each device is periodically synchronized with the enterprise system over wired or wireless networks (Charland & Leroux, 2011).

Summary and Conclusions

As mobile technology continues to evolve, IT managers are beginning to embrace the growing number of personal devices employees desire to use within the organization. However, they are overwhelmed with the idea of how to secure the associated risk to the corporate information system or support the devices. Managers of IT departments are finding they are unprepared for the rapidly growing use of this technology within the workplace, and a widening gap is evident between companies allowing personal mobility devices and those that refuse, as more organizations realize the trend is either unstoppable or inevitable (Ellis, Saret, & Weed, 2012). The literature review show gaps concerning personal mobile devices being allowed access to the corporate information system. Governance, risk assessment, roles, responsibilities and policies that have been previously established for IT environments are now identified as concerns with security and support as it relates to mobile devices. Additionally, the concentration by IT departments has been an emphasis on closed IT environments to control security and support and not an open system approach.

This study addresses several of these gaps by showing that corporations that are planning to allow mobile devices must consider if the company will fully security and support the devices as part of their methodology as indicated in chapter 3. By taking the

approach to understand the security and support needs, IT personnel will be better equipped to handle incident problems.

Chapter 3: Methodology

The purpose of the study was to examine the relationship between employees desire to use personal mobile devices and corporation's needs for security and support. I sought to determine whether the variables affected each other independently or collectively. A quantitative survey approach was used and convenience sampling was implemented with subsequent survey administration. Once the surveys was collected for data analysis, they were translated into numerical codes to facilitate statistical representation.

Research Design and Rationale

An effective study requires an appropriate research design. If chosen correctly based on the intent and procedures of the study, and the strengths and weaknesses associated with each method, will establish a body of knowledge in a specific subject area (Babbie, 2001).

Mixed methods was not considered because it involves extensive time and resources to collect, merge, and analyze both quantitative and qualitative data. Using a mixed methods approach would have complicated this study by requiring that the researcher be trained in quantitative, qualitative, and mixed methods approaches.

The qualitative method was excluded because of its tendency for studying small numbers of subjects and its labor-intensive and costly data collection methods (Creswell, 2003). This method is also criticized for being subject to researcher bias, for its lack of reproducibility and the lack of generalizability of its findings. Common data collection methods used in qualitative research is focus groups, triads, dyads, in-depth interviews,

and uninterrupted observation that draws out hidden explanations of social behavior to find the details of why and how in the phenomena being studied (Yin, 2003). While qualitative and mixed methodology may be suitable for other types of research , they involve extensive time in the field, effort, and cost

The quantitative method using a survey design was chosen for this study; the aim was to determine the relationship between the independent variables of support and security and dependent variable of personal mobile devices. Quantitative research uses strategies of inquiry when collecting data and yielding statistical analysis. The findings from a quantitative research can be both predictive and explanatory, confirming knowledge through cause and effect; specific variables, hypotheses, and research questions; measurement and observation; and theory testing (Creswell, 2003).

Careful consideration was given to the types of quantitative strategies, including descriptive, experimental, and survey. A descriptive strategy was not chosen because its primary concerns are with describing events and instrumentation that require many years to perfect for accuracy and reliability (Glass & Hopkins, 1984). Within experimental research the conditions are manipulated for the purpose of determining what the effects are on certain types of behavior without the knowledge of the participants. This type of study normally consists of two groups, a control group and experimental group. These groups are kept unaware of their participation so to keep their actions as normal as possible. This type of study can have different designs depending on the number of variables being investigated. This type was also not accepted because it requires control over participants in various groups that is not practical for this study. Quasi-experimental

is another type of study that also includes multiple groups that are assigned for evaluation by nonrandomized standards; it is commonly used in medical studies. Quasi-experimental is sometimes called the pre-post intervention and it is often used to evaluate the benefits of a specific type of intervention. Common designs of this method are the comparison design with groups before and after the tests are completed. However, the main focus of the design is that the subjects cannot be randomly assigned to any particular group and the researcher cannot control which group will get what treatment. This type was also rejected from the study because its use with multiple groups in a medical setting.

Nonexpermimental research is used in various categories, single-variable research, correlational, and qualitative research. This type of research focuses on the statistical relationship between variables but does not introduce the manipulation of an independent variable, or random assignment of participants. This research is used in relationship with qualitative research were the researcher measures the variables of interest with no attempt to control extraneous variables or the relationship between them. The conclusion was to use nonexpermimental with a survey to obtain information from a predefined population to collect data on phenomena that cannot be directly observed. As noted by Basha and Harter (1980), a population is any set of persons or objects that possesses at least one common characteristic. With non experimental the survey relationships can be established between the independent variables and dependent variable.

I tested the following hypotheses:

H_{01}*:* There is no relationship between the use of personal mobile devices and

corporate support.

H_{A1}: There is a relationship between the use of personal mobile devices and corporate support.

H_{02}:There is no relationship between the use of personal mobile devices and corporate security.

H_{A2}: There is a relationship between the use of personal mobile devices and corporate security.

The goal of the study was to determine (a) whether a relationship exists between the success of allowing access of personal mobile devices and the success of security, and (b) whether a relationship exists between the success of allowing access of personal mobile devices and the success of support. The dependent variable in the study was personal mobile devices; the independent variables were identified as security and support.

In quantitative research, the aim is to determine the relationship between independent and dependent variables. As stated by Trochim and Donnelly (2007), "A variable is an entity that can take on different values based on the situation, circumstances, treatment, or other reasons" (p. 35). The independent variable can be manipulated, and the dependent variable is affected by the independent variable. Researchers attempt to predict the dependent variable, and any variable used to make those predictions is an independent variable. The independent variables in the study are security and support. The dependent variable is personal mobile devices interfaced into an existing IT system (see Figure 2).

The study was conducted to establish the relationship between independent and dependent variables. Quantitative research was appropriate for the study because the researcher was seeking to establish a relationship between the variables (Trochim & Donnelly, 2007). This also enables statistical interpretation of the results and allows measurement of the direction of movement or the relationship. The independent variable can be manipulated by a treatment, program, or cause. Security objectives includes confidentiality, where only authorized users can transmit and store business data, the next is integrity, having the ability to detect unauthorized attempts to infiltrate the IT system, and finally the availability, by ensuring that users have access to the corporate information system as needed through secure access. Support criteria includes standards for the operating functionality and applications modules on the mobile device. This also encompasses supporting account creation with password activation, and limited hardware support to ensure the device is operational.

IT personnel were asked to answer the prepared survey questions. This method of data collection is both cost and time effective. The Pearson product-moment coefficient correlation was applied to the data collected to determine whether either a positive or negative relationship exists between the variables. This calculation determined whether an increase in the value of one variable can affect other variables and enable a measure of the strength and direction of the linear relationships between the quantitative variables. This is accomplished by assigning the coefficient to vary between -1 and + 1, with the positive or negative symbol indicating the direction of the relationship. Once a value is determined, the coefficient will indicate the strength of the relationship. Additional

calculations was included as deemed appropriate or necessary.

Research Methodology

The success of allowing personal mobile devices to connect to existing computer systems depends upon internal factors such as support, security, bandwidth, memory, and resources (Cho, Kim, & Baek, 2011). According to the literature review conducted for the study, limited understanding exists among IT personnel of internal factors contributing to implementation success. In addition to management, individual, and organizational factors, other internal factors such as workflow, knowledge management, transaction processing, security, support, and reporting can also affect the success of this type of integration (Viscusi, 2006). Wagner (2005) stated that

> The success of mobile implementation will ultimately revolve around a mosaic of rich converged experiences. These experiences will rest, in turn, on a foundation of converged network and device technologies, wireless services, rights management, content management, search management, and transactional processing power. (p. 52)

Contributing factors challenging IT organizations considering the introduction of personal mobile devices and their connectivity to the corporate information computer system is the delivery of a secure remote network access. This is while concurrently limiting other resource access based upon authentication, authorization, and user identity. Essentially, businesses planning to allow personal mobile devices must consider the security and support of the devices carefully via analysis by their IT teams (Jun-Sub, & Jin, 2012).

As the dynamics of business requirements increase, the need for faster response from personnel and greater flexibility of the technology upon which they rely increase proportionately. To meet these challenges, businesses have realized that, by incorporating mobile devices, they can offer an excellent solution with both functionality and popularity by enabling remote data accessibility. However, personnel now prefer their own mobile devices for its ease of use and so they can maintain control of both personal and business tasks. As Internet deployment steadily increases, coupled with advances in wireless communication, a greater number of business opportunities are emerging with a prevailing mobile workforce. The downside to the associated improved productivity, is that the mobile devices may remove control of the technology from the centralized IT support infrastructure, thereby increasing the challenges of systems management, risk management, and maintaining configuration and compliance initiatives (Tarasewich, 2008).

The study collected data via a survey for working IT professionals experienced in IT support, security, and connectivity. For a representative sample, an adequate sample size must be recruited that also accounts for non-response bias. Holton and Burnett (2005) stated, "One of the real advantages of quantitative methods is their ability to use smaller groups of people to make inferences about larger groups that would be prohibitively expensive to study" (p. 71). There are formulas that have been created to calculate an adequate sample size that includes the level of risk, standard deviation, and acceptable margin of error. These formulas were incorporated to achieve a response rate that is suggested as appropriate for this type of study (Bartlett, Kotrlik, & Higgins, 2001).

To achieve the accepted response percentage, the survey to be used in the study was designed in a manner allowing easy access and cost effectiveness (Trochim & Donnelly, 2007). Additional consideration was given to the sampling to enable generalization of the findings. The instrument will present a prestablished set of questions with a Likert-type response scale from (1 *strongly disagree* to 5 *strongly agree*). The collected survey data was entered into a statistical software program for analysis (Aczel & Sounderpandian, 2009).

Population

One hundred and seventy IT professionals who are working in an IT group were considered for this research because this group works within areas associated with the study. Additionally, these individuals have expertise related to IT development, connectivity, security and support that can contribute to the development of valuable insight relevant to testing the hypotheses and answering the research questions. These members work in various locations and will receive an e-mail requesting their assistance with the research. A pilot study was carried out in which 5 members of the 170 were asked to participate; they were subsequently excluded from the general study. The remaining 165 were sent an email requesting their participation by completing the survey.

Sampling and Sampling Procedure

The setting for the study was an international company located in the south-eastern part of the United States. The study sample consisted of IT professionals working within the IT department for the company. The sampling technique for the study was convenience sampling. This type of sampling is based upon a nonprobability method to

save time and help keep cost to a minimum. The target sample is a single IT group of 165 members working for the company. Determining an adequate sample size is a foundational aspect of all research and, if performed incorrectly will yield invalid and unreliable data. It is the responsibility of the researcher to calculate the appropriate number of responses needed for the study that will accurately represent a cross section of the target population. Therefore, to gain validity with an accuracy of +/-10% for the survey questions, the appropriate number of responses the researcher will need a minimum of 107 participants to return the survey out of the total 165 population, this will give a 65% rate, (165 x .65 = 107). In an effort to gain the expected number of responses additional reminder e-mails were sent out to the participants to achieve the required number of responses needed.

Recruitment and Participants

To ensure participation and maintain confidentiality, a consent form was distributed via e-mail to each potential study participant (see Appendix C). This form advised that participation in the research was strictly voluntary and that completion of the survey was considered consent to participate in the study. The consent form clearly outline the purpose of the study and the information gathered. The participants were further advised that their identities will not be disclosed because this information is not captured within the survey. Dresser (1998) stated that "the administrative burden of ethical reviews and procedures is balanced by the protection of participants" (p. 23). The survey and consent form also adhered to the standards set forth by the Institutional Review Board.

Data Collection

For convenience, data collection was via a survey circulated to IT professionals experienced in IT support, security, and connectivity. In order to gain a representative sample, an adequate sample size must be recruited that also accounts for non-response bias. Holton and Burnett (2005) stated, "One of the real advantages of quantitative methods is their ability to use smaller groups of people to make inferences about larger groups that would be prohibitively expensive to study" (p. 71). Formulas have been created to calculate an adequate sample size that includes the level of risk, standard deviation, and acceptable margin of error. These formulas were incorporated to achieve a response rate that is suggested as appropriate for this type of study (Bartlett, Kotrlik, & Higgins, 2001).

Therefore, to achieve the accepted response percentage, the survey to be used in this study was designed in a manner allowing easy access and cost effectiveness (Trochim & Donnelly, 2007). Additional consideration was given to the sampling to enable generalization of the findings. The survey included a established set of questions with a Likert-type response scale from 1 to 5, with 1 equating to *strongly disagree* and 5 to *strongly agree.* The collected survey data was entered into statistical computer software for analysis (Aczel & Sounderpandian, 2009). One hundred seventy IT professionals with expertise relating to IT development and connectivity was requested to complete the survey. There was a pilot study of 5 participants that was selected from the170 members that was excluded from the research study. The remaining 165-member population was sent additional e-mails requesting their support by completing the

survey.

Pilot Study

A pilot study was performed with a subgroup of participants within the study site organization to help validate the survey and survey instructions. The information collected from this subgroup was used to determine if the instructions and questions are clear and easy to understand or if the questions need to be changed by adding, deleting or restating the questions. The primary strengths of this pilot study was that it enabled critical thinking that will lead to a better understanding of the data collection survey (Paul & Elder, 2001). Yin (2003) covered pilot tests in qualitative case studies. He noted that "the pilot case study will help you to refine your data collection plans with respect to both the content of the data and the procedures to be followed" (pp.78–79). Seidman (2006) agreed as he noted "I urge all interviewing researchers to build into their proposal a pilot venture in which the try out their interviewing design with a small number of participants" (p. 39).

A good heuristic is that if a researcher is using a survey that he or she developed for either qualitative or quantitative studies, then a pilot study should be used to help validate the instrument. Additional questions can be asked of the participants to address Seidman's ideas on both content and procedures such as the following.

1. Are the instructions clear and easy to understand?
2. If not, what should be changed?
3. Are the questions clear and easy to understand?
4. If not, what should be changed?

5. Do the questions cover the topic?
6. If not, what questions should be asked? Should any be changed or deleted?

These are simple critical thinking questions derived from Paul and Elder's (2001) framework on critical thinking standards. This sort of questioning leads to a better overall study as the researcher learns more about the instrument and the procedures that would be known otherwise. This also permits any corrective action to be taken before the actual study.

Researcher Instrument

Designing and implementing a survey is a systematic process of gathering information on a specific topic by asking questions of individuals for generalization of the results to other groups represented by the participants (Baxter & Babbie, 2004). The survey was administered by a Web-based company (see Appendix B). This enables the participants easy access to the survey with one hyperlink that was included as a link on the emails. The use of such Web-based solutions has been growing in popularity because it renders an administrate process that is particularly quick and cost-effective. The survey questions (see Appendix B) were based upon factors addressed within the literature reviewed for the study that affect the integration of personal mobile devices into an existing computer environment.

There are drawbacks to using a Web-based solution for the survey process of the study because of potential computer problems, hostile attitudes toward emails, and the limitation of a sample comprised of solely those individual with Internet access. An online survey company was selected for its user-friendly and salient survey designs.

Participants are more likely to complete a survey if they perceive the questions as pertinent and time effective (Arapakis, Jose, & Gray, 2008).

Data Analysis

Contingency tables will clarify the various relationships between the hypotheses and the survey questions. Such tables are extensively used with statistics to analyze the relationships between two or more variables that are exclusive, do not overlap, and include all possibilities (Tarsitano & Falcone, 2011). They are also used to collect the data according to the studied variables, which enables the researcher to glean deeper insight into the relationships between the variables. Once approval is received from the Walden Institutional Review Board, a pilot study was conducted with the 5 chosen participants previously mention in the sample size section. Cooper and Schindler (2003) noted that it is best to use a panel of experts to evaluate the survey for conceptual clarity by pretesting in a pilot study to ensure that the questions are clear and precise.

As previously stated descriptive and inferential statistics are the two methodologies selected to test the hypotheses. These statistical methodologies was aided by SPSS 19.0 software, and used together to address the entire analytical process during the data analysis phase. This software used the data collected from the survey with the variables to complete the analysis toward determining the existence of relationships and facilitate in the creation of graphs and charts to present the findings in an understandable manner. A survey code table (see Appendix D) was created to assign values to the survey question responses to help with the data analysis. This table simplified data entry and was used with the statistical software package to examine relationships.

Coding is the process of assigning numeric values to responses collected from the completed questionnaires. There was also a wide range of analyses and procedures conducted including descriptive statistics, crosstabs, differences of means, linear regression, factor analyses, and survival analyses. The data analysis was conducted to determine whether any relationships exist between the variables of the study and to what degree (Neuman, 2006). Once this determination was made, it did not necessarily mean that one variable causes another to fluctuate (Simon & Francis, 2006) because the affects can be caused from both positive and negative coefficients by increases or decreases to the variables. Zero is the only indicator that will reflect no relationship between the variables.

In an effort to measure the variables through correlational, I designed the survey to include three sections that targeted each one of the variables. Once the data was collected a survey code table (see Appendix D) was used to assign values to the survey question responses to help with the data analysis. This table simplified data entry and was used with the statistical software package to determine relationships. As previously mentioned a Likert scale was used for statistical analysis to help generate original data. Sub-variables (see Figure 2) were merged into the survey for each set of the main variables thereby creating weighed indexes. These indexes yielded an accumulation of scores from the survey thereby giving validity to the variables.

Chi Square

The chi square test is to compare what is observed and what is expected by change. The chi-square methodology was used to compare each of the hypothesis to see

if there are any relationships between the variables. The chi-square methodology tests for independence when there are variables from a single population and it is used to determine whether there is a significant association between the variables. One description of the chi-square approach consists of four steps: (a) state the hypotheses, (b) formulate an analysis plan, (c) analyze sample data, and (d) interpret results (Byrne, Shavelson, & Muthén, 1989).

Pearson Product Moment Correlation

Once completed the analysis showed interval level of measurement thereby giving way to the Pearson product-moment coefficient of correlation. This coefficient of correlation can determine whether an increase in the value of one variable leads to an increase or decrease in the other variable or if a decrease in the value of one variable leads to a decrease or increase in the value of the other variable. Pearson correlation also enables a researcher to measure the strength and direction of linear relationships between variables. This is determined as the value or coefficient varies between -1 and + 1. Additionally, the negative and positive sign can indicate the direction of the relationship. The absolute value or magnitude of the coefficient indicates the strength of the relationship. The stronger the association the closer the Pearson correlation coefficient will be depending on whether the relationship is positive or negative. This technique was used to compute a correlation between the random variables of support and security.

Reliability and Validity

Reliability is the extent to which an experiment or tests yields the same result on repeated bases. This holds true for the accurate representation of the total population

under study and the research instrument, that if the results of a study can be reproduced under a similar methodology, then the research is considered to be reliable (Golafshani, 2003). Reliability is a means of assessing the quality of the measurement procedure used to collect data in a study. In order for the results from a study to be considered valid, the measurement procedure must first be reliable. In order to provide reliability for the research survey and survey instructions, a pilot study was performed with a subgroup of participants within the study site organization. The primary strengths of a pilot study is that it enables critical thinking that will lead to a better understanding of the data collection survey (Paul & Elder, 2001). A pilot study can reveal deficiencies in the design of a proposed experiment or procedure and these can then be addressed before time and resources are expended on large scale studies.

External Validity

In order to minimize bias that is inherited in research, a researcher will take proactive steps to ensure that key elements are aligned with similar studies. This will allow validity to provide legitimacy to the research. Integrity equals validity; therefore, every effort to maintain this status was taken while constructing the survey questions for this study. Furthermore, the literature review and pilot study are being used to validate the survey. In order to maintain the external validity for this study only one group from the organization were selected to participate in the study (Leedy & Ormrod, 2005).

The threat to external validity is a clarification of how the researcher might be wrong in making any generalization concerning the participants, places and times used during the study. Additionally, other reviewers may show that the results of the study

were simply due to these three major factors and had the research been performed with different participants, at a different place or a different time, the results would not have been the same. This is why the researcher must consider these threats and take precautions to minimize any potential biases that threaten the validity of the study. However, not all biases can be eliminated; therefore, the researcher needs to acknowledge their presence within the study and state what impact they may have on the results (Gerhard, 2008).

Internal Validity

Internal validity is about the validity of results within or internal to a study and is normally relevant in cause–effect studies when a researcher is trying to link a cause with an effect. It is not relevant in observation or descriptive studies that are merely report findings (Trochim & Donnelly, 2007). Internal validity is not threatened in this study because the scope is to determine if there is any correlational relationships between the independent variables of support and security and dependent variable of personal mobile devices within an existing IT environment.

Ethical Procedures

Several ethical steps were taken to protect the participants for this study. First, the data collection plan for this study was reviewed and approved by the Walden University Institutional Review Board (IRB; approval # 08-27-13-0059325). Once received, the approval number was included on all correspondence and forms. I e-mailed an introduction to establish my credentials and stated the grounds for the research. I then e-mailed a consent form that informed the participants that involvement in this study was

strictly on a volunteer basis and that any information provided would be kept confidential and anonymous.

Summary

The research methodology and data collection and analysis procedures for this study were presented. Several types of procedures were described such as those to be implemented with data collection, data analysis, and the supporting computer software. The protection of participant rights was explained. Participants were drawn from the study-site organization and the sample consisted of IT professionals with an in-depth knowledge of the research topic.

Chapter 4: Results

The purpose of this quantitative survey study was to examine the relationship between employees desire to use personal mobile devices and a corporation's needs for security and support. Companies are recognizing the advantages of mobile devices to the overall welfare of their enterprises; however, they are struggling with the uncertainty of supporting and securing these devices if they are personally owned. Businesses must begin planning strategies for incorporating standard solutions to the support and deployment of organizational mobilization that will control the cost of these business objectives with successful models. As technology advances continue, mobile-device capabilities increase proportionately. No longer are these devices limited to voice and e-mail components. Current devices present a full range of applications and services including video and voice with data speed that equals or surpasses the desktop computer. This equates to little distinction between the functionality of the desktop computer and mobile devices (Nah, Siau, & Sheng, 2005).

Today, companies are addressing employees' use of their personal mobile devices to connect to corporate computer systems with and without approval (Signorini & Hochmuth, 2010). Researchers have noted how mobile devices are transforming the workplace into a transparent landscape. Mobile devices are limiting reliance on physical location and increasing business productivity. Workers increasingly rely upon mobile devices to research their competition products and conduct business transactions across mobile networks (Swaroop, Kumar, & Shanker, 2011). However, IT personnel have limited understanding of the factors that would make connecting personal mobile devices

with the appropriate support and security to the corporate information computer systems a success. Support is characterized by procedures to maintain the functionality of the mobile device and corporate enterprise system, while security is ensuring physical, regulatory compliance to guard against unauthorized access to the communications network. Thus, the research question for this study was as follows: Does security and support affect the successful integration of personal mobile devices, given that a company approves the use of the personal mobile devices?

The problem was the lack of research on the roles that security and support play when using personal mobile devices to access corporate information systems. There are numerous types of security and support that have to be addressed before the implementation of personal mobile devices. The two main types of security is network and information security. Network security involves methods used to protect the total computer network from unauthorized accesses. Information security is concerned with network security as well as cryptography, access control, physical security, and data. Both have to be considered because mobile device users trust that their devices will have the capability to keep confidential information truly confidential, thereby limiting access to only the authorized user. There are several types of support including remote, live chat, hardware and software repair and a variety of different technical support options available. This is why selecting the correct mobility strategy is so important and must be designed with consideration to the business as a whole, rather than merely a reaction to the latest trend or popular device.

In this study, I gathered information from various employees who are used to

working on IT projects and who have expertise in IT development, connectivity, security and support. The conclusions drawn from the statistical data supported the research question presented in Chapter 1: Does security and support affect the successful integration of personal mobile devices? Basic linear regression analyses (see Table 10) found a highly significant relationship between personal mobile use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score also found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. These tests supported the hypotheses that there are relationships between the use of personal mobile devices and support and security.

Pilot Study

Prior to the full study, a pilot study using the same survey questions was completed to ensure that the survey was clear, comprehensive, and easy to use. Five participants were chosen to participate in the pilot study because of (a) their expertise in the field of IT and (b) the research topic. They were asked (a) whether the purpose of the study was clear, whether the survey questions would provide the required information , whether any of the questions needed to be changed or deleted, and whether the order of the questions was understandable (see Appendix B). The results of the pilot study indicated that the survey did not need to be revised. By using a pilot study the responses yielded similar themes that support the design of the survey. The primary strengths of this pilot study was that it enabled critical thinking that will lead to a better understanding of

the data collection survey (Paul & Elder, 2001). Yin (2003) covered pilot tests in qualitative case studies. He noted that "the pilot case study will help you to refine your data collection plans with respect to both the content of the data and the procedures to be followed" (pp.78–79). Seidman (2006) agreed as he noted "I urge all interviewing researchers to build into their proposal a pilot venture in which to try out their interviewing design with a small number of participants" (p. 39).

Data Collection

The participants invited to complete the online survey were managers, team leads, project managers, support personnel, and individual contributors in IT departments for a private international company in the southeastern portion of the United States. These candidates were chosen are from a subset of employees and received an e-mail requesting their participation . These participants worked in IT software engineering or project management and were considered subject matter experts. They are used to working in a team environment because of the complexity of their work and the large amount of information they have to process on a daily basis to complete their assignments. They also have a need to share information constantly in a fast-paced environment. The target sample was a single IT group of 165 members. Determining an adequate sample size is a foundational aspect of all research and, if performed incorrectly will yield invalid and unreliable data. It is the responsibility of the researcher to calculate the appropriate number of responses needed for the study that will accurately represent a cross section of the target population. Therefore, to gain validity with an accuracy of +/-10% for the survey questions, the appropriate number of responses I needed was a minimum of 107

participants to return the survey out of the total 165 population, this will give a 65% rate, (165 x .65 = 107). In an effort to gain the expected number of responses additional reminder e-mails were sent out to the participants to achieve the required number of responses needed.

The survey was made up of 22 questions, with a Likert-type response scale from (1 *strongly disagree* to 5 *strongly agree*). These questions were meant to encourage responses from the participants and were designed to obtain answers based on the participants' knowledge and experience. Each participant was sent an introductory e-mail, which contained a link to the online survey. A survey with pre-established questions is ideal for the data-collection process in a study (Neuman, 2006). The online survey was left open for access for 3 weeks, with additional e-mails being sent out requesting participation.

One hundred sixty-five participants received an invitation email with an introduction to establish identification and state the grounds for the research. Additionally, attached to the emails was a consent form that informed the participants that their involvement in the study was strictly on a voluntary basis and that any information provided would be kept confidential and anonymous. Furthermore, financial incentives were included in the consent form stating, "As compensation for your participation in this study a $5 Starbucks card will be given to the participants who complete the survey and email the researcher indicating same." The response rate for the online survey was 65% with a total of 108 participants responding out of the 165 emails sent out.

There were five questions relating to demographics in the study. These questions concerned age, gender, education, job role, and years of IT experience. The questions were created to segment the audiences and discover any trends based on the main topic of the survey. The first demographic showing the age category (see Table 1), indicates that 108 participants reported their ages, ranging from 18-20 to 50-59. The mean reported age was 35.25 years with a standard deviation of 9.5 years. The second table shows gender (see Table 2) with a total of 107 participants reporting their genders, with one missing response. The participant pool included 81.3% men and 18.7% women. Table 3 illustrates the highest level of educational attainment, 108 participants reported their highest level of educational achievement with the vast majority of participants completing their bachelor's degree, but not their master's degree. The remaining participants, most (13.9% overall) had completed their associate's degree. The remaining 3.7% had earned master's degrees. All 108 participants reported their job role (see Table 4). The vast majority (91.7%) reported being individual contributors. The remaining 5.6% are team leaders, while 1.9% being managers, and the one remaining participant (0.9% overall) is a senior manager. The final table reports the number of years of IT experience the participants have (see Table 5). This table indicates that 108 participants reported their IT experience ranging from 1-25. The mean reports the number of years was 2.4 with a standard deviation of 1.1.

Table 1

Age of Participants

Age	Frequency	Percent

18-20	1	0.90
21-29	33	30.60
30-39	42	38.90
40-49	23	21.30
50-59	9	8.30
Total	108	100.00

Table 2

Gender

Gender	Frequency	Percent
Men	87	81.30
Women	20	18.70
Total	107	100.00

Table 3

Educational levels

Education	Frequency	Percent
Associates	15	13.90
Bachelors	89	82.40
Masters	4	3.70
Total	108	100

Table 4

Job Role

Job Role	Frequency	Percent
Individual Contributor	99	91.70
Team Lead	6	5.60
Manager	2	1.90
Senior Manager	1	0.90
Total	108	100

Table 5

Years of IT Experience

Years	Frequency	Percent
1-5	26	24.1
6-10	41	38.0
11-15	25	23.1
16-20	9	8.3
21-25	7	6.5
Total	108	100.00

Study Results

As previously stated, the survey questions were developed and administered using the Survey Monkey website. The data were collected using the same website. Each participant was informed about the purpose of the study as described in the Consent Form (see Appendix C). There were two phases for collecting the research data; the first phase concerned the pilot study. Five participants who were experts in the IT field were asked to participate in the pilot study. These participants received the consent letter and the web link used on Survey Monkey web site. The pilot group provided feedback concerning, clarity of questions, the timing and additional comments. Based on the group's feedback, the determination was made that the survey was satisfactory and ready to present.

In the second phase, the survey was sent as a link to the target sample. The participants were asked to complete the 22 multiple choice questions that were used in the pilot study, and were advised that there were no time limits and participation was strictly voluntary. The Survey Monkey web site was chosen because it is designed for researchers and has the capabilities for secure data collections. This web site allows easy

download of the collected data and allow for various data analysis. Once the allotted time period had expired for the survey, all responses were downloaded to my computer that is password and encryption protected. Overall a total of 113 participants took part in the online interview with no missing responses. There were five participants for the pilot group and 108 for the actual study.

At the conclusion of the data collections period, the results concerning support and security factors were placed into categories and measured on a 5-point Likert scale from (1 *strongly disagree* to 5 *strongly agree*). This technique allows each category to be organized by the hypothesis. Organizing the findings by hypothesis provides an understanding of the data collected (Leedy & Ormrod, 2005). There are two types of statistics, descriptive and inferential, and these can provide the results necessary to determine the findings and make conclusions related to the dependent and independent variables. As stated by Creswell (2005), descriptive statistics "present information that helps a researcher describe responses to each question in a database as well as determine overall trends and the distribution of the data" (p. 591). Descriptive statistics will allow the researcher to describe the basic features of the data. This gives the researcher the ability to effectively analyze the quantitative data; and give summaries in a graphical representation. Descriptive statistic analysis can be used to depict and describe results in a measurable format.

Summary of Hypothesis 1

H_{01}: There is no relationship between the use of personal mobile devices and corporate support.

H_{A1}: There is a relationship between the use of personal mobile devices and corporate support.

To test these hypotheses, the study compared the survey questions with the independent variable support and dependent variable personal mobile devices. The relationship was to determine if the participants owned a mobile device, for how long and determine how often the mobile device was used. One hundred and eight participants reported owning a mobile phone. The length of time the participants had owned their mobile devices ranged from 1-5 years to 21-25 years. The mean reported time having own mobile devices was 7.91 years with a standard deviation of 3.9 years (see Table 6) with a mobile use means (see Table 7) of 3.97 with a standard deviation of 0.5.

Continuation of testing the hypothesis to determine if there were any relationships was accomplished using several of the responses to the survey questions. The dependent variable personal mobile device and independent variable support was analyzed against 5 of the survey questions with the responses. The mean corporate support score of the 108 participants was 4.26 with a standard deviation of 0.43 (see Table 8). As Table 8 indicates, 78 (72.2%) of participants reported that if mobile devices are allowed to have access to corporate information systems, the company would have to provide support for the process to be successful.

Summary of Hypothesis 2

Hypothesis 2:

H_{02}: There is no relationship between the use of personal mobile devices and corporate security.

H_{A2}: There is a relationship between the use of personal mobile devices and corporate security.

To test these hypotheses, I correlated the survey questions with the independent variable security and dependent variable personal mobile devices. The correlation was to determine if the participants owned a mobile device, for how long and determine how often the mobile device was used. 108 participants reported owning a mobile phone. The length of time the participants had owned their mobile devices ranged from 1-5 years to 21-25 years. The mean reported time having own mobile devices was 7.91 years with a standard deviation of 3.9 years (see Table 6) with a mobile use means (see Table 7) of 3.97 with a standard deviation of 0.5.

Continuation of testing the hypothesis to determine if there were any relationships was accomplished using several of the responses to the survey questions. The dependent variable personal mobile device and independent variable security was analyzed against 5 of the survey questions with the responses. The mean Corporate Security score of the 108 participants was 4.10 with a standard deviation of 0.36 (see Table 9). As Table 9 indicates, 80 (74.07%) of participants reported that if mobile devices are allowed there will have to have access to corporate information systems, the company would have to provide security for the process to be successful.

Table 6

Years of Mobile-Phone Ownership

Mobile Ownership	Frequency	Percent
1-5	30	27.80
6-10	53	49.10

11-15	23	21.30
16-20	1	0.90
21-25	1	0.90
Total	108	100

Table 7

Mobile Use Score

Use Score	Frequency	Percent
3.00-3.24	0	0.00
3.25-3.49	6	5.56
3.50-3.74	42	38.89
3.75-3.99	19	17.59
4.00-4.24	17	15.74
4.25-4.49	0	0.00
4.50-4.74	5	4.63
4.75-5.00	19	17.59
Total	108	100.00

Table 8

Corporate Support

Corporate Support	Frequency	Percent
4.0	78	72.2
4.5	4	3.7
5.0	26	24.1
Total	108	100.0

Table 9

Corporate Security

Corporate Security	Frequency	Percent
2.50-2.99	1	0.93
3.00-3.49	3	2.78
3.50-3.99	4	3.70

4.00-4.49	80	74.07
4.50-5.00	20	18.52
Total	108	100.00

Summary of Results. Basic linear regression analyses (see Table 10) were conducted to investigate relationship between personal mobile use score and the dependent variables corporate support & corporate security. Each test found a highly significant relationship between personal mobile use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. This finding was also significant at $p < 0.001$. Each test found a highly significant relationship between personal mobile Use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. This finding was also significant at $p < 0.001$. Linear regression analyses assume that the residuals or error terms resulting from the best-fit line are normally distributed. As illustrated in Figure 5 and 6 shows the observed residuals compared with the expected residuals.

To further illustrate the correlation between the dependent and independent variables chi-square tests were conducted. The methodology is used against each of the

hypothesis to see if there are any relationships between the variables and tests for independence when there are variables from a single population and it is used to determine whether there is a significant association between the variables. The first chi-square test (see Table 11) indicates that there is a relationship between the variable personal mobile devices and corporate support. 72.2% of the participants answered there should be corporate support given when incorporating personal mobile devices. Additionally, the same chi-square was produced (see Table 12) for security and Hypothesis 2 with similar results. 71.3% of the participants answered there should be corporate security given when incorporating personal mobile devices.

Table 10

Standardize Regression Coefficients Score

Relationship		Beta	t	p	95% Confidence Interval	
Personal Mobile Use	Corporate Support	0.905	21.9	< 0.001	0.706	0.846
Personal Mobile Use	Corporate Security	0.655	8.9	< 0.001	0.366	0.575

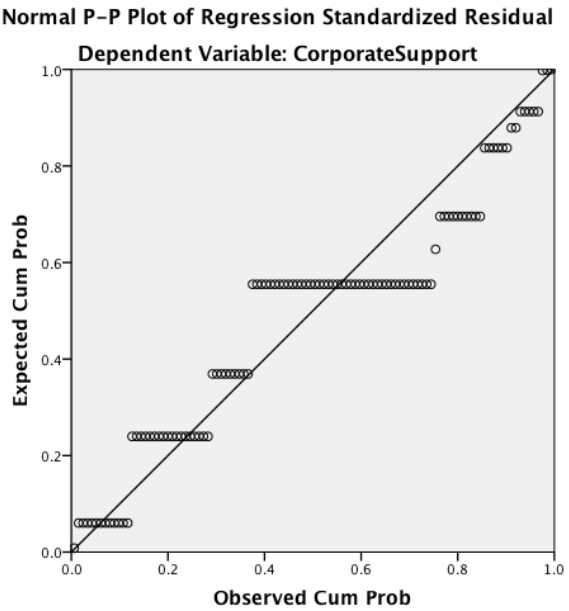


Figure 5. P-P Plot for personal mobile use score vs corporate support score.

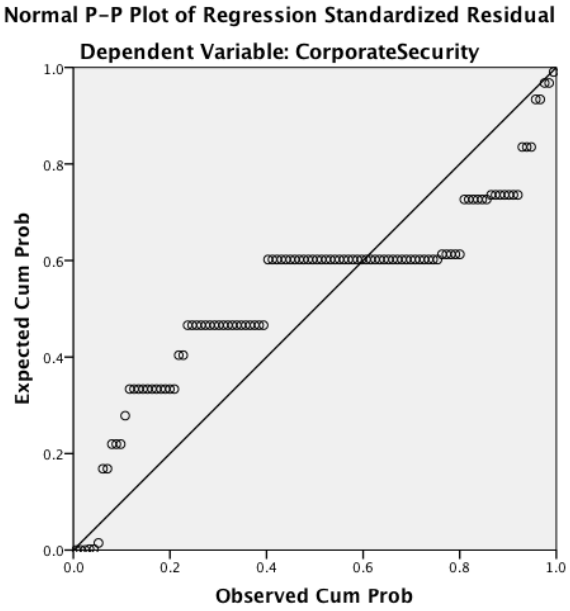


Figure 6. P-P Plot for personal mobile use score vs corporate security score.

Table 11

Chi-square support

Personal Mobile Use			Corporate Support			Total
			4.0	4.5	5.0	
	3.4	Count	6	0	0	6
		Expected Count	4.3	.2	1.4	6.0
		% within Personal Mobile Use	100.0	0.0	0.0	100.0
	3.6	Count	41	1	0	42
		Expected Count	30.3	1.6	10.1	42.0
		% within Personal Mobile Use	97.6	2.4	0.0	100.0
	3.8	Count	18	0	1	19
		Expected Count	13.7	.7	4.6	19.0
		% within Personal Mobile Use	94.7	0.0	5.3	100.0
	4.0	Count	12	2	0	14
		Expected Count	10.1	.5	3.4	14.0
		% within Personal Mobile Use	85.7	14.3	0.0	100.0
	4.2	Count	1	1	1	3
		Expected Count	2.2	.1	.7	3.0
		% within Personal Mobile Use	33.3	33.3	33.3	100.0
	4.6	Count	0	0	5	5
		Expected Count	3.6	.2	1.2	5.0
		% within Personal Mobile Use	0.0	0.0	100.0	100.0
	4.8	Count	0	0	10	10
		Expected Count	7.2	.4	2.4	10.0
		% within Personal Mobile Use	0.0	0.0	100.0	100.0
	5.0	Count	0	0	9	9
		Expected Count	6.5	.3	2.2	9.0
		% within Personal Mobile Use	0.0	0.0	100.0	100.0
Total		Count	78	4	26	108
		Expected Count	78.0	4.0	26.0	108.0
		% within Personal Mobile Use	72.2	3.7	24.1	100.0

Table 12

Chi-square security

Personal Mobile Use		Corporate Security							
		2.7	3.4	3.7	4	4.3	4.7	5	Total
3.4	Count	0	0	0	6	0	0	0	6
	Expected Count	.1	.2	.2	4.3	.2	.9	.2	6.0
	% within Personal Mobile Use	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
3.6	Count	0	1	2	39	0	0	0	42
	Expected Count	.4	1.2	1.6	29.9	1.2	6.2	1.6	42.0
	% within Personal Mobile Use	0.0	2.4	4.8	92.9	0.0	0.0	0.0	100.0
3.8	Count	0	0	0	18	0	1	0	19
	Expected Count	.2	.5	.7	13.5	.5	2.8	.7	19.0
	% within Personal Mobile Use	0.0	0.0	0.0	94.7	0.0	5.3	0.0	100.0
4.0	Count	1	2	0	11	0	0	0	14
	Expected Count	.1	.4	.5	10.0	.4	2.1	.5	14.0
	% within Personal Mobile Use	7.1	14.3	0.0	78.6	0.0	0.0	0.0	100.0
4.2	Count	0	0	0	3	0	0	0	3
	Expected Count	.0	.1	.1	2.1	.1	.4	.1	3.0
	% within Personal Mobile Use	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
4.6	Count	0	0	0	0	2	3	0	5
	Expected Count	.0	.1	.2	3.6	.1	.7	.2	5.0
	% within Personal Mobile Use	0.0	0.0	0.0	0.0	40.0	60.0	0.0	100.0
4.8	Count	0	0	0	0	1	7	2	10

	Expected Count	.1	.3	.4	7.1	.3	1.5	.4	10.0
	% within Personal Mobile Use	0.0	0.0	0.0	0.0	10.0	70.0	20.0	100.0
5.0	Count	0	0	2	0	0	5	2	9
	Expected Count	.1	.3	.3	6.4	.3	1.3	.3	9.0
	% within Personal Mobile Use	0.0	0.0	22.2	0.0	0.0	55.6	22.2	100.0
	Count	1	3	4	77	3	16	4	108
	Expected Count	1.0	3.0	4.0	77.0	3.0	16.0	4.0	108.0
	% within Personal Mobile Use	.9	2.8	3.7	71.3	2.8	14.8	3.7	100.0

Summary

In this chapter, the results of a study designed to understand the effect on existing IT environments if mobile devices are allowed to interconnect as it relates to corporation's needs for security by ensuring regulatory compliance to guard against unauthorized access to a communications network and support procedures to maintain the operating functionality of the mobile device. The results of the analysis were organized according to the study's hypotheses statements, and were presented in tabular and narrative form. Results showed that corporate support and security has a positive effect on successful implementation of mobile devices. Each test found a highly significant relationship between personal mobile use score and the dependent variable. However, the correlation coefficient (0.905) indicates that these variables are highly related and the findings are significant at $p < 0.001$. This can be explained by the fact that the

participants work in the IT field and are very aware of the association between support and security. Chapter 5 includes the results, conclusions, and recommendations.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this quantitative study was to examine the relationship between employees desire to use personal mobile devices and a corporation's needs for security and support. Support was characterized by procedures to maintain the operating functionality of the mobile device, while security was ensuring physical regulatory compliance to guard against unauthorized access to a communications network. The approach was chosen to acquire the statistical data required to understand any relationship among the independent variables of support and security and the dependent variable of personal mobile devices (see Figure 2).

A significant number of employees are requesting to use their personal mobile devices to connect to company computer systems and companies must now address the issue (Signorini & Hochmuth, 2010). The problem is understanding what level does security and support issues relate to employees using their own personal mobile devices when accessing corporate information systems. Researchers have noted the importance of mobile devices with regard to transforming the workplace into a transparent landscape with less reliance on physical location and greater impact on productivity. Workers increasingly rely on mobile devices to research products and conduct transactions across mobile networks (Swaroop, Kumar, & Shanker, 2011). However, IT personnel have a limited understanding of the factors that contribute to successfully implementing the connection of personal mobile devices to a corporate computer system. Many factors can affect the success of this integration: management, individual, and organizational factors; internal factors such as personal data loss, privacy, device seizure and loss of use,

transaction processing, security, and support.

This study used a quantitative approach with survey design. Numerical data were collected the responses were analyzed using mathematical methods to determine the strength of the relationship between the variables. The quantitative method was optimum for accepting or rejecting the hypotheses and thus establishing the relationship between the dependent variable (personal mobile electronic devices within an existing IT environment) and the independent variables (support or security).

This type of research necessitates a clear understanding of the dependent and independent variables (Sukamolson, n.d.). The variables were determined through investigation of the relationship of security and support with implementation of personal mobile electronic devices within an existing computer environment. Selected participants were requested to complete an electronic survey. By using this type of survey with prestablished questions, it was ideal for the data collection process in this study. The data was collected and the values were determined, which in turn, facilitates.

Interpretation of the Findings

The literature review indicated a direct positive relationship between the confidence level of employees and their perception of their job performance while using mobile devices. However, there was a lack of data identifying the type devices used by the participants as personally-owned, nor were any conclusions reached about the ability of the participating companies to secure or support these devices. This quantitative study examined the relationship between employees desire to use personal mobile devices and a corporation’s needs for security and support.

Mobile-device technologies can uniquely contribute to the communications revolution by eliminating the need for physical, land-based connectivity between people, processes, and entities. Businesses that adopt a mobile, wireless connectivity solution may discover a significant effect on productivity, irrespective of the size and geographical location of the organization. This effect includes changes to the respective organizational structures both internal and external business processes by allowing these devices access to corporate information systems. The challenge is to institute a standard process and strategy that will allow the integration of new technology into existing systems that address current and future fiscal and technological constraints. A mobility strategy must be designed with consideration to the business as a whole, rather than merely a reaction to the latest trend or popular device. To remain competitive, companies need to have a mobile strategy and reiterate it often.

The greatest chance for success is to have the mobile strategy aligned with the IT technology goals, the usage patterns of the target audience, and the budget. The strategy will need a phased mobile roadmap, and leverage as much as possible any existing technology to maximize the budget, and extend any consistent experience in transformation. This strategy starts with defining the mobile goals for the company. Once this has been accomplished the company will have a better understanding of the target audience, budget and internal efforts. A synergy among users is a goal, with the primary focus on those actively using their mobile devices to increase business success. The strategy must meet the requirements of various types of mobile devices because there is no single technology or service plan that can be expected to meet the entire set of

enterprise-mobility requirements. As individuals within an organization begin to rely upon their mobile devices, they will have different communication needs, depending upon their work roles and responsibilities (Crumlish & Malone, 2009). One approach is to allow mobile devices to connect seamlessly into the operating-system model, while ensuring that security and support is maintained and protected (Peters & Allouch, 2005).

The conclusions drawn from the statistical data supported the research hypothesis presented in Chapter 1: Does security and support affect the successful integration of personal mobile devices? Basic linear regression analyses (see Table 10) found a highly significant relationship between personal mobile use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. This finding was also significant at $p < 0.001$. Each test found a highly significant relationship between personal mobile use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. This finding was also significant at $p < 0.001$. Linear regression analyses assume that the residuals or error terms resulting from the best-fit line are normally distributed.

Table 13 shows the findings that resulted from the testing of each hypothesis. Mobile device implementation can be called a success if it meets the security and support

objectives. The results showed that corporate support and security has an effect on successful implementation of mobile devices. Each test found a highly significant relationship between personal mobile use score and the dependent variable.

Table 13

Hypotheses Results

Hypotheses	Results
H_{01}: There is no relationship between the use of personal mobile devices and corporate support.	Rejected
H_{02}: There is no relationship between the use of personal mobile devices and corporate security.	Rejected
H_{A1}: There is a relationship between the use of personal mobile devices and corporate support.	Accepted
H_{A2}: There is a relationship between the use of personal mobile devices and corporate security.	Accepted

Limitations of the Study

All studies have limitations. They need to be identified and taken into account because (a) they can affect the quality of the research and (b) some could be seen as fruitful avenues for future research under the same theme. There were several limitations that existed in this study. The first limitation was with the lack of generalizability due to the number of participants. The sample size was 108 participants working for a company in the United States, which means that the size group was limited. Other limitations, such as prolonged engagement, observation, and debriefing could not be used because of the need for anonymity. Not having the ability to validate the answers and numeric data given by the participants was another limitation. Final limitation was the reliability and validity of the survey instrument because of biases that can threaten the study.

Recommendations

The purpose of this quantitative study was to examine the relationship between the independent variables, security and support, and the dependent variable, personal mobile devices. The analysis of the research study findings revealed a statistically significant relationship exists between the variables. Basic linear regression analyses (see Table 10) were conducted to investigate the relationship between personal mobile use score and the dependent variables corporate support & corporate security. Each test found a highly significant relationship between personal mobile use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. This finding was also significant at $p < 0.001$. Each test found a highly significant relationship between personal mobile Use score and the dependent variable. In the case of corporate support score, the correlation coefficient (0.905) indicates these variables are incredibly highly correlated and the finding is significant at $p < 0.001$. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. This finding was also significant at $p < 0.001$. Linear regression analyses assume that the residuals or error terms resulting from the best-fit line are normally distributed. As illustrated in Figure 5 and 6 shows the observed residuals compared with the expected residuals.

To further illustrate the correlation between the dependent and independent variables chi-square tests were conducted. The methodology is used against each of the

hypothesis to see if there are any relationships between the variables and tests for independence when there are variables from a single population and it is used to determine whether there is a significant association between the variables. The first chi-square test (see Table 11) indicates that there is a relationship between the variable personal mobile devices and corporate support. 72.2% of the participants answered there should be corporate support given when incorporating personal mobile devices. Additionally, the same chi-square was produced (see Table 12) for security and Hypothesis 2 with similar results. 71.3% of the participants answered there should be corporate security given when incorporating personal mobile devices.

However, additional statistical research should be conducted to determine the correctness of the outcomes addressed with this research. This study concluded that if businesses are interested in allowing personal mobile devices to have access to the enterprise system they must consider incorporating security and support within their operating model. However, this research did not answer questions concerning as to what extent or what type of security and support should be considered. There are several types of security and support measures that can be incorporated with personal devices. These range from high to low standards and by just picking a standard without research can cause undue hardship on either the IT staff or the in-users resulting in failure.

There are also several legal questions that could be investigated to further this study with personal mobile devices also known as bring your own device (BYOD) being used in the businesses. Companies are finding that by allowing employees to use their BYOD, it introduces potential risks and legal ramifications requiring assessment and

evaluation. The ricks can vary , but there are several categories to be considered. First, risks relates to the fact that a company's data is now being stored and transmitted using devices that the employer does not own or control. This potential loss of control can clash government regulations requiring companies to carefully protect the privacy and security of sensitive personal, financial, and health-related data. It also poses risks to the protection of a company's trade secret, proprietary, or confidential information. The second set of risks from the impact of BYOD may have an impact on employees behavior. Employees may believe that with the use of their own personal devices there should not be regulations by company concerning policies on acceptable use during and after working hours. This could also include any images and other material that would be in conflict with company policies.

Another risk is the security features found on most mobile devices that will allow a company to deactivate or delete data from an employee's personally own device once it has been reported lost or stolen. This feature deletes not only the employer's information stored on the mobile device but also all other information stored on the device. In other words, the company can send a remote command to an employee's device and the results will delete all of the employee's personal contacts, personal e-mail, photos, videos, books, music, and all other personal information stored on the device including any company information. If the employee has not recently backed up their personal data stored on the device, the deletion could result in the significant loss of potentially irreplaceable data. Even if the employer activated the remote wipe command with the intention of destroying only the employer's business information, the employer still could

be subject to criminal and civil liability if the employee did not provide prior authorization for deletion of his or her personal items.

Another recommendation to expand the research for this study would be to selected a larger population and not just members working in information technology fields. I would recommend future research be done by replicating the study with a larger geographical target population and revamping the questionnaire. This will give businesses an insight from a general view point. Existing literature related to this study indicates there is minimal research on the internal factors affecting the success of personal mobility. Most studies point to external factors such as application downloads or the type of available devices (Ahmad, 2009). Although, it is clear that factors, such as functionality, workforce productivity, physical constraints, time-zone differences, resources, and geographic location, do affect the success of personal mobility, additional studies should be done to substantiate this claim.

Implications

This study has implications for positive social change. As mobile devices become more sophisticated, the demands for this technology within business environments have rapidly increased. By being able to supply real-time access to employer's enterprise systems, employees will benefit by efficiently achieving their goals to swiftly respond to market opportunities that would otherwise result in business loss or losing a competitive edge (James, 2011). Companies are much more likely to achieve competitive advantage and earn above-average profits if managers are able to find unique ways of delivering superior value to customers (Ziolkowski, 2011). Once businesses realize the benefits

associated with personal mobile devices the demand will increase. One of the greatest challenges to management is finding new ways to improve the cost structure, increase efficiency and improve productivity. By allowing employees to access their work from their personal mobile devices, they can utilize time that would otherwise be wasted on long commutes, or waiting for client meetings to begin. Along with an increase in productivity, enterprises can help reduce their hardware costs by implementing policies that allow employees to use their own mobile devices. Employees want to be able to utilize their own phone for convenience. Allowing employees to carry one phone that acts both as a personal and a business phone helps satisfy this demand. To help entice employees to utilize their phones, some enterprises are starting to reimburse a portion of employees' mobile phone plans. By doing so, it acts as both a benefit to employees and a cost savings for enterprises, which no longer have to pay for the entire phone plan as has been the case historically for company issued phones.

While mobile devices are prevalent in private, public and government sectors, this study can have significant implications on integrations to existing information technology environments. At some point there will be a merge in the road for end users and enterprise technology, with each side requiring minimal crossover between the two. The integration can be successful when it incorporates all of the technology components and becomes routine and transparent. The long-term success will hinge on the mobile strategy selected and enforced by the company to integrate mobile devices into the larger strategies for management to identity, access, and protect data throughout the entire IT infrastructure. The greatest chance for success is to have the mobile strategy aligned with

the IT technology goals, the usage patterns of the target audience, and the budget.

The strategy will need a phased mobile roadmap, and leverage as much as possible any existing technology to maximize the budget, and extend any consistent experience in transformation. This strategy starts with defining the mobile goals for the company. Once this has been accomplished the company will have a better understanding of the target audience, budget and internal efforts. A synergy among users is a goal, with the primary focus on those actively using their mobile devices to increase business success. The strategy must meet the requirements of various types of mobile devices because there is no single technology or service plan that can be expected to meet the entire set of enterprise-mobility requirements. As individuals within an organization begin to rely upon their mobile devices, they will have different communication needs, depending upon their work roles and responsibilities (Crumlish & Malone, 2009). This study suggests an approach that can enhance mobile success and contributes to information technology by identifying internal factors that could have an impact on these types of projects.

Conclusion

The purpose for this study was to establish whether or not a company would need to provide support and security for successful integration of personal mobile devices. The academic framework for this study was built upon organizational theory-based methods addressing resource dependency. The analysis of the research study findings revealed a statistically significant relationship exists between the independent variables of support and security and the dependent variable of personal mobile devices (see Figure

2). Basic linear regression analyses (see Table 10) were conducted to investigate the relationship between personal mobile use score and the dependent variables corporate support & corporate security. Each test found a highly significant relationship between personal mobile use score and the dependent variable. The corporate security score was found to be strongly correlated ($R^2 = 0.655$) with the personal mobile use score. While corporate support score, correlation coefficient (0.905) indicates the variables are incredibly highly correlated and the finding is significant at $p < 0.001$.

To further illustrate the correlation between the dependent and independent variables chi-square tests were conducted. The methodology is used against each of the hypothesis to see if there are any relationships between the variables and tests for independence when there are variables from a single population and it is used to determine whether there is a significant association between the variables. The first chi-square test (see Table 11) indicates that there is a relationship between the variable personal mobile devices and corporate support. 72.2% of the participants answered there should be corporate support given when incorporating personal mobile devices. Additionally, the same chi-square was produced (see Table 12) for security and Hypothesis 2 with similar results. 71.3% of the participants answered there should be corporate security given when incorporating personal mobile devices. The results of the analysis compared to the literature indicates a direct relationship between employees abilities to use their mobile devices and employers perception of allowing mobile devices to have access to their internal system.

The need for technological innovation is continually increasing to provide a source of competitive advantage (Perdomo-Ortiz, Gonzalez-Benito, & Galende, 2009). The ubiquity of mobile devices in the corporate environment has allowed the further expansion of the corporate office. From a security and support perspective, the risks and potential effects of allowing devices to connect to corporate IT systems must be understood and managed.

The challenge is to institute a standard process that will allow the integration of new technology into existing systems that address current and future technological constraints. One approach is to allow devices to connect seamlessly with the appropriate support and security evaluations. The challenge is to merge new technology with fiscal and technological constraints while maintaining existing infrastructure investments. An open-technology system that is always connected to various devices is such an approach. This type of environment facilitates an efficient integration that may reduce costs and encourage efforts toward an integrated operational readiness with standards and protocols across the enterprise. The benefits of mobile technology, including connection and accessibility, enable workers to adapt their work lifestyle for efficiency. In the process, they remove the boundaries between work and personal life (Peters & Allouch, 2005), which gives mobile users the desire to use their personal devices for both business and social purposes.

References

Aczel, A. D., & Sounderpandian, J. (2009). *Complete business statistics* (7th ed.). New York, NY: McGraw-Hill Irwin.

Ahmad, N. (2009). *Examining the effectiveness of a mobile electronic performance support system in a workplace environment* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3368366)

Alkazemi, B. Y. (2012). A conceptual framework to analyze enterprise business solutions from a software architecture perspective. *International Journal of Computer Science Issues*, *9*(3), 77-84. doi:10.4304/jsw.6.3.349-365

Aloul, F. A., Zahidi, S. H., & El-Hajj, W. C. (2009). Two factor authentication using mobile phones. *AICCSA, 1*(1), 1–4. doi:10.1109/AICCSA.2009.5069395

Anderson, K., Wright, M., & Wheeler, M. (2011). Snap judgment polling. *International Journal of Market Research, 53*(4), 463-478. doi:10.2501/IJMR-53-4-463-478

Arapakis, I., Jose J. M., & Gray P. D. (2008). *Affective feedback: An investigation into the role of emotions in the information seeking process.* New York, NY: ACM Press.

Babbie, E. R. (2001). *Survey research methods* (2nd ed.). Belmont, CA: Wadsworth.

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology Learning and Performance Journal*, *19*(1), 43–50. Retrieved from http://www.osra.org/itlpj/bartlettkotrlikhiggins.pdf

Basole, R. C. (2004). *Strategic planning for enterprise mobility: A readiness-centric approach.* Atlanta, GA: Tennenbaum Institute, Georgia Institute of Technology.

Basole, R. C. (2008). *Enterprise mobility: Applications, technologies and strategies.* Fairfax, VA: IOS Press.

Basole, R. C., & Rouse, W. (2007). Towards the mobile enterprise: Readiness and transformation. In D. Taniar (Eds.), *Encyclopedia of mobile computing and commerce* (pp. 481–486). Hershey, PA: IDEA Group. doi:10.1002/sys.v8:4

Baxter, L. A., & Babbie, E. R. (2004). *The basics of communication research.* New York, NY: Wadsworth/Thomson.

Bellavista, P., Xie, J., & Tugcu, T. (2009). Recent advances in mobile middleware for wireless systems and services. *Mobile Networks & Applications*, *3*(1),1-3. doi:10.1007/s11036-008-0118-5

Berl, A., & de Meer, H. (2011). Integrating mobile cellular devices into popular peer-to-peer systems. *Telecommunication Systems, 48*(1-2), 173-184. doi:10.1007/s11235-010-9327-x

Brans, P. (2003). *Mobilize your enterprise: Achieving competitive advantage through wireless technology.* New York, NY: Prentice Hall.

Brent, A. C., & Pretorius, M. W. (2008). Sustainable development: A conceptual framework for the technology management field of knowledge and a departure for further research. *South African Journal of Industrial Engineering, 19*(2), 171–182. doi:10.1007/s10669-008-9201-5

Brown, B., & Sikes, J. (2011). How strategic is our technology agenda? *McKinsey Quarterly*, (4), 115-119. Retrieved from http://www.lonerganpartners.com/files/assets/docs/How%20strategic%20is%20our%20technology%20agenda_0.pdf

Bulearca, M., & Bulearca, S. (2009). Internet and interactive websites: Cornerstones of competitive advantage in the virtual economy. *Global Business & Management Research*, *1*(3/4), 44-56. doi: 10.1108/19355181111124070

Burgelman, R. A., Maidique, A.M., & Wheelwright, S. C. (2001). *Strategic management of technology and innovation.* New York, NY: McGraw-Hill.

Burr, W. E., Dodson, D. F., & Polk, W. T. (2008). Electronic authentication guideline. *National Institute of Standards and Technology*, *1*(1), 800–863. doi:10.1109/ACSAC.2008.13

Busha, C. H., & Harter, S. P. (1980). *Research methods in librarianship: Techniques and interpretation*. Orlando, FL: Academic Press.

Byrne, B. M., Shavelson, R. J., & Muthén, B. (1989). Testing for the equivalence of factor covariance and mean structures: The issue of partial measurement invariance. *Psychological Bulletin*, *105*(3), 456-466. doi:10.1037/0033-2909.105.3.456

Byrne, G. (2007). A statistical primer: Understanding descriptive and inferential statistics. *Evidence based library and information practice*, *2*(1), 32-47. doi:10.1108/03074800110390545

Cervone, F. (2010). An overview of virtual and cloud computing. *OCLC Systems &*

Services, 26(3), 162-165. doi:10.1108/10650751011073607

Charland, A., & Leroux, B. (2011). Mobile application development: Web vs. native. *Communications of the ACM*, *54*(5), 49-53. doi:10.1145/1941487.1941504

Chenoweth, T., Minch, R., & Tabor, S. (2010). Wireless insecurity: examining user security behavior on public networks. *Communications of the ACM, 53*(2), 134-138. doi:10.1145/1646353.1646388

Cho, H., Kim, J., & Baek, Y. (2011). Enhanced precision time synchronization for wireless sensor networks. *Sensors, 11*(8), 7625-7643. doi:10.3390/s110807625

Cooper, D. R., & Schindler, P. S. (2003). *Business research methods* (8th ed.). Boston, MA: McGraw-Hill Irwin.

Creative Research Systems. (2009). *Survey design.* Retrieved from www.surveysystem.com/sdesign.htm

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.

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

Crumlish, C., & Malone, E. (2009). *Designing social interfaces: Principles, patterns, and practices for improving the user experience.* Sebastopol, CA: O'Reilly Media.

Daesung, M., Byungkwan, P., Yongwha, C., & Jin-Won, P. (2010). Recovery of flash memories for reliable mobile storages. *Mobile Information Systems*, *6*(2), 177-191. doi:10.3233/MIS-2010-0098

Daniellou, R., & Cilleros, N. (2006). Fingerprint identification and mobile handheld

devices: Overview and implementation. *National Institute of Standards and Technology, 1*(12), 18–25. doi:10.1177/1460458210377482

Davis, C., Schiller, M., & Wheeler, K. (2007). *IT auditing: Using controls to protect information assets.* New York, NY: McGraw-Hill/Osborne.

Davis, M. A., Bodmer, S. M., & LeMasters, A. (2010). *Hacking exposed malware & root kits: Malware & root kits security secrets & solutions.* New York, NY: McGraw-Hill.

Dearman, D. A., & Pierce, J. S. (2008). It's on my other computer: Computing with multiple devices. *Computer Graphics and Applications, 2*(3), 144–1153. doi:10.1145/1357 054.1357177

De Virgilio, R., Torlone, R., & Houben, G. J. (May, 2006). *A rule-based approach to content delivery adaptation in web information systems.* Paper presented at 7th International Conference on Mobile Data Management, Universita Roma Tre, Italy. doi:10.1109/MDM.2006.16

Doherty, I. (2010). Project management for e-learning developments. *Journal of Distance Education*, *24*(1), 91-106. Retrieved from http://www.jofde.ca/index.php/jde/article/view/605/1028

Drejer, A. (2004). Back to basics and beyond: Strategic management - an area where practice and theory are poorly related. *Management Decision, 22*(3-4), 508–520. doi:10.1108/01437720810904194

Dresser, R. (1998). Time for new rules on human subjects research? *Hastings Center Report, 28*(6), 23–24. Retrieved from http://www.ncbi.nlm.nih.gov/

Eliasson, C., Fiedler, M., & Jorstad, I. (2009). A criteria-based evaluation framework for authentication schemes in IMS. *Proceedings of the 4th International Conference on Availability, Reliability and Security, 1*(2), 865–869. doi:10.1109/ARES.2009.166

Ellis, L., Saret, J., & Weed, P. (2012). When company IT is consumerized. *McKinsey Quarterly*, (3), 29. Retrieved from http://www.mckinsey.com/insights/business_technology/when_company_it_is_consumerized

Entner, R. (2010). *Smartphones to overtake feature phones in U.S. by 2011.* Retrieved from http://bit.ly/agwN35

Fang-Yie, L., Ilsun, Y., Feilong, T., Palmieri, F., Fiore, U., & Castiglione, A. (2011). Automatic security assessment for next generation wireless mobile networks. *Mobile Information Systems, 7*(3), 217-239. doi:10.3233/MIS-2011-0119

Farahmand, F., Navathe, S., Sharp, G., & Enslow, P. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management 6*(2). doi:10.1007/s10799-005-5880-5

Fitzgerald, J. (2009). Managing mobile devices. *Computer Fraud & Security*, *2009*(4), 18-19. doi:10.1016/S1361-3723(09)70049-1

Flisi, M. (2000). Smart handheld devices: The emergence of convergence. *Harvard Business Review, 70*(1), 165–175. Retrieved from http://hbr.org

Fonner, K. L., & Roloff, M. E. (2010). Why teleworkers are more satisfied with their jobs than are office-based workers: When less contact is beneficial. *Journal of Applied*

Communication Research, *38*(4), 336-361. doi:10.1080/00909882.2010.513998

Frese, R. (2003). *Project success and failure.* doi:10.1177/0163278712469813

Frieden, T. (2006). *VA will pay $20 million to settle lawsuit over stolen laptop's data*. Retrieved from http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/index.html

Frolick, M. N., & Ariyachandra, T. R. (2008). Performance & management. *Information Systems Management*, *23*(1), 41-48. doi:10.1080/10580 530801941504

Gajmez, N., Cubo, J., Fuentes, L., & Pimentel, E. (2012). Configuring a Context-Aware Middleware for Wireless Sensor Networks. *Sensors*, *12*(7), 8544-8570. doi:10.3390/s120708544

Garretson, C. (2007). Mobile devices expose networks to security threats. *Network World*, *24*(8), 11. doi:10.1080/10580530802384639

Gerhard, T. (2008). Bias: Considerations for research practice. *American Journal of Health-System Pharmacy*, *65*(22), 2159–2169. doi:10.2146/ajhp070369

Glass, G. V., & Hopkins, K. D. (1984). *Statistical methods in education and psychology* (2nd ed.). Englewood Cliffs, NJ: Prentice-Hall.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597-606. doi:10.1007/ BF01172995

Goth, G. (2012). Mobile security issues come to the forefront. *IEEE Internet Computing*, *16*(3), 7-9. doi:10.1109/MIC.2012.54

Grant, K. A. (2008). Developing a model of next generation knowledge management. *Issues in informing science and information technology*, *1*(5), 571–590. Retrieved

from http://proceedings.informingscience.org/InSITE2008/IISITv5p571-590Grant532.pdf

Gray, B. (2009). Mobile device management solutions. *Forrester Research, 1,* 12–23. Retrieved from http://www.microsoft.com/presspass/itanalyst/docs/04-27-09 MobileDeviceManagementSolutions.aspx

Guerrero, L. A., Ochoa, S. F., José A. Pino, & César A. Collazos. (2006). Selecting computing devices to support mobile collaboration. *Group Decision and Negotiation, 15*(3), 243-271. doi:10.1007/s10726-006-9020-3

Guo, P. (2007). *Architectural style based modeling and simulation for mobile systems* (Doctoral dissertation, Add Name of University). Retrieved from http://ubdata.uni-paderborn.de/ediss/17/ 2007/guo/disserta.pdf

Haag, S., Cummings, M., & McCubbrey, D. J. (2005). *Management information systems for the information age* (5th ed.). New York, NY: McGraw-Hill Irwin.

Hennig, N. (2010). *It's a mobile world, where do you fit?* doi:10.1145/1358628.1358652

Holton, E. F., & Burnett, M. (2005). Qualitative research methods. In R. A. Swanson & E. F. Holton (Eds.), *Human resource development research handbook: Linking research and practice* (pp. 20-29). San Francisco, CA: Berrett-Koehler.

Hu, R. (2010). *Discovery & delivery mobile strategy.* Retrieved from http://www.cdlib.org/services/uxdesign/mobile_project/docs/D_D_strategy.pdf

Hussain, A., & Kutar, M. (2012). Apps vs Devices: Can the Usability of Mobile Apps be Decoupled from the Device? *International Journal of Computer Science Issues*, *9*(3), 11-16. Retrieved from http://ijcsi.org/papers/IJCSI-9-3-3-11-16.pdf

Indulska, J., Loke, S. W., Rakotonirainy, A., Witana, V., & Zaslavsky, A. (2002). An open architecture for pervasive systems. *IFIP International federation for information processing 70*(1), 175-187. doi:10.1007/0-306-47005-516

Jacobides, M., & Billinger, S, (2006). Designing the boundaries of the firm: From "make, buy, or ally" to the dynamic benefits of vertical architecture. *Organization Science 17*(2), 249-261. doi:10.1287/orsc.1050.0167

Jamaluddin, J., Zotou, N., Edwards, R., & Coulton, P. (2004). Mobile phone vulnerabilities: a new generation of malware. *IEEE Conference Publications 1*(1), 199-202. doi:10.1109/ISCE.2004.1375935

James, L. (2011). *Making business intelligence easy.* Retrieved from http://www.yellowfinbi.com/Document.i4?DocumentId=179234

Jang, H. (2009). Performance, performance system, and high performance system. *Performance Improvement*, *48*(3), 16-20. doi:10.1002/pfi.20058

Jansen, A., Daniellou, R., & Cilleros, N. (2006). *Fingerprint identification and mobile handheld devices: Overview and implementation.* Gaithersburg, MD: National Institute of Standards and Technology. doi:10.1051/jp4:2004114001 C

Jun-Sub, K., & Jin, K. (2012). Improved secure anonymous authentication scheme for roaming service in global mobility networks. *International Journal of Security & Its Applications*, *6*(3), 45-53. doi:10.1155/2013/302582

Kafaie, S., Kashefi, O., & Sharifi, M. (2011). A low-energy fast cyber foraging mechanism for mobile devices. *International Journal of Wireless & Mobile Networks*, *3*(5), 199-210. doi:10.5121/ijwmn.2011.3516

Kahn, C., & Urie, A. (2011). Managing multi-connectivity for IP services. *Bell Labs Technical Journal*, *15*(4), 45-62. doi:10.1002/bltj.20471

Kauffman, R. J., Ting, L., & Heck, E. (2010). Business network-based value creation in electronic commerce. *International Journal of Electronic Commerce*, *15*(1), 113-144. doi:10.2753/JEC1086-4415150105

Kwong, C. K., Chen, Y. Y., & Chan, K. Y. (2011). A methodology of integrating marketing with engineering for defining design specifications of new products. *Journal of Engineering Design*, *22*(3), 201-213. doi:10.1080/09544820903173180

Lenhart, A., Ling, R., Campbell, S., & Purcell, K. (2010). *Teens and mobile phones.* doi:10.3102/0013189X09339057

Leedy, P., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Pearson Merrill Prentice Hall.

List of programming and computer science terms. (2011). Retrieved from http://www.labautopedia.org/mw/index.php?title=List_of_programming_and_computer_science_terms

Lo Storto, C. C. (2010). Assessing product development performance analyzing the information flows structure using social network analysis measurements. *World Academy of Science, Engineering & Technology*. Retrieved from http://www.waset.org/member/corradolostorto

Lopez, M. (2010). *IT best practices: Mobile policies and processes for employee- owned smartphones.* Retrieved from http://us.blackberry.com/business/leading/IT_Best_

Practices-_Mobile_Policies_and_Processes_for_Employee-owned_Smartphones.pdf

Malik, Y. (2011). The safest haven for data. *Networkworld Asia*, *8*(3), 26. doi:10.1371

Masli, A., Richardson, V. J., Sanchez, J., & Smith, R. E. (2011). The business value of IT: A synthesis and framework of archival research. *Journal of Information Systems*, *25*(2), 81-116. doi:10.2308/isys-10117

May, T. A. (2010). Mobility will be massive and massively disruptive. *Computerworld*, *1*(1), 1. Retrieved from http://www.computerworld.com/s/article/9195422/Mobility_will_be_massive_and_massively_disruptive_

Miller, K. D., & Tsang, E. K. (2011). Testing management theories: Critical realist philosophy and research methods. *Strategic Management Journal*, *32*(2), 139-158. doi:10.1002/smj.868

Ming-Shian, W., Sun-Jen, H., & Li-Wei, C. (2011). The preparedness of critical success factors of IT service management and its effect on performance. *Service Industries Journal*, *31*(8), 1219-1235. doi:10.1080/02642060903437014

Mobile electronics glossary. (2011). Retrieved from http://www.the12volt.com/glossary/glossaryofterms

Momaya, K., & Ajitabh, A. (2005). Technology management and competitiveness: Is there any relationship? *International Journal of Technology Transfer and Commercialization*, *4*(4), 518–524. doi:10.1504/05.6702

Montana, P. J., & Charnov, B. H. (2000). *Management* (3rd ed.). Hauppauge, NY: Barron's Education.

Morabito, J., Sack, I., Stohr, E. A., & Bhate, A. (2009). Designing flexible organizations. *Global Journal of Flexible Systems Management*, *10*(2), 1-10. doi:10.1007/978-81-322-1560-8

Mukherjee, I. (2008). The complexity paradigm: Implications for information systems and their strategic planning. *Journal of Computer Science, 4*(5), 382-392. doi:10.3844/jcssp.2008.382.392

Nah, F., Siau, K., & Sheng, H. (2005). The value of mobile applications: A utility company study. *Communications of the ACM, 2*(48), 85–90. doi:10.1145/1042091.1042095

Neuman, W. L. (2006). *Social research methods: Qualitative and quantitative approaches.* Boston, MA: Pearson Education.

Nevo, S., & Wade, M. R. (2010). The formation and value of IT enabled resources: Antecedents and consequences of synergistic relationships. *MIS Quarterly, 34*(1), 163-183. doi:10.1016/j.jsis.2011.08.001

Nixon, M. S., Tan, T., & Chellapppa, R. (2006). *Human identification based on gait.* New York, NY: Springer Science Business Media.

Oren, R. A. (2009). *Contributory success factors for projects with the project management profession: A quantitative analysis* (Doctoral dissertation). Capella University, Minneapolis, MN. Retrieved from http://gradworks.umi.com/33/68/3368756.html

Otim, S., Dow, K. E., Grover, V., & Wong, J. A. (2012). The impact of information technology investments on downside risk of the firm: Alternative measurement of

the business value of IT. *Journal of Management Information Systems*, *29*(1), 159-194. doi:10.1287/mnsc.1060.0542

Paap, J., & Katz, R. (2004). Anticipating disruptive innovation. *Research Technology Management 47*(5), 13–22. doi:10.1109/EMR.2004.25138

Paul, R., & Elder, L. (2001). *Critical thinking: Tools for taking charge of your learning and your life.* Upper Saddle River, NJ: Prentice-Hall.

Payne, A. (2006). Management: From strategy to implementation. *Journal of Marketing Management, 22*(1), 135–168. doi:10.1108/S1548-6435

Perdomo-Ortiz, J., Gonzalez-Benito, J., & Galende, J. (2009). The intervening effect of business innovation capability on the relationship between Total Quality Management and technological innovation. *International Journal of Production Research*, *47*(18), 5087-5107. doi:10.1080/00207540802070934

Peslak, A., & Stanton, M. (2007). Information technology team achievement: An analysis of success factors and development of a team success model (TSM). *Team Performance Management, 13*(2), 21–33. doi:10.1108/13527590710736707

Peters, O., & Allouch, S. B. (2005). Always connected: A longitudinal field study of mobile communication. *Telematics & Informatic, 22*(3), 239–256. doi:10.1016/j.tele.2004.04.003

Pfaffenberger, B. (2009). *Webster's new world dictionary of computing terms* (6th ed.). New York, NY: Simon and Schuster.

Pinkerton, W. J. (2003). *Project management: Achieving project bottom-line success.* New York, NY: McGraw-Hill.

Porter, M. (2007). Towards a dynamic theory of strategy. *Strategic Management Journal 12*(2), 95-117. doi:10.1002/smj.4250121008

Priestnall, G. (2009). Landscape visualization in fieldwork. *Journal of Geography In Higher Education*, *33*104-112. doi:10.1080/03098260903034020

Rouse, W. B. (2005). A theory of enterprise transformation. *Systems Engineering, 8*(4), 279–295.

Sanni, M. L., Hashim, A. A., Anwar, F. F., Naji, A. W., & Ahmed, G. M. (2011). Mobile multicast in wireless mesh networks. *Australian Journal of Basic & Applied Sciences*, *5*(9), 957-966. doi:10.2306/scienceasia1513-1874.2013.39S.095

Saravani, S., & Haddow, G. (2011). The mobile library and staff preparedness: Exploring staff competencies using the unified theory of acceptance and use of technology model. *Australian Academic & Research Libraries*, *42*(3), 179-190. doi:10.1108/00330331111151638

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526–531. doi:10.1016/s0167-4048(02)01009-x

Semer, L. (2013). Auditing the BYOD program. *Internal Auditor*, *70*(1), 23-27. Retrieved from HighBeam Research: http://www.highbeam.com/doc/1G1-321173133.html

Seidman, I. (2007). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (3rd ed.). New York, NY: Teachers College Press.

Sejong, O. (2010). New role-based access control in ubiquitous e-business environment. *Journal of Intelligent Manufacturing*, *21*(5), 607-612. doi:10.1007/s10845-008-

0208-z

Sharples, M. (2000). The design of personal mobile technologies for lifelong learning. *Computers and Education, 1*(34), 177–193. doi:10.1016/S0360-1315(99)00044-5

Signorini, E., & Hochmuth, P. (2010). Creating a business class mobility environment in the enterprise. *Yankee Group Research, Inc., 1*(1), 1-10. doi:10.4018/978-1-4666-2533-4.ch009

Simon, M. K. , & Francis, J. B. (2006). *The dissertation and research cookbook: From soup to nuts.* Dubuque, IA: Kendall/Hunt.

Singleton, R., & Straits, B. C. (2005). *Approaches to social research.* New York, NY: Oxford University Press.

Smith, K. J., & Forman, S. (2014). Bring your own device—challenges and solutions for the mobile workplace. *Employment Relations Today*, *40*(4), 67-73. doi:10.1002/ert.21436

Smith, L. (2010). Security policies put a tight leash on enterprise mobile use. *Enterprise Innovation*, *6*(5), 28-29. doi:10.1177/1094670509357611

Solanas, A. (2010). *Advances in artificial intelligence for privacy protection and security.* Hackensack, NJ: World Scientific.

Standing, C., Guilfoyle, K., Lin, C., & Love, I. (2006). The adoption of IS/IT evaluation methodologies. *Proceedings of the Sixteenth Australasian Conference on Information Systems,* Sydney, Australia. doi:10.4018/978-1-60566-026-4.ch010

Sukamolson, S. (n.d.). *Fundamentals of quantitative research.* Retrieved from http://www.culi.chula.ac.th/Research/e-Journal/bod/Suphat%20Sukamolson.pdf

Swaroop, V., Kumar G. G., & Shanker, U. (2011). Issues in mobile distributed real time databases: Performance and review. *International Journal of Engineering Science & Technology, 3*(4), 3504-3517. doi:10.1007/s11832-011-0368-9

Tama, J. (2012). Mobile data privacy: Snapshot of an evolving landscape. *Journal of Internet Law, 16*(5), 1-23. doi:10.1504/IJCSE.2012.046177

Tarasewich, P. (2008). Mobile interaction design: Integrating individual and organizational perspectives. *Information Knowledge Systems Management, 7*(1), 239–256. doi:10.1145/953460.953489

Tarsitano, A., & Falcone, M. (2011). Missing values adjustment for mixed type data. *Journal of Probability & Statistics*, 1-20. doi:10.1155/2011/290380

Teral, S. (2009). Identifying and controlling mobile network costs. *Journal of Telecommunications Management*, *2*(3), 238-243. Retrieved from http://henrystewart.metapress.com/app/home/contribution.asp?referrer=parent&backto=issue,6,11;journal,6,12;linkingpublicationresults,1:120820,1

Terzi, S. (2005). *Elements of product lifecycle management: Definitions, open issues and reference models* (Doctoral dissertation). Retrieved from http://tel.archives-ouvertes.fr/docs/00/04/81/65/PDF/tel-00009559.pdf

Thanh, D., Jorstad, I., Jonvik, T., & Thuan, D. (2009). Strong authentication with mobile phone as security token in mobile adhoc and sensor systems. *IEEE International Conference, 1*(6), 777–782. doi:10.1109/MOBHOC.2009.5336918

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

Tripathi, K. (2012). M - Commerce: A recent trend in business and management. *Researchers World: Journal of Arts, Science & Commerce, 3*(4), 25-28. doi:10.4018/978-1-4666-4936-1

Trochim, W. M., & Donnelly, J. P. (2007). *The research methods knowledge base.* Cincinnati, OH: Atomic Dog.

Tsalgatidou, A., & Pitoura, E. (2001). Business models and transactions in mobile electronic commerce: Requirements and properties. *Computer Networks, 37*(1), 221–236. doi:10.1016/S1389-1286(01)00216-X

Varshney, U., & Vetter, R. J. (2001). A framework for the emerging mobile commerce applications. *Proceedings of the 34th Hawaii International Conference on System Sciences,* Los Alamitos, CA. Retrieved from http://dl.acm.org/citation.cfm?id=820766

Viscusi, S. (2006). The risky business of mobile device compliance in the workplace. *Workforce Management, 2*(4), 8–10. Retrieved from http://www.tmcnet.com/channels/workforce-management/articles/3774-risky-business-mobile-device-compliance-the-workplace.htm

Wagner, E. D. (2005). Enabling mobile learning. *EDUCAUSE Review*,*40*(3), 40–53. doi:10.1037/0278-7393.30.6.1302

Ward, S., Bridges, K., & Chitty, B. (2005). Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications, 11*(1), 21–40. doi:10.1080/1352726042000263575

Washburn, B. (2010). *OCLC research: Library mobile app development, current conditions and strategic choices.* doi:10.1145/1358628.1358652

Weiling, K., & Ping, Z. (2009). Motivations in OSS communities: The mediating role of effort intensity and goal commitment. *International Journal of Electronic Commerce, 13*(4), 39–66. doi:10.2753/JEC1086-4415130403

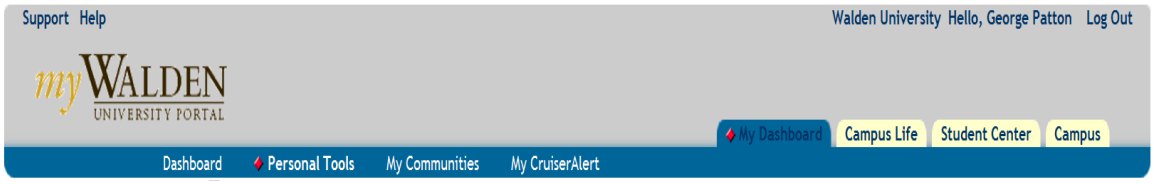
Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy, 2*(5), 25–31. doi:10.1109/MSP.2004.81

Yin, R. K. (2003). *Case study research* (3rd ed.). Thousand Oaks, CA: Sage.

Yoo, C. (2011). Cloud Computing: Architectural and Policy Implications. *Review of Industrial Organization*, *38*(4), 405-421. doi:10.1007/s11151-011-9295-7

Ziolkowski, M. F. (2011). Municipal telecommunications master planning to achieve competitive advantage in a global economy. *Industrial Geographer*, *8*(1), 26-43. doi:10.1080/0965431032000088506

Appendix A: Permission to Use Copyrighted Material



Subject : Permission granted
Date : Thu, Jan 26, 2012 05:10 PM CST
From : Lachlan James <lachlan.james@yellowfin.com.au>
To : george.patton@waldenu.edu

Hello George,

With proper source attribution, we're perfectly happy for you to quote some statistics/figures from our Mobile BI white paper.

Best regards,

Lachlan James
Yellowfin Communications Manager

e. lachlan.james@yellowfin.com.au
p. +61 03 9090 0454
m. 0431 835 658

For regular updates follow us on Twitter @YellowfinBI

Subject : RE: Permission to use the following pictures from Strategic Planning For Enterprise Mobility: A Readiness-Centric Approach

Date : Wed, Aug 12, 2011 05:12 AM CDT

From: "Rahul C. Basole" rahul.basole@ti.gatech.edu

To: George Patton <george.patton@waldenu.edu>

Dear George-

Thank you for your email. I am glad to hear that my work has proven useful to you. I hereby grant you permission to use the two figures as long as you fully cite my work in your dissertation and associated presentations.

You may want to cite my dissertation as well: http://etd.gatech.edu/theses/available/etd-06162006-142751/unrestricted/basole_rahul_c_200606_phd.pdf

Best of luck with your dissertation.

Thanks,
Rahul

Appendix B: Survey Questions

Section I - Demographic information

1. Age ☐ 22 -31 ☐ 32- 41 ☐ 42-51 ☐ 52-61 ☐ 62 +
2. Gender ☐ Male ☐ Female
3. Years of IT experience.
   ☐ 1- 5 ☐ 6 – 10 ☐ 11 – 15 ☐ 16 – 20 ☐ 21 – 25 ☐ 26+

4. Education
   ☐ High school ☐ Associate's degree ☐ Bachelor's ☐ Master's ☐ Doctorate

5. What is your job role?
   ☐ Manager ☐ Team Lead ☐ Analysis ☐ Developer ☐ Support ☐ Other

Section II - General Questions

6. Do you own a SmartPhone?
   ☐ Yes ☐ No

7. How long have you had a personal mobile device?
   ☐ 1- 5 ☐ 6 – 10 ☐ 11 – 15 ☐ 16 – 20 ☐ 21 – 25

8. Is an optimization connection a concern for using your personal mobile device?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strong-ly agree
☐	☐	☐	☐	☐

9. Is user simplicity important to you?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strong-ly agree
☐	☐	☐	☐	☐

10. Should personal mobile devices be allowed to connect to the corporate IT system if given permission?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strong-ly agree
☐	☐	☐	☐	☐

11. Would access to a corporate application system through personal mobile device benefit you at work?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

12. How essential would access to corporate applications become to your job role?

Little essential	Somewhat essential	Neither little nor somewhat essential	Very essential	Extremely essential
☐	☐	☐	☐	☐

Section III – Support Questions

13. Should corporate IT assist in the first time device set-up for personal mobile devices?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

14. Should corporate IT provide continuing support for personal mobile devices after connection is established ?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

15. Should corporate IT be able to automatically load support application to the personal mobile device for support?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

16. Should personal data be kept private and not stored as part of the IT backup/recovery procedures?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

17. Should there be a limit on the types of mobile devices supported by corporate IT?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

Section IV – Security Questions

18. Should security measures be enforced on personal mobile devices (i.e., passwords, device encryption, etc.)?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

19. Should security software be provided by corporate IT support?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

20. Should corporate IT have access to personal mobile devices to disable them in case they are lost or stolen?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

21. Should auditing and archiving of personal phone records, messaging records, emails and voice messages be allowed by corporate IT?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

22. Should corporate IT be able to remotely remove corporate software from a personal mobile device after an employee is terminated or leaves the organization?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
☐	☐	☐	☐	☐

Appendix C: Email Introduction

Dear <Participant>:

I am George Patton and I am completing the final requirements for my doctorate degree. This email is an invitation requesting your participation in a study on supporting and securing personal mobile devices within an existing Information-Technology Environment. Please reference the attached consent form concerning the details on the study and survey that will only take few minutes of your time to complete.

You have been chosen to take part in this study because of your associations within the IT department and as a result you meet the initial eligibility requirements to participate in this research study. Should you have any questions or concerns please contact me at george.patton@waldenu.edu or my chairperson Dr. David Gould by email at david.gould@waldenu.edu.

Thanking you in advance for your participation in this important study.

Regards,

George Patton

Doctor of Management (candidate)

Appendix D: Survey Code Table

Answers to Questionnaire	Assigned numbers
Strongly disagree	1
Disagree	2
Neither agree nor disagree	3
Agree	4
Strongly agree	5
Little critical	1
Somewhat critical	2
Neither little nor somewhat critical	3
Very critical	4
Extremely critical	5

Curriculum Vitae

George A. Patton
george.patton38017@yahoo.com

Professional Profile

Eager to bring students into the twenty-first century using a unique combination of education experience coupled with twenty years' of business background in computer systems management.

- Achieving a PhD Degree in Management
- Hold Master Degree in Business Administration.
- Experienced in use of the Internet educational software.
- Dedicated to enthusiastic and dynamic teaching as a means of creating and nurturing a lifelong love of knowledge in the classroom.

Education, Honors, and Certifications

Ph.D. Management
Specialization: Leadership and Organizational Change
Dissertation Title: Supporting Personal Mobile Devices within an Existing Information Technology Environment
Walden University
Graduate: May 2014
Member: Walden University International Honour Society

Master of Business Administration Degree,
Strayer University
Graduated: June 2006
Dissertation: Synchronization of Electronic Information using Global Supply Chain

Bachelor of Science Degree in Business Administration
California Coast University
Graduated: June 1989

Key Qualifications

Innovative teaching methods
Effective use of multi-media teaching tools
Exceptional written and verbal communicator
Online course instructor
Innovative thinker
Natural leader
Plan and instruct each subject area using wide variety of teaching aids, motivational and implementation strategies to engage students in active learning.
Incorporate learning modality principles into classroom and individual instruction.
Develop and conduct inter-grade activities. Implement technological approaches to subject material. Research educational resources on the Internet. Assist with information retrieval.

Experienced Computer Educator

Introduced students to the concepts of E-Commerce. Challenged and motivated students through in-depth lectures and discussions. Initiated thought-provoking classroom discussions to help students develop their critical thinking abilities. Challenged and motivated students through in-depth lectures and discussions.

Computer Technical Proficiencies

Platforms: ITX Basic/ITX advanced Operating Systems, SCO/AIX/ATT UNIX Operating Systems, Windows/Windows NT Operating System, IBM Mainframe
Networking: TCP/IP, FTP/SFTP, PGP, RAFTS, web Methods, VPN
Languages: COBOL, COBOL 74/85, COBOL RM, ACCESS, FOURTH GL

Tools: Gentran Basic for MVS, Gentran Basic for DOS, Gentran Mentor for UNIX, Gentran Server for UNIX with EC Workbench, Gentran Server Extension for SAP R/3, Contivo, Microsoft Project, Microsoft Excel, Job Control Language (JCL), Lotus SmartSuite, Access Programming Development, Web Methods SOA, VISO, SharePoint, Quality Management Concepts, Managing Successful Projects, Finance and Strategy, How to Motivate, Manage, and Lead a Team, Leadership Development Core I, PMP Certification: In progress

Employment

International Paper Company, Memphis, TN 1998 – Present
Senior Project Manager

Reviewed and prepared responses to RFIs/RFPs. Manage and support customer trials/proof of concepts, ensuring closure upon completion. Act as liaison between customers and development plus support groups to assure smooth technical adoption during and after the project. Management responsibilities are to strategically budget, plan, and monitor IT projects for the department.

Moeller Products Co, Greenville, MS 1995-1998
IT Systems Manager

Management of IT, sales and accounting staff to encompass day to day operations and assignments. Research and purchases of new computer hardware and software for the company as needed.

Southwest Community College, Memphis, TN 2000-2007
Adjunct professor

Introduced students to the concepts of E-Commerce. Challenged and motivated students through in-depth lectures and discussions. Initiated thought-provoking classroom discussions to help students develop their critical thinking abilities.

Mississippi Delta Community College, Moorhead, MS 1994-1998
Adjunct professor

Programming instructor for evening classes on campus. Challenged and motivated students through in-depth lectures and discussions. Initiated thought-provoking classroom discussions to help students develop their critical thinking abilities.