**Volume 9, Issue 1**
April 2016
ISSN: 1946-1836

# JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

**In this issue:**

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **ISCAP,** Information Systems and Computing Academic Professionals. Publishing frequency is currently quarterly. The first date of publication was December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for JISAR.

# JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

## Editors



## JISAR Editorial Board

# Exploring Relationships between the Strategic Importance of IT and the Effectiveness of IT Security and Mobile Device Management

James A. Sena
jsena@calpoly.edu

Taryn Stanko
tstanko@calpoly.edu

Management Area
Orfalea College of Business
California Polytechnic State University
San Luis Obispo, CA 93407, USA

Mark Sena@xavier.edu
Xavier University
Cincinnat, Ohio, USA

## Abstract

Based on the analysis of 131 executive interviews, this study explores the relationships among three key aspects of the strategic use of information technology: the perceived strategic importance and effectiveness of IT, the perceived effectiveness of information security, and the perceived effectiveness of mobile device management. Relationships among the three sets of items are explored using NVivo qualitative assessment of executive comments along with correlation measures and differences in mean responses of Likert scale responses. The research findings indicated that organizations recognize the strategic importance of IT and the effectiveness of IT. Across industries, IT is strategically important but for some industries not as effective. Security is linked closely to mobile devices.

**Keywords:** IT Strategy, Effectiveness, Security, Mobility, Mobile devices

### 1. INTRODUCTION

Organizations of all sizes recognize the opportunities to deploy mobile devices that foster collaboration and drive new levels of productivity. However, many IT administrators, developers, and organizational leaders are struggling to find an effective way to secure and control mobile use while stimulating user adoption. Early uses of smart devices at work centered on a few core apps: email, calendar, and contacts. Users then started bringing their "personal apps" into the workplace, and software providers recognized this trend and began offering productivity apps for the workplace. IT must secure and support corporate apps on devices they do not own or entirely control. This support is vital to ensure security and governance of corporate assets (Mobile Application Management, 2015).

As the distinction between personal and organizational device usage continues to blur, the combination of applications that interact increases the need to investigate potential security issues (Suby, 2014). Mobile devices are

integrating into increasingly globally transparent business infrastructures (IBM MobileFirst, 2015). Gartner (2012) predicted that, by 2016, 40 percent of the workforce will be mobile and that the majority of them would possess a smartphone. This evolution potentially impacts a range of business strategies that include network security, device and application development, and data management.

A study conducted by IBM (Taft, 2015) highlights the lax security practices among enterprises. The results indicate that mobile app developers are not investing sufficiently in security. Nearly 40% of large companies, including many in the Fortune 500, are not taking proper precautions to secure the mobile apps they build for customers. The study also found organizations are not protecting their corporate and BYOD mobile devices against cyber-attacks—opening the door for hackers to access user, corporate and customer data. All the while, the number of mobile cyber-security attacks is continuing to grow. At any given time, malicious code infects more than 11.6 million mobile devices. The study showed that most organizations tend to prioritize speed-to-market and user experience over security. Moreover, they tended to scan their mobile apps for security vulnerabilities infrequently and much too late.

For enterprise CIOs, this means creating strategies to ensure that their IT component within their organizations is secure. At the same time, they need to ensure that IT continues to be effective as a partner in an organization's strategic plan. IT is becoming stewards of business agility and change – and serves as the primary engine for implementing change (IBM Institute for Business Value 2012).

According to Gartner (2014) by 2020, 75% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2012. Most external assessments of enterprise value, security and viability will include explicit analysis of IT assets and capabilities. IT will continue to performance, competitive advantage, risk management and transparency -and– the enterprises ability to merge, acquire and partner.

In this paper, we explore the relationship between the strategic importance and effectiveness of IT and the effectiveness of security and mobile device management. We address the pros and cons of IT as an effective instrument in maintaining companies have an increasing impact on competitive business strategies. Figure 1 shows the relationships and proposed framework. We focus on information security and mobility as change agents across industries. We begin with a consideration of IT as a part of corporate strategy and competitive positioning. The main focus of this study addresses the need for an effective competitive strategy gave the changing landscape of mobility and mobile work and security measures. In section two, we provide a background and a brief discussion on varying strategic perceptions of IT across industries and the impact of mobility and security issues. In section three, we detail the methodology and research questions addressed in the study. In section four, we reveal the results of the analysis and related discussion. Lastly, in section five we provide conclusions, limitations, and opportunities for future research on this subject.

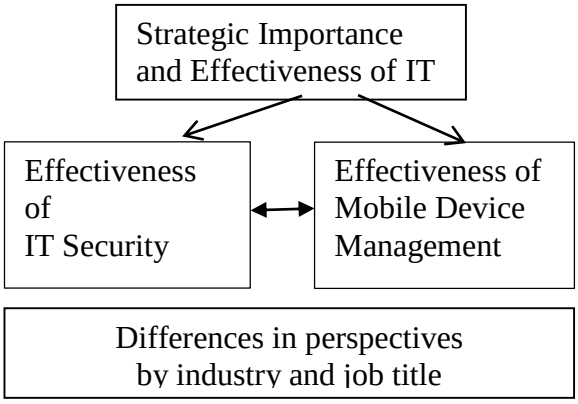


**Figure 1: Research Framework**

## 2. DISCUSSION OF THE FRAMEWORK

### Strategic Use of IT

As with other forms of capital, organizations are motivated to invest in IT to increase productivity, gain an advantage over competitors, and increase profitability. Competitive advantage through investment in IT alone, however, is difficult to achieve and sustain and is vulnerable to the ability of competitors to replicate the productivity and profitability improvements gained through innovation. Investments in IT are more likely to be effective when coupled with some other sustainable advantage(s) by taking advantage of changing conditions in the workplace. There are four forces driving innovations: maintaining data control; implementation costs (e.g. software as a service); responses to changes; and, foremost providing a secure work environment.

**IT Considerations**

In general, the literature supports the notion that IT initiatives do not necessarily lead to a positive return on investment. A McKinsey Global Institute study (Manyika, 2011) on "U.S. Productivity Growth for 2000-2008" found a positive correlation between IT investments and productivity in only 35% of the industries. Strassmann (2003) earlier contended that "profitability and IT spending were unrelated" and return on IT investments is a primary concern and appropriate measures necessary to "distinguish fads from substance." He asserted that the major pitfall in IT decision making was embracing a solution without fully understanding underlying needs.

According to McKinsey (Arandejelovic et al., 2015), when CIOs play an active role in business strategy, IT performance on a wide range of functional and business tasks improves. In their business technology survey, few executives say their IT leaders are involved closely in helping shape the strategic agenda, and confidence in IT's ability to support growth and other business goals is waning. Akella et al., 2012).

**Mobility Issues**

Today work is becoming less defined as a place where one *goes to* and is more defined by what one *does*. There has been a rapid shift in workplace dynamics with workers outside the traditional office boundaries. The increase in remote workers and the trend to work on-the-go requires the need to be connected and to interact with business-critical information. Wherever one is — whether it is visiting customers, teleworking or accessing information in the manufacturing plant about customer orders or product performance requires connectivity.

At the tip of the iceberg, organizations are feeling the pressure to allow users to access sensitive corporate data via their personal mobile devices. These devices have become a widespread issue as 74% of organizations are allowing or planning to allow employees to use their own devices in the workplace (Zdnet, 2015). Employees want the flexibility to use applications from within the workplace, and at any time from any device. Such applications include enterprise resource planning (ERP), customer relationship management (CRM), and other enterprise systems; not only e-mail and instant messaging. With so much at stake, including network security and customer privacy the organization needs to address these new and changing requirements cautiously. Already organizations of all sizes are taking advantage of anytime, anywhere access; web services; and social networking features to boost employee collaboration, improve customer service and speed of decision-making, providing organization's competitive edge. Like previous technology waves, these personal devices are a godsend for productivity and collaboration (Akella et al., 2012). As users become more adept in utilizing computing resources in their private lives, they tend to demand more from their business resources as well. This concept referred to as "consumerization" reflects the changing expectations that users place on workplace technology resources (Symantec Global Services, 2015).

Organizations must exist and function competitively and profitably in the virtual world of cyberspace (Harrell, 2002). More people in the world now have a mobile phone than a land line. Mobile devices outnumber personal computers by three to one, credit cards by two to one and TVs by two to one (Campbell, 2009)..

**The Mobile Worker Issues**

Every organization has a distinct threshold for absorbing change. This threshold ultimately determines the pace at which many initiatives are implemented. When considering the mobile worker both IT and the organization at large need to understand the supply and demand of change and anticipate appropriately. To be a successful enabler the organization and the IT function must achieve a balance between tolerance and need for change.

With work no longer a "place" where one receives pertinent business information and remain productive, the trend towards a larger mobile or remote workforce is more of a reality. Advances in mobile-accessible technology, from more sophisticated devices with increased processing power to business intelligence software, enable a more productive workforce by pushing the boundaries of what can be accomplished "on-the-go." No longer does location mean restricted access.

One characteristic of the high-performance workplace is the inclusion of ubiquitous collaboration, defined *as collaboration anytime, anyplace, and anywhere* (Gartner, 2011). Because of its ubiquitous nature, technologies for accomplishing collaborative tasks are of high importance to individuals at all levels and in all types of organizations. While organization leaders frequently focus on the cost benefits analysis in choosing technologies for their firms,

members of the collaborative work teams may be more impressed with features that aid in efficient and effective task accomplishment. These divergent aims may prevent organizations from achieving maximum efficiency and effectiveness from new technologies.

As organizations stretch their wings and adjust to operating in the world without boundaries management must take steps to eliminate the distance between data centers and remote and mobile workforces. Access to business-critical applications and data, while maintaining a secure environment, is critical. The structure of the traditional work environment is continuously changing. Existing work practices and managerial strategies are often not appropriate in those environments. In particular, traditional office communication with coworkers and management, usually dependent on physical proximity, has been disrupted (Gargiulo, 2010).

Most employees already use some mobile device in their personal lives. Moreover, more and more companies are expecting their workers to be available when they are out of the office. All of these factors combine to make handheld mobile devices a necessity, and. Therefore, IT must support them. It is the forward-thinking companies that have seen benefits across the organization, including IT, executive management, field service delivery and repair technicians, sales, operations, marketing and customer service. They've seen a positive impact on employee collaboration and productivity, real-time access to critical business information and employee satisfaction. They've also witnessed reduced costs, faster decision making and improved customer satisfaction (Sybase, 2010).

However, organizations face a particular challenge (Desouza, 2009). While teleworking and remote-access are becoming the norm increasingly, the majority of business applications and the critical customer data contained within them remain cordoned inside the four walls of the enterprise. Once field workers leave the office, they become isolated from vital customer information and desk-bound enterprise applications lose their immediate value. A mobilization strategy can counter this. At a corporate level, mobile business applications play an integral part of increasing customer satisfaction levels and meeting increasingly stringent service level agreements in an ever more competitive marketplace.

As mobile workforces grow, the demands on IT (McDowell, 2010) executives to provide the tools that allow employees to have access to key organizational data anytime, anywhere is growing as well. Add to that today's business environment, which moves at breakneck speed, and more CIOs are incorporating a mobile strategy into their IT infrastructure plans. According to Forrester Research (Leggett, 2015), providing more mobility support to employees is a top telecommunications and IT initiative of today's enterprises. Also, Forrester states that nearly half of enterprises say that formalizing and executing a mobile strategy (one that contains architectural frameworks for mobility) is a priority.

**Security Issues**

The sheer size and complexity of today's enterprises makes it nearly impossible to keep up with the rate of change in IT security, requiring a top-down strategy that prioritizes risk and accepts the limitations of available technologies. Only through the adoption of high-level policies and controls aimed at fostering flexible security practices across the organization and via more aggressive sharing of information about threats with others can companies improve their protection.

Mobility (Oliver, 2010) brings numerous opportunities – but also challenges. Mobile workers are imperative to an organization's success, but their device usage varies broadly. For example, information workers (that is, people who work both at a desk and outside of the office) need to use their devices for email, PDFs, and scheduling. By contrast, task workers need access to the most up-to-date customer information and require fast approval for business processes such as work orders. Adding to this complexity, the number of devices that support these workers are proliferating throughout corporations. With a mobile workforce comes the widespread distribution of sensitive, proprietary, and sometimes top-secret data outside the secure walls of headquarters. It is critical to the success of a mobile deployment to put measures in place to control and protect mobile assets. By implementing a solution that proactively manages and secures mobile data, devices, and applications, mobile projects can improve efficiency, customer service and – ultimately – profitability.

Organizations are in a difficult position of maintaining security provisions while enabling the productivity and conveniences afforded by mobile devices. Users are challenging, and even

rejecting, traditional mobile-device management (MDM) solutions, fearing their employers' ability to access, alter or delete personal data stored on their mobile devices (Eddy, 2015).

Corporate policy should limit the amount and type of sensitive information that's storable on a remote laptop or handheld device. If a small amount of sensitive information must be stored, the policy should mandate software that executes some Storage-level encryption. Of course, for the highest levels of data sensitivity, the policy should entirely prevent data storage on mobile devices. Access and control of mobile devices within the corporate network is imperative because software-based virtual private network (VPN) clients allow secure remote access to corporate networks from laptops. Thus, the second set of requirements addresses selecting mobile devices is based on security. Each remote device must have VPN software support, and basic locks and password protection**.**

Protecting the confidentiality, integrity and availability of electronic information -- is an important issue for businesses. Security incidents cost money regardless of the size or scale of the business operation. Most all businesses, regardless of size, have a web presence, interact with their suppliers and customers via the Internet and perhaps have offices or presence in different geographical areas. Also, the presence of the cloud and the myriad of mobile devices further serve to confound firm's IT policies. These changes dramatically increase security risk. Security solutions exist to support businesses of all sizes but do not necessarily take into account the specific nature of the business.

## 3. RESEARCH QUESTIONS AND METHODOLOGY

To investigate the ramifications of IT security, mobility and the cloud on IT strategy and effectiveness we offer the following research questions:

**Research Question 1**: **To what extent is IT used as a strategic resource? How effective are efforts to use IT as a strategic resource?**

**Research Question 2**: **To what extent are effective security policies related to the strategic use of IT?**

**Research Question 3**: **To what extent are effective mobile policies related to security policies?**

The investigation based on these research questions consisted of personal interviews with 131 senior level executives during a three-year period (2012 to 2014). We used a subset of questions described in Table 2 that closely followed our primary long-term research effort. MBA graduate students at their place of employment conducted the interviews primarily face-to-face. The subjects were offered confidentiality -- their names and affiliations were not revealed in the data set. Most of the interviews were conducted with executives in a relatively large city in the Midwestern United States. Thus, the findings in this research paper may be limited if there are regional differences in perspectives. Consistent with other academic empirical research, the subject pool was not restricted to one respondent per organization. Thus, the results should be interpreted with the potential that large companies might have multiple entries.

The executives were asked to comment on a series of questions about IT strategy, effectiveness, mobile policies, and security and provide a Likert scale rating (5=strongly agree, 3=neutral, 1=strongly disagree). The comments were accompanied by narrative discussions related to each question.

| | | Question |
|---|---|---|
| IT Strategic | | 1. My organization uses IT as a strategic, competitive resource? |
| IT Effective | | 2. My organization manages IT projects effectively? |
| Maintain Security | | 3. My organization maintains effective IT security (policies, education, technologies) to manage risks within a reasonable budget? |
| Mobile Computing | | 4. Has my organization an effective policy for managing mobile devices? |

Table 2. Interview Questions

Using Figure 1 as a starting point we constructed two tables (see the Appendix) that presented the question results by industry classification and position expressed in mean values and percentages. Also, correlations along with relevant question nomenclatures were included.

The intent was to place the research questions interpretation in a holistic manner. We also made extensive use of Pivot Tables and filters to examine further the findings.

To help us better understand these dimensions, our interviewees were asked to describe in more detail why they gave a particular rating for each of the questions listed in Table 2. We used NVivo, a qualitative analysis software package, to analyze this additional data. Each interviewer provided detailed notes and quotes from the interview conducted, and the notes for all 131 interviews were imported into NVivo for analysis. To conduct this analysis, we first grouped the interviewees into categories depending on how they answered the study questions. Responses to each study question were placed into one of two categories: (1) high (Likert score above 3), or low (Likert score less than or equal to 3). We then created collections of interviewees in NVivo for each of our research questions based on responses to the study questions. For example, to help us explore our second research question we created collections (groups of interviews) based on the respondents' answers to interview questions 1 and 3 – regarding whether the company uses IT as a strategic resource and whether they are particularly effective in maintaining IT security.

Two of the authors then met in a series of face-to-face meetings to code the data to identify common themes that emerged and clustered these themes into categories. For example, "Lack of IT staff" and "Shifting Priorities" emerged in coding responses to the questions of whether IT is strategical. These codes were clustered into a higher level category called "Barriers." Themes that emerged are displayed and discussed for each research question.

## 4. ANALYSIS AND FINDINGS

The Pearson Correlation was conducted to examine the research questions (see Appendix). The Pearson Correlation is a measure of linear dependence between two variables. It is common in academic literature to perform statistical tests for linear, continuous relationships among the variables since the study data are Likert-scaled, with end points of "strongly agree" to "strongly disagree."

**Research Question 1**: **To what extent is IT used as a strategic resource? How effective are efforts to use IT as a strategic resource?**

The question as to whether IT is a strategically important resource has generated many controversies in the past decade. Carr's (2003) publication of "IT Does not Matter" in the *Harvard Business Review* was a tipping point. Table A-1 (in Appendix) reveals that there is statistically significant correlation between the strategic importance of IT and the effective use of IT to manage IT projects (.348). Based on the survey Information Technology is regarded as being very important to the strategic success of their organization with an overall mean value of 3.89. As one might expect, there is a very significant correlation between perspectives on IT as being strategically important and the effectiveness of IT. However, there is a curious anomaly when examining the responses. For those respondents (Table 3) that did not view IT to be strategically Important (35.1%) over two-third of the respondents did not rate IT to be effective. Moreover, for those that viewed IT to be strategically important only 58% felt that IT was effective. Hence, the debate about the relevance of IT strategically continues.

The Nvivo analysis allowed us to identify key facilitating factors and constraints that either enabled or hindered companies in using IT strategically and effectively (see Table 3). On the positive side, nine key facilitating factors emerged from the qualitative coding process. For example, companies that reported both that IT was used strategically and the company was effective at harnessing IT reported that major investments were made in IT both for general systems as well as specifically in the areas of mobile device and cloud use. IT also brought internal and external data to connect staff with mission critical stakeholders. Strategic use of IT was not always linked with the effective use of IT, however. Constraints to using IT effectively include changes and delays in scope and project size, risk averse stakeholders, and other activities (e.g. security compliance) slowing down systems.

With respect to the industry categories respondents across most all industries rated IT to be of strategic importance. Only Government and Non-Profits rated IT Strategy to not be important. In terms of effectiveness, there was not a substantial variation in service industries *(professional services, energy, retail)* whereas *technology, consumer products, and manufacturing industries* had greater agreement that IT serves as a basis for competitive advantage and effectiveness. We can conclude that the relevance of IT strategically varies across industries.

| **IT Strategic** = Yes [64.9%] | |
|---|---|
| **IT Effective** | |
| Yes [57.5%] | No [42.5%] |
| ***Facilitating Factors*** | ***Constraints*** |
| Company made a major investment in IT | Lack of key IT resources, such as equipment and staff |
| Major investments made in mobile and cloud areas | Change takes too much time, training, and attention |
| Company able to maintain scale and cost | Security compliance slows implementation |
| Provided outside IT services | Key stakeholders are highly risk averse |
| Supply chain operates efficiently | Sense of complacency |
| IT harnessed to connect with mission critical people | Delays due to scope and size |

| **IT Strategic** = No [35.1%] | |
|---|---|
| **IT Effective** | |
| Yes [33.3%] | No [66.7%] |
| ***Facilitating Factors*** | ***Constraints*** |
| High commitment to providing mobile solutions to employees | Company believes IT is not a differentiator because all companies utilize it |
| Ample supply of contract IT workers | Industry regulation creates constraints |
| Company uses latest IT collaboration tools | Company believes IT plays only a supporting role |

Table 3. Comparison of IT Strategy with IT Effectiveness

With respect to the industry categories respondents across most all industries rated IT to be of strategic importance. Only Government and Non-Profits rated IT Strategy to not be important. In terms of effectiveness, there was not a substantial variation in service industries *(professional services, energy, retail)* whereas *technology, consumer products, and manufacturing industries* had greater agreement that IT serves as a basis for competitive advantage and effectiveness. We can conclude that the relevance of IT strategically varies across industries.

| Breakdown (within) | IT Strategic | |
|---|---|---|
| **Position** | No | Yes |
| 0-CIO (CTO, MIS,IT) | 50.0% | 55.3% |
| 1-CEO(Pres, Ex VP) | 21.7% | 14.1% |
| 2- Other | 28.3% | 30.6% |
| **Grand Total** | 35.1% | 64.9% |

| Breakdown (within) | IT Effective | |
|---|---|---|
| **Position** | No | Yes |
| 0-CIO (CTO, MIS,IT) | 46.8% | 59.4% |
| 1-CEO(Pres, Ex VP) | 21.0% | 13.0% |
| 2- Other | 32.3% | 27.5% |
| **Grand Total** | 47.3% | 52.7% |

| Breakdown (overall) | IT Strategic | |
|---|---|---|
| **Position** | No | Yes |
| 0-CIO (CTO, MIS,IT) | 17.6% | 35.9% |
| 1-CEO(Pres, Ex VP) | 7.6% | 9.2% |
| 2- Other | 9.9% | 19.8% |
| **Grand Total** | 35.1% | 64.9% |

| Breakdown (overall) | IT Effective | |
|---|---|---|
| **Position** | No | Yes |
| 0-CIO (CTO, MIS,IT) | 22.1% | 31.3% |
| 1-CEO(Pres, Ex VP) | 9.9% | 6.9% |
| 2- Other | 15.3% | 14.5% |
| **Grand Total** | 47.3% | 52.7% |

| **Position** | Overall |
|---|---|
| 0-CIO (CTO, MIS,IT) | 54.2% |
| 1-CEO(Pres, Ex VP) | 16.8% |
| 2- Other | 29.0% |
| **Grand Total** | 100.0% |

Table 4. Position Breakdown for IT Strategic and Effectiveness

From a job position standpoint (see Table A-3 in Appendix) there were slight differences in the means of the three position categories for IT being strategic. Table 4 depicts the breakdown for IT Strategic and IT Effectiveness in the position survey and the distribution for each preference. Of note though for those that regard

IT to be strategic (65%) only 53% felt IT be effective. The CIOs in contrast to the other two positions (CEO and other professionals) regarded the IT Effectiveness as much higher than the CEOs and Others. We can also conclude that the perception of IT as being strategic depends on the position within the organization.

*Given the various data, we can conclude that strategic IT is an important concern across most industries. However, there is not a strong link between effectiveness and competitive strategy for those that do not regard IT projects to be effective.*

**Research Question 2**: **To what extent are effective security policies related to the strategic use of IT?**

The correlation table in the Appendix reveals that there is a moderate statistically significant correlation (.216) between the strategic importance of IT and the security policies. The mean values for IT Strategy were 3.89, for IT being Effective was 3.55 and Security Policies 4.20. The relationship between IT effectiveness and Security Policies showed a somewhat moderately significant correlation (.178).

For those respondents (Table 5) that did not view IT to be strategically Important (35.1%) over eighty percent of the respondents felt Security policies was important. Moreover, for those that viewed IT to be strategically important over eighty-five percent felt that Security was important.

To further explore this data, we examined the qualitative data to identify clusters of security policies used and security weaknesses reported. These are shown in Table 5. For those companies that felt they used IT strategically and had effective security policies in place, the most common policies discussed were actively conducting vulnerability assessments and extensively training and educating employees on security issues. Common regarding security include lack of necessary IT tools to manage security issues, lack of training and education of employees regarding security, and delayed response to security threats.

| **IT Strategic** = Yes [64.9%] | |
|---|---|
| **Maintain Security** | |
| Yes [85.8%] | No [14.1%] |
| ***Security Policies Used*** | ***Security Weaknesses*** |
| Proactively conduct vulnerability assessments of IT systems | Lack of necessary IT tools regarding security |
| Extensively train and educate employees on secure use of IT | Lack of employee training around policies |
| Actively monitor IT use for breaches | Company is slow to respond to threats |
| Implement digital security measures (e.g. password protection, encryption, etc.) | Lack of employee education around policies |

| **IT Strategic** = No [35.1%] | |
|---|---|
| **Maintain Security** | |
| Yes [81.3%] | No [18.8%] |
| ***Security Policies Used*** | ***Security Weaknesses*** |
| Strongly control physical devices (e.g. disallowing USB keys) | Company has deficient and incomplete security policies |
| Train and educate employees on secure use of IT | Lack of employee education around policies |
| Actively monitor IT use for breaches | Slow to respond to security threats |

Table 5. Comparison of IT Strategy with Security

From a Position standpoint approximately 81% overall considered Security to be important. Of note, all positions rated Security policies as high. With respect to the industry categories respondents across all industries rated security measures to be very important (over 79%). Across industries there does not appear not to be substantial variation. *Given the various data, we can conclude that security is an important concern across all industries. However, there is not a strong link between security and IT.*

**Research Question 3: To what extent are effective mobile policies related to effective security policies?**

The correlation table A-1 in the Appendix reveals that there was a statistically significant correlation (.329) between mobile policies and security policies. The mean values for security were 4.20, and for Mobile Policies was 3.40. This was further substantiated in Table 6 where Security is rated as very important (81%) but

Mobile Computing was only rated as important by 63%. Curiously those that did not rate Security to be important (19%) over eighty percent rated Mobile Computing to be important. The relationship Mobile Policies and IT strategy did not have a significant correlation (.072).

| **Maintain Security**= Yes [81%] | |
|---|---|
| **Mobile Computing** | |
| Yes [63.3%] | No [36.6%] |
| ***Mobile Policies Used*** | ***Mobile Constraints*** |
| Extensive mobile device management policies created | Company lacks a mobile device management plan |
| Company tailors access, so that different employees have access to select data | Deep-seated concerns about how mobile will threaten security |
| Company likely to provide heavily controlled work mobile device | Company struggles with the tension between going mobile and balancing the expense involved |
| Company uses formal written agreements regarding mobile use | Company struggles with the rapid pace of technological change |

| **Maintain Security** = No [19%] | |
|---|---|
| **Mobile Computing** | |
| Yes [87%] | No [13%] |
| ***Mobile Policies Used*** | ***Mobile Constraints*** |
| Extensive mobile device management policies created | Company lacks a mobile device management plan |
| BYOD almost always allowed | Deep-seated concerns about how mobile will threaten security |
| Company provides mobile work device | Lack of necessary resources to go mobile |

Table 6. Comparison of Security with Mobile Policies

A qualitative assessment of responses regarding company mobile policies revealed several key themes around effective mobile policies and key constraints that limited companies' ability to harness mobile devices. These are shown in Table 6. Those companies is reporting high levels of effective mobile policy use, not surprisingly, commonly reported having detailed and comprehensive mobile device management plans in place that employees were well aware of. For those companies who were also effective in their use of security measures, we see evidence of policies that reflect a thoughtful implementation of mobile devices that include the use of formal written agreements that employees must sign as well as greater frequency in the deployment of heavily controlled company-provided mobile devices.

*Security is considered much more important than Mobile Computing. However, for those that do not rate Security to be important the majority rate Mobility to be important.*

## 5. CONCLUSIONS

This research provides insights into the potential differences and commonalities among organizations regarding IT as being strategic and effective—a competitive weapon and the impact of effective security and mobile device policies. The key findings of this study can be summarized as follows:

- *Strategic IT is an important concern across most industries. However, there is not as strong a link between effectiveness and competitive strategy for those that do not regard IT projects to be effective. Analysis of the qualitative data reveals that for those companies that harness IT strategically the main factor preventing effective use of IT is high levels of risk aversion and a sense of complacency. For those companies that does not harness IT strategically, key factors preventing effective IT use stem from a belief that IT cannot function as a differentiator and instead mainly plays a supportive role.*
- *Given the various data, we can conclude that security is an important concern across all industries. However, there is not a strong link between security and IT. Assessment of the qualitative data suggests that those who are effective at harnessing IT strategically and have effective security policies are those who are aggressively and proactively working to assess vulnerability to attack.*
- *Security is considered much more important than Mobile Computing. However, for those that do not rate Security to be important the majority rate Mobility to be important. Qualitative analysis of interview data also indicates that those companies that was highly effective in managing IT security were also those who were more likely to struggle with embracing change around mobile device use.*

There are a few potential limitations to this study. Interviews for this study were conducted primarily in one metropolitan city in the mid-western part of the United States. The perceptions of the respondents may not reflect the national or worldwide view of the subject matter. While interview subjects were granted assurances that results were confidential, there may be inherent bias in the results if respondents were reluctant to express criticism of the role of IT and the impact of security and the use of mobile devices in their organization. Despite these limitations, these findings provide an important foundation for future research on the research to develop models and analyze in a more complex and rigorous nature, the issues raised in this exploratory study.

## 6. REFERENCES

Accellion, Inc (2014). Mobile Data Security: Best Practices for Securing Your Mobile Workforce. An Accellion Whitepaper. Accellion, Inc, Palo Alto, CA.

Akella, Janaki, Brown, Brad, Gilbert, Greg and Lawrence Wong (2012), Mobility Disruption: A CO Perspective, McKinsey Quarterly: Insights & Publications, September, 2012.

Arandjelovic, Pedja Libby Bulin, and Naufal Khan (2015) Why CIOs should be business-strategy partners, McKinsey Quarterly Insights, February, 2015.

Campbell, Don (2009) Mobile Evolution Opens Doors to New Definitions of Work Place, CIO Magazine. January 2009.

Carr Nicholas G. (2004) In Praise of Walls. MIT Sloan Management Review April 15, 2004.

Carr, N.G. (2003). IT doesn't matter. *Harvard Business Review*, *81*(5), 41-49.

Desouza Kevin C. (2009) Securing information assets: The great information game. Business Information Review Vol 26(1): 35–41,SAGE Publications Los Angeles, London, New Delhi, Singapore and Washington DC, [DOI: 10.1177/0266382108101305].

Eddy, Nathan. (2015) BYOD Security Issues Cause Headaches for Employees, IT Pros. eWeek. http://www.eweek.com/security/byod-security-issues-cause-headaches-for-employees-it-pros.html.

Garglulo, Terence. The Ten Top Strategies for Managers of Mobile Workers. Making Stories. 2010.

Gartner Inc. (2011) Gartner's Top Predictions: For IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency. Gartner.com/predicts2011.

Gartner Inc. (2012). Gartner Says 821 Million Smart Devices Will Be Purchased Worldwide in 2012

Gartner, Inc. (2014) Information Security: Is your Information Security Program a Roadblock to Business Progress?. Gartner Webinar, http://www.gartner.com/technology/topics/information-security.jsp, Gartner Inc.

Harrell, G. D. (2002). Marketing: Connecting with customers (2nd ed.). Upper Saddle River, NJ.

IBM Institute for Business Value. *Leading through Connections.* IBM.com/ceostudy2012, IBM, 2012.

IBM Institute for Business Value. *Tne New Voice of the CIO.* ibm.com/iibv, IBM, 2010.

IBM MobileFirst (2015), http://www.ibm.com/mobilefirst/us/en/ Put your Business in Motion).

Legett, Kate (2015): Transform The Contact Center For Customer Service Excellence. Executive Overview: The Contact Centers For Customer Service Playbook June 3, 2015. |

Manyika, James and David Hunt. *Growth and renewal in the United States: Retooling America's economic engine.* McKinsey Global Institute, 2011.

Marquis, H. A. (2006) Finishing Off IT. Harvard Business Review. July 1, 2006.

McDonald, M. and Aron, D (2011) Reimagining IT: The CIO Agenda. Gartner Executive Programs.

McDowell. Making Mobility your Business Advantage. CIO Magazine. Customer Solutions Group, 2010.

Mobile Application Management (2015), Definitive Guide to Mobile Application Management | Apperian. https://www.apperian.com/mobile-application-management-gui.

Oliver, Mike. Mobility for Dummies. Sybase: A John Wiley and Sons, Ltd. Publication, 2010.

Sale, Nick. The way we will all work. Global Telecoms Business. London: Jul/Aug 2007. pg. 1.

Strassmann, P. A. (2003). Letters to the editor, Does IT matter? An HBR Debate. Harvard Business Review, 81(7), 7-9.

Suby, Michael (2014) Best Practice Security in a Cloud-Enabled World, Stratecast, Frost and Sullivan.

Symantec Endpoint Security Services (2015), Symantec Endpoint Global Services, Symantec Corp, Cupertino, CA.

Taft, Darryl (2015) IBM Study Shows Mobile App Developers Neglecting Security, eWeek (2015-03-21), http://www.eweek.com/developer/ibm-study-shows-mobile-app-developers-neglecting-security.html.

ZdNet (2015) Research: 74 percent using or adopting BYOD, (2015-09-29), http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod.

**Editor's Note:**

*This paper was selected for inclusion in the journal as a CONISAR 2015 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2015.*

# Appendices

| Correlation | IT Strategic | IT Effective | Security | Mobile |
|---|---|---|---|---|
| IT Strategic | 1 | | | |
| IT Effective | 0.348 | 1 | | |
| Security | 0.216 | 0.178 | 1 | |
| Mobile | 0.072 | 0.081 | 0.329 | 1 |

Table A-1. Correlations

| Category | Percent | IT Strategic | IT Effective | Security | Mobile |
|---|---|---|---|---|---|
| CONSPROD | 14.5% | 3.89 | 3.68 | 4.37 | 3.45 |
| Energy | 10.7% | 3.50 | 3.00 | 4.25 | 3.71 |
| FINSVC | 14.5% | 4.00 | 3.66 | 4.34 | 3.61 |
| Govt | 2.3% | 2.75 | 3.50 | 4.25 | 3.25 |
| Health | 16.8% | 3.95 | 3.59 | 4.14 | 3.32 |
| INSURANCE | 3.1% | 3.75 | 4.50 | 5.00 | 3.75 |
| MFG | 8.4% | 4.00 | 3.73 | 3.73 | 3.36 |
| NONPROFIT | 2.3% | 3.00 | 3.67 | 3.67 | 1.67 |
| Other | 5.3% | 4.00 | 3.33 | 3.50 | 3.17 |
| PROFSVC | 5.3% | 3.86 | 3.00 | 3.86 | 3.00 |
| Retail | 3.1% | 4.25 | 2.75 | 4.75 | 3.75 |
| Tech | 13.7% | 4.22 | 3.78 | 4.33 | 3.44 |
| Grand Total | 100% | **3.89** | **3.55** | **4.20** | **3.40** |

Table A-2 Mean Values by Category

| **Position** | Percent | IT Strategic | IT Effective | Security | Mobile |
|---|---|---|---|---|---|
| 0-CIO (CTO, MIS,IT) | 53.40% | 3.9 | 3.66 | 4.21 | 3.37 |
| 1-CEO(Pres, Ex VP) | 16.80% | 3.68 | 3.23 | 3.98 | 3.45 |
| 2- Other | 29.80% | 3.97 | 3.53 | 4.31 | 3.44 |
| **Grand Total** | 100% | **3.89** | **3.55** | **4.2** | **3.4** |

Table A-3 Mean Values by Position