Volume 8, Issue 2
October 2015
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 **EDSIG,** the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is currently semiannually. The first date of publication is 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.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

JISAR Editorial Board

Identifying User Behavior from Residual Data in Cloud-based Synchronized Apps

George Grispos
g.grispos.1@research.gla.ac.uk
University of Glasgow
United Kingdom

William Bradley Glisson
bglisson@southalabama.edu
University of South Alabama
Mobile, AL, USA

J. Harold Pardue
hpardue@southalabama.edu
University of South Alabama
Mobile, AL, USA

Mike Dickson
michael.dickson@scotland.pnn.police.uk
Police Scotland
United Kingdom

Abstract

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. Although security and forensic researchers have been able to recover a variety of artifacts, empirical research has not examined a suite of application artifacts from the perspective of high-level pattern identification. This research presents a preliminary investigation into the idea that residual artifacts generated by cloud-based synchronized applications can be used to identify broad user behavior patterns. To accomplish this, the researchers conducted a single-case, pretest-posttest, quasi experiment using a smartphone device and a suite of Google mobile applications. The contribution of this paper is two-fold. First, it provides a proof of concept of the extent to which residual data from cloud-based synchronized applications can be used to broadly identify user behavior patterns from device data patterns. Second, it highlights the need for security controls to prevent and manage information flow between BYOD mobile devices and cloud synchronization services.

Keywords: Residual Data, Cloud, Apps, Digital Forensics, BYOD.

1. INTRODUCTION

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

Hence, organizations are investigating various ideas to extend existing information technology infrastructures to include mobile devices (Scheepers & Scheepers, 2004). One possible solution is the implementation of a Bring Your Own Device (BYOD) program. BYOD programs potentially offer several benefits that include an increased level of productivity, mobile device procurement and maintenance cost reduction, increased workforce mobility, location flexibility, increased accessibility and longer working hours (Copeland & Crespi, 2012; Scarfo, 2012).
In addition to corporate environments, governments are embracing BYOD programs. Forrester Research (2012) found that 59% of smartphones connected to various government networks were personally-owned devices. TrendMicro (2012) reports that security vulnerabilities found in legitimate smartphone applications can make the extraction of personal and corporate data much easier for cybercriminals. Hence, there are growing concerns that the amount of business and personal information collected by mobile applications could lead to increased end-user profiling (Cleff, 2007). These concerns prompted the research question:

Is it possible to recover residual data from a reset, resynchronized mobile device running a suite of cloud-based synchronized apps to identify the device user's daily behavioral patterns, social activities, and relationships with other individuals?

The contribution of answering this question is two-fold. First, it provides a proof of concept that data recovered from cloud-based synchronized applications on a reset, resynchronized mobile device can be used to identify user behavior patterns. Second, it highlights the need for security controls to prevent and manage information flow between BYOD mobile devices and cloud synchronization services.

The paper is structured as follows: Section two discusses related work concerning smartphone security and privacy. Section three presents the methodology and summarizes recovered artifacts. Section four discusses the results. Section five draws conclusions and presents future work.

2. RELATED WORK

Smartphone privacy and security have attracted considerable attention from various aspects of academia. Researchers have used a number of methods to assess and understand the risks associated with storing personal information on these devices. Warden and Allen (2011) demonstrated how Apple mobile devices collected and stored location information such as mobile cell towers and Wi-Fi access points. Although no personal information was being recorded, Warden and Allen (2011) argued that should an Apple mobile device be stolen and jail-broken, cybercriminals could easily access and identify previous device owner whereabouts.

The security and privacy of Android devices and applications have also come under scrutiny. TaintDroid (Enck, Gilbert, Chun, Cox, Jung, McDaniel, & Sheth, 2010) was developed to dynamically track the flow of private information through third-party applications installed on an Android device. Enck, et al. (2010) tested thirty random applications with the primary objective of analyzing data leakage from both a privacy and a security perspective. Over one-half the tested applications were reported to be transmitting user location and device information to remote services. Similarly, Gibler, et al. (2012) presented AndroidLeaks which performed a static analysis of code to identify data leakage from Android applications. A third of the 24,000 applications tested were found to store and leak private information such as the device location, Wi-Fi data and audio conversations. Although the authors of TaintDroid and AndroidLeaks have highlighted the amount of personal information being stored and leaked by Android applications, neither author's research focused on assimilating collected information to establish data patterns.

The literature indicates that many researchers focus on the impact of mobile privacy and security from the perspective of individuals and not from the perspective of an organization (Glisson & Storer, 2013). Glisson and Storer (2013) did investigate mobile devices from an

organizational privacy and security viewpoint. In terms of organizational security, mobile devices which utilize location and cloud synchronization services are at risk for targeted attacks and can introduce the potential for data leakage within an organization (Grispos, Glisson, & Storer, 2013; Keyes, 2013). Keyes (2013) indicates there is the potential for attackers to use location services to determine where the device owner is located at a specific time, to correlate this information with other sources, to establish associates and provide an indication of the kinds of activities performed in specific locations. However, Keyes does not elaborate on how this information can be extracted by attackers or evaluate any methods for performing this attack.

Miller, et. al., (2012) notes that in a BYOD scenario location, and synchronization services can complicate security issues for an organization. Grispos, et al., (2013) highlighted the technical opportunities for accessing data stored on cloud synchronization services, such as Box, via residual data stored on a mobile device. In corporate environments, the literature identifies security issues related to BYOD solutions as originating from a lack of end-user device controls coupled with a blurring of the distinction between personal and work-related data (Glisson & Storer, 2013; Scarfo, 2012).

Harris, et. al., (2013) conducted a survey with college students, who were about to enter the workforce, to determine their attitudes towards BYOD security. The results from the survey indicated that there is a lack of security awareness from the participants towards BYOD. Twenty percent of the participants admitted that they 'root' or 'jailbreak' their mobile device, potentially creating a major security risk for organizations that would accept these devices on their networks (Harris, et al., 2013). Although researchers have highlighted the security risks of mobile applications in a BYOD context, empirical research has not examined a suite of application artifacts from the perspective of device data pattern identification.

3. METHODOLOGY

In order to test the research question of this study, two hypotheses were formulated.

H1: Residual data can be recovered from a reset, resynchronized smartphone device that is using cloud-based synchronized applications.

H2: Residual data recovered from a reset, resynchronized smartphone is sufficient to correlate device data patterns with known device user behavior patterns.

For the purpose of this research, user behavior patterns are broadly defined as an individual's daily behavioral characteristics, social activities and relationships with other individuals using electronic devices.

Experimental Design

The experimental design employed in this study is the Single Case Pretest-Posttest Quasi Experiment (Campbell & Stanley, 1963). The primary characteristic of a quasi-experiment is the lack of randomization. In a single case design, there is one subject (in this case a smartphone device) that undergoes a measurement, a treatment, and a measurement (O1 X O2) or pretest-treatment-posttest.
The smartphone device used in the pretest-posttest quasi experiment is an HTC One X with 3G data services. An HTC Desire was used in the post-hoc experiment to measure residual data captured from a secondary device. Table 1 – Smartphone device features, highlights the notable features of these devices. The two smartphones selected in this experiment were chosen for their operating systems. The Operating System (OS) for the HTC One X was a recent version at the time of the experiment. This created compatibility issues with 'push-button' forensics solutions. Lack of compatibility forces investigators to use more traditional software development tools. The OS for the HTC Desire represents an older version of Android that is compatible with 'push-button' solutions. This allows for an initial assessment of the output from each approach.

Feature	HTC One X	HTC Desire
Operating System	Android 4.0 (Ice Cream)	Android 2.1 (Éclair)
RAM	1 GB	567 MB
Internal Memory	32 GB Storage	512 MB ROM
Memory Card	No (Virtual SD Card)	Yes (4 GB)

Table 1. Smartphone Device Features

It should be noted that the scope of the quasi experiment was limited in the following ways. The HTC One X smartphone was rooted prior to being used. This experiment was conducted in the United Kingdom using Global System of

Mobile Communications technology. The experiment focused on a specific version of the Android operating system and specific versions of Google applications. The HTC One X solely utilized the Android Debug Bridge for data extraction. The password for the resynchronized smartphone is presumed to be known. The password to the account is not the focus or the research. This is due to legislation that requires suspects to provide this password and encryption information like the Regulation of Investigatory Powers Act of 2000 in the United Kingdom (UK Parliament, 2000) and companies retaining ownership and rights to devices. The emphasis on passwords is further diminished when considered in conjunction with individuals commonly reusing small sets of passwords and current research into resolving this information (Das, Bonneau, Caesar, Borisov, & Wang, 2014; Stobert, 2014).

The applications included in this experiment were official Google applications that are compatible with the Android operating system v4.0. The Google applications selected for inclusion in this experiment are: Google+ (version 4.0.0.46852618); Google Search (version 1.4.1.278776); Google Calendar (version 201305280); Google Tracks (version 2.0.4); Google Maps (version 6.14.4); Google Drive (version 1.2.182.26); Google Keep (version 1.0.79); and Gmail (version 4.3.1).

It is submitted that the phone used in this experiment is representative of all phones of identical make, model, and configuration. The O1 instance of our design serves as the experimental "control" and is referred to as "Image 1". Image 1 contains the forensically recovered residual data prior to the treatment, the pretest. The treatment is a hard-reset of the device, formatting of the memory card, and a re-synch of the device with the cloud-based apps. The posttest is the recovery of residual data after the treatment and is referred to as "Image 2". Consistent with our research question and hypotheses, the posttest examines the casual impact of the treatment (X) on the amount of forensically recoverable data on the device (O1). A post-hoc forensics test was conducted on a secondary device not included in the control (O1). The results of this test are referred to as "Image 3".

Pretest

The following steps describe how the device was tested for residual data prior to treatment. The residual data forensically recovered from the device serves as the control or baseline against which the posttest results were compared.

1. The HTC One X smartphone's boot-loader was unlocked using the steps on the HTC website (2013) and then the device was 'rooted' using a method described on the CNET website (Griffin, 2012).
2. A desktop computer was used to create a Google account.
3. After the Google account was created, Google contacts were accessed through a desktop web browser to store information for fifteen individuals. The contact information included: first name, last name, mobile phone number and email address.
4. The smartphone device was powered on and the Google account was used to sign-on to Google Services during the initial device setup. An automatic sync with the Google Cloud and the option to allow Google to use location services were also selected during the setup. The device was then configured to use the 3G data services to gain access to the Internet.
5. After the device setup was completed, the Google applications were downloaded and installed using the default installation parameters from the Google Play market.
6. The applications were executed and the test account was used to sign-in to various Google services.
7. Applications were used over a two-week period. Table 2 – Daily Activities presents the activities performed and when they were specifically repeated for each application. Table 3 – Other Activities defines application activities performed on varied days and at varied times. A total of 212 activities were performed using the device which included 58 activities from Table 2 – Daily Activities and 154 activities from Table 3 – Other Activities.
8. Upon completion of the two week period, artifacts associated with the suite of Google applications were extracted using Android Debug Bridge (ADB). USB debugging was activated on the device and the ADB was used to access the shell command prompt. The Android OS traditionally stores application-related artifacts in the /data/data folder on the User partition (Hoog, 2011). The contents of this folder were copied to a folder on the virtual memory card using the ADB. The virtual memory card was accessed using a write blocker via a desktop computer

and a forensic image (Image 1) was created using FTK Imager (AccessData, 2008).

Occurrence	Activity	Activity Count
Monday – Friday 9am-10:30am	Google+ Check-in: Kelvin Hall Subway – "Off to Work"	10
Monday – Friday 10am-11:30am	Google Search: "Starbucks Near Me" and Check-in: "Starbucks Coffee"	20
Monday – Friday 6pm-8pm	Check-in, Google Tracks: Go for a jog along either University Avenue or Kelvin Way (alternative days) to Home	10
Tuesday or Friday 8pm-9pm	Google Search, Check-in: Chinese or Indian Restaurant	4
Monday – Friday 11am-12pm	Google Search: "What's the weather like tomorrow?"	10
Saturday and Sunday 9am-11am	Google+ Check-in: "At home"	4
Total Daily Activities		**58**

Table 2. Daily Activities

Treatment
The treatment involved the three-step process described below.

1. The HTC One X device was hard-reset and the virtual memory card formatted.
2. The HTC One X device was powered on and the artifact collection process, described in Step 8, was repeated to create a copy of the /data/data folder on the device. This step was implemented to verify that data, related to the Google applications, was no longer on the device.
3. The test account was then used to sign-in to Google services and the applications used in the experiment were reinstalled. The HTC One X device and the applications were allowed to synchronize with the Google Cloud.

Posttest
The purpose of the posttest is to measure the degree to which re-synchronizing a wiped reset device (O2) to the cloud-based apps results in recoverable residual data. Image 2 was produced by repeating the process described in Step 8.

Post-hoc Test

Application	Activity	Activity Count
Google+	Posted message on wall; posted on friend's wall; friends posted on wall; sent and received messages; check-in locations; joined, viewed Google+ communities; deleted wall posts, check-ins, messages and left communities.	81
Google+ Hangouts	Conducted a 'Hangout'	8
Google Search	Performed searches using typed and voice features.	10
Google Calendar	Added and deleted entries to calendar.	7
Google Tracks	'Tracked' jogging activities.	4
Google Maps	Requested directions to locations; used Navigation feature for travel.	15
Google Drive	Saved two XLSX spreadsheet files, two PDF files, and two JPEG images to Drive; deleted PDF files after viewing on the device.	6
Google Keep	Saved and deleted Notes.	11
Gmail	Sent and received emails.	12
Total Other Activities		**154**

Table 3. Other Activities

A post-hoc test was conducted on O1, independent of the influence of the treatment (X), by introducing a secondary device. The purpose was to test the degree to which it was possible to recover residual data from O1 with a

secondary device while the O1 device was still connected to the cloud-based apps.

The secondary device, an HTC Desire smartphone, was used to sign-in to the Google account using Google services and the applications used in the experiment were installed. This device was allowed to synchronize with the data stored in the Google Cloud. After the synchronization was completed, this device was processed using Cellebrite UFED (version 1.8.5.0). The result of this processing was Image 3. All three forensic images were examined using Physical Analyzer (version 3.7.0.352) and AccessData Forensic Toolkit 4.

Artifacts related to the pretest activities performed using the Google applications listed in Table 2 – Daily activities, were all recovered from Image 1 (O1). All of these artifacts contained timestamp information which matched the date and time the activity took place. The artifacts recovered included Google+ check-in information, posts and messages, as well as Google Search results. One hundred and fifteen (74.6%) out of the 154 artifacts related to the activities in Table 3 – Other activities were also recovered from Image 1.

4. ARTIFACTS RECOVERED

It is interesting to note that no artifacts related to Google+ Hangouts were recovered from Image 1. In addition, events or files which were deleted during the experiment were also not recovered from the device. A total of 173 (81.6%) out of 212 activities were found on Image 1. In addition, all fifteen contacts stored in the Google Cloud were also recovered.

The posttest results show that after the HTC One X was hard-reset to factory settings and then re-synched with the Google Cloud, a total of 83 (39%) out of 212 activity artifacts were recovered from Image 2 (O2). The artifacts recovered included 35 artifacts (60%) from Table 2 and 48 artifacts (31%) from Table 3. All fifteen contacts stored in the Google Cloud were recovered from Image 2.

In the post-hoc test, artifacts related to the Google applications were recovered from the HTC Desire which was synchronized with the Google account. In total, 84 (39.6%) out of 212 activity artifacts were recovered from Image 3. The artifacts recovered included 36 (62%) out of 58 from Table 2 and 48 (31%) out of 154 from Table 3. Although the number of artifacts recovered from the Desire and the HTC One X after the resynchronization are similar, different artifacts were recovered from each device. For example, no Google Keep artifacts were recovered from the HTC Desire but they were recovered from the second image of the HTC One X. All fifteen contacts stored in the Google Cloud were recovered from Image 3.

Table 4 – Activity Artifacts Recovered summarizes the number of artifacts recovered from each device image for the pretest, posttest, and post-hoc test, as well as providing examples of metadata recovered from each application. This table is available in the appendix.

5. DISCUSSION

The results of this quasi-experiment are discussed from three perspectives: digital forensics; Bring Your Own Device (BYOD); and high-level device data patterns.

Digital Forensics

The Google artifacts recovered from the device can be used to either confirm or refute the events already discovered from other sources or storage media. Therefore, the evidence recovered from the Google applications can be used to validate or refute a portion of the device owner's social behavior. Furthermore, the Google artifacts recovered can also be correlated with physical evidence to link individuals to certain events, for example, using the check-in data recovered from Google+ with CCTV footage from the related area (Carrier & Spafford, 2003). From an investigative perspective, there is the potential to use the artifacts recovered to develop social relationship profiles of suspects.

Voigt, et al. (2013) reported how law enforcement agencies in Germany are using social networking sites such as Facebook and Google+ to locate personal information and social relationship profiles of suspects. This usually involves police officers befriending suspects on the social network using 'fake' accounts and then examining the social life of the person in question (Voigt, et al., 2013).

Alternatively, law enforcement agencies have also used a social network 'crawler' to identify and analyze these relationships (Voigt, et al., 2013). Although these approaches have not been declared illegal, Voigt, et al. state that evidence gathered using these methods may be inadmissible as evidence in court (Voigt, et al.,

2013). The Google artifacts recovered from the experiment in this paper could be considered as an alternative source by law enforcement to identify a suspect's social relationship with other individuals. The Google+ check-ins, posts, messages and pictures, as well as Gmail messages and Google Map locations could all be used to provide investigators with a more complete representation of activities.

BYOD

The implementation of BYOD programs in an organization leads to a potential situation where the boundaries become increasingly blurred between personal and corporate data. In a BYOD environment it is plausible that a personally-owned device could be accessing corporate data while interacting with cloud synchronization services (Morrow, 2012). This presents an opportunity for a malicious insider to use these services to steal corporate data and save it in cloud storage services such as Dropbox (Morrow, 2012). This scenario recently resulted in IBM restricting its workforce from using cloud services, as well as Siri, Apple's personal assistant (Leyden, 2012). The results of this experiment further highlight the potential risk that cloud synchronization applications can introduce to an organization in a BYOD context.

The experiment's results demonstrated that application information is synchronized and stored offsite. When the HTC One X was reset to factory settings, the Google applications were reinstalled and synchronized with the Google Cloud. A total of 83 activity artifacts were restored to the device and recovered from Image 2. This represents nearly 48% of the activity artifacts which were recovered from Image 1. Furthermore, this information was only secured by a single username and password. The recent attacks on Google (Fletcher, 2010) and Evernote (Forbes Online, 2013), have highlighted that single-sign-on systems can further complicate BYOD scenarios for corporate organizations.

Another threat identified in the post-hoc test is the potential for an attacker to hijack a specific account without the user being aware they are under attack. When a second device, an HTC Desire was synchronized with the same credentials as those on the HTC One X, the device could be used to access all the information stored in the Google Cloud while it was still accessible from the One X. There was no notification from Google that an additional device was accessing the experimental data set. This could lead to the following scenarios:

- Corporate information could be compromised from a 'piggy-back device'. The organization and device owner may be unaware this has occurred; or
- A victim could use a secondary device primarily used by another individual such as a spouse or family member to access corporate information. The secondary device, if stolen or compromised could expose residual data to attack; or
- A victim could be locked out of his/her account causing the device to no longer synchronize with the Google Cloud.

The results of the experiment coupled with these scenarios highlight challenges associated with the management and protection of corporate data.

Pattern Development

Mobile location-based services are predominantly used to determine where a mobile device user is located. These services are used to not only tell the device user where and how to get to their destination, but also to disclose which friends are nearby, what the weather forecast is and what places of interest are located nearby (Vaughan-Nichols, 2009). The problem arises when this location information is integrated with personal or business information.

Google currently requires users to sign-in to their Google accounts to use any smartphone application, Gmail and any other Google service (Bauer, Bravo-Lillo, Fragkaki, & Melicher, 2013). Google can, potentially, assimilate data about an individual's habits using any of their services with their activities on Google+. This integration of information can be dangerous from a high-level pattern recognition perspective, particularly in corporate environments.

However, the amount of information stored in Google applications is of greater concern when lost and/or stolen mobile devices, such as smartphones, can be used in social engineering attacks against an organization (Friedman & Hoffman, 2008; Landman, 2010; Weippl, Holzinger, & Tjoa, 2006). Should a device which has been used for both work and personal use be lost or stolen, there is the potential for the device to be 'rooted' and the data on the device used for a social engineering attack.

The artifacts recovered from the pretest and posttest images, in relation to the activities in

Table 2 – Daily activities and Table 3 – Other activities, indicate that this data can be used to establish high-level device data patterns. All of the artifacts from Table 2 and 74% of the artifacts from Table 3 were recovered from the pretest image, while 60% of the artifacts from Table 2 and 31% of the artifacts from Table 3 were recovered from the posttest image. The recovery and clustering of timestamps for the activities presented in Table 2 suggests that it may be possible to identify high-level blocks of time when an individual is typically engaged in some activity. This type of information can be valuable to a social engineering attacker who would like to know when the device owner may be away from his/her workstation or office. The results from Image 2 (posttest) also indicate that a substantial portion of this data is being stored in the cloud. The synchronization of a device, with no personal data, with the Google Cloud retrieved nearly 48% of the activity artifacts which were recovered from Image 1.

6. CONCLUSIONS AND FUTURE WORK

The results of the quasi experiment described in this paper provide preliminary support for both hypothesis 1 and 2. Substantial residual data of known user activities were recovered from the pretest and posttests, 81% and 39% respectively. The post-hoc test also resulted in a recovery of 39% of known user behaviors.

This initial investigation provides a proof of concept that known user behavior can be correlated with high-level device data patterns based on data generated from a smartphone using cloud-based synchronized apps. The clustering of the timestamps for the activities presented in Table 2 indicates high-level data patterns are identifiable. The research also indicates that a substantial portion of this data is being stored in the cloud. The synchronization of a device with no personal data with the Google Cloud retrieved 83 activity artifacts. This represents nearly 48% of the activity artifacts which were recovered from Image 1. This finding reinforces the need to investigate security controls to be able to prevent or manage information flow between BYOD mobile devices and cloud synchronization services. The experiment also highlights a potential hijacking opportunity. A secondary device can be used to login to the Google Cloud and synchronized without the victim being aware or notified that this action has occurred.

This study provides a foundation for expanded, richer, more extensive and real-world based datasets for individuals and organizations. The data raises additional questions about the discrepancies between data extraction methods like the android debug bridge and the Cellebrite extraction tool. These inconsistencies should be examined in future studies.

Future research will investigate the introduction of mobile devices into real-world environments in order to track, visualize and compare algorithms designed to de-couple business and personal data. The idea is not only to be able to look backward at the static residual data on the device to develop detailed device profiles but to be able to investigate effective ways to link individuals to specific device behavior. The ultimate goal is to develop algorithms that can link devices to individuals and predict future behavior with a high degree of certainty. Success in this area could have positive implications in minimizing the current risk associated with BYOD solutions in organizations. Detailed activity profiles created from the algorithms could be used to alert security personnel to a suspicious activity. The establishment of metrics to determine an organizations' comfort level with an employee's mobile device activities could provide insight into potential security issues and, potentially, mitigate BYOD concerns for organizations. In addition, future work will expand the experiment to include a variety of smartphones and Operating Systems (OS). The focus is to evaluate pattern identification and validation across multiple devices and OSs.

7. REFERENCES

AccessData. (2008). Forensic Toolkit, from http://www.accessdata.com/

Allan, A., & Warden, P. (2011). Got an iPhone or 3G iPad? Apple is recording your moves, from http://radar.oreilly.com/2011/04/apple-location-tracking.html

Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. (2013). *A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality.* Paper presented at the 2013 ACM workshop on Digital identity management.

Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi-experimental designs for research*: Houghton Mifflin Boston.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1-20.

Cleff, E. B. (2007). *Privacy issues in mobile advertising*. Paper presented at the BILETA 22nd Annual Conference.

Copeland, R., & Crespi, N. (2012). *Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules*. Paper presented at the 16th International Conference on Intelligence in Next Generation Networks.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). *The Tangled Web of Password Reuse*. Paper presented at the Network and Distributed System Security Symposium, San Diego, CA. https://security.cs.princeton.edu/publications/

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2010). *TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones*. Paper presented at the 9th USENIX conference on Operating systems design and implementation.

Fletcher, O. (2010). Google Attack Targeted 'Gaia' Password System, from http://www.pcworld.com/article/194557/article.html

Forbes Online. (2013). Evernote joins the notably hackable club, from http://www.theregister.co.uk/2013/03/04/evernote_password_reset/

Forrester Research. (2012). BYOD in Government: Prepare For The Rising Tide.

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information, knowledge, systems management, 7*(1), 159-180.

Gartner. (2012). Gartner Says 821 Million Smart Devices Will Be Purchased Worldwide in 2012, from http://www.gartner.com/newsroom/id/2227215

Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012). Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale *Trust and Trustworthy Computing* (pp. 291-307): Springer.

Glisson, W. B., & Storer, T. (2013). *Investigating Information Security Risks of Mobile Device Use within Organizations*. Paper presented at the The 19th Americas Conference on Information Systems (AMCIS), Chicago.

Griffin, B. (2012). How to root the HTC One X, from http://reviews.cnet.co.uk/mobile-phones/how-to-root-the-htc-one-x-50010022/

Grispos, G., Glisson, W. B., & Storer, T. (2013). *Using smartphones as a proxy for forensic evidence contained in cloud storage services*. Paper presented at the 46th Hawaii International Conference on System Sciences, Maui, Hawaii.

Harris, M. A., Patten, K., & Regan, E. (2013). *The Need for BYOD Mobile Device Security Awareness and Training*. Paper presented at the The 19th Americas Conference on Information Systems (AMCIS), Chicago.

Hoog, A. (2011). *Android Forensics - Investigation, Analysis and Mobile Security for Google Android* Syngress.

HTC. (2013). Unlock Bootloader, from http://www.htcdev.com/bootloader/faq

Keyes, J. (2013). *Bring Your Own Devices (BYOD) Survival Guide*: CRC Press.

Landman, M. (2010). *Managing smart phone security risks*. Paper presented at the 2010 Information Security Curriculum Development Conference.

Leyden, J. (2012). IBM bans Dropbox, Siri and rival cloud tech at work, from http://www.theregister.co.uk/2012/05/25/ibm_bans_dropbox_siri/

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and Privacy Considerations. *IT Professional, 14*(5), 53-55.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security, 2012*(12), 5-8.

Scarfo, A. (2012). *New Security Perspectives around BYOD*. Paper presented at the Seventh International Conference on Broadband, Wireless Computing, Communication & Applications.

Scheepers, H., & Scheepers, R. (2004). *The implementation of mobile technology in organizations: expanding individual use contexts*. Paper presented at the 25th International Conference on Information Systems, Washington DC.

Stobert, E. (2014). *The agony of passwords: can we learn from user coping strategies?* Paper presented at the CHI '14 Extended Abstracts on Human Factors in Computing Systems, Toronto, Ontario, Canada.

TrendMicro. (2012). *Security in the Age of Mobility*.

UK Parliament. (2000, December 8, 2000). Regulation of Investigatory Powers Act 2000 Retrieved May 7, 2014, from http://www.legislation.gov.uk/ukpga/2000/23/contents

Vaughan-Nichols, S. J. (2009). Will Mobile Computing's Future Be Location, Location, Location? *Computer, 42*(2), 14-17. doi: 10.1109/MC.2009.65

Voigt, S., Hinz, O., & Jansen, N. (2013). *Law enforcement 2.0: the potential and the (legal) restrictions of Facebook data for police tracing and investigation*. Paper presented at the 21st European Conference on Information Systems, Utrecht.

Weippl, E., Holzinger, A., & Tjoa, A. M. (2006). Security aspects of ubiquitous computing in health care. *Elektrotechnik und Informationstechnik, 123*(4), 156-161.

Editor's Note:

This paper was selected for inclusion in the journal as a CONISAR 2014 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 2014.

APPENDIX

Application (Real Activity Count)	Metadata Recovered	Pretest (Image 1)	Post-test (Image 2)	Post-hoc (Image 3)
Google+ Activities (105)	Timestamps; wall posts; comments; check-in and geo-location points; community feeds and conversations; private messages sent and received; message author information.	88	50	47
Google+ Hangouts (8)	-	0	0	0
Google Search (34)	Timestamps; search terms, Google URL; and number of visits.	34	0	0
Google Calendar (7)	Appointment: title, location, start and end time and creation date and time.	4	4	4
Google Tracks (14)	Timestamps; geo-location points; journey coordinates; and Keyhole Markup Language files.	14	14	13
Google Maps (15)	Destination information requested; longitude and latitude coordinates; and request time.	12	0	5
Google Drive (6)	Timestamps; Favorite files; storage service metadata; files viewed on the device and saved for offline viewing.	6	0	6
Google Keep (11)	Notes created; creation and last modified times.	5	5	0
Gmail (12)	Email body and subject; sent and received email addresses; email sent/received date and time.	10	10	9
Total (212)		**173**	**83**	**84**

Table 4. Activity Artifacts Recovered

ERP Customization vs. Business Process Reengineering: Technical and Functional Perceptions

Meg Fryling
mfryling@siena.edu
Computer Science
Siena College
Loudonville, NY 12211, USA

Abstract

Information system failures and cost overruns have plagued organizations for decades. In order to take full advantage of Enterprise Resource Planning (ERP) systems, implementations require drastic structural and cultural changes within the organization including business process reevaluation and reengineering. These changes are difficult to accomplish and organizations continue to struggle with change management of ERP systems. Stakeholder involvement and perceptions regarding the ERP system change over time. Understanding evolving perceptions may lead to improved long-term ERP system management and reduced costs. The purpose of this research is to gain dynamic insight into the software project management of pre-packaged enterprise-wide information systems (i.e. ERP). This study uses system dynamics modeling together with interviews of ERP project members to better understand the technical and functional perceptions regarding customization versus business process reengineering to satisfy functionality gaps.

Keywords: ERP, System Dynamics, Business Process Reengineering, Enterprise Resource Planning, Customization, Total Cost of Ownership

1. INTRODUCTION

Enterprise Resource Planning (ERP) information systems emerged during the 1990s as a cross-functional enterprise-wide information system solution. ERP systems integrate data and processes from disparate organizational departments into a single information system (Dodds & Spencer, 2007; Rashid, 2005; Sammon & Adam, 2005). This vast integration is intended to improve data access, data accuracy and workflow as well as to enhance efficiency, agility and responsiveness (Sammon & Adam, 2005). ERP systems were initially intended for large industrial companies but are now implemented by a wide variety of organizations, including higher education institutions. A key piece of ERP integration is the use of a single database and multiple software modules covering various departmental business functions. ERP implementations force the merger of disparate organizational data and functions (Dodds & Spencer, 2007; Rashid, 2005; Sammon & Adam, 2005). This enterprise-wide integration of diverse departments is what makes ERPs more complex and larger in scope than traditional software packages (Brehm, Heinzl, & Markus, 2001; O'Brien & Marakas, 2006). This complexity is due to the underlying business processes embedded in ERP systems (Bansal & Negi, 2008). Therefore, ERP systems require vigilant change management to implement successfully (Dong, 2000; Somers & Nelson, 2001).

Issues related specifically to the implementation of traditional pre-packaged ("off-the-shelf") information systems have overwhelmed

organizations since the 70s, decades before the emergence of ERP systems. As McNeil discussed in 1979, the fact that both user requirements and vendor offerings are constantly fluctuating and evolving; making the proper management of pre-packaged information systems nearly impossible. There are unique challenges associated with implementing these types of information systems. Organizations have little control over the quality of "off-the-shelf" information system functionality and are at the mercy of vendors who make software improvements based on their strategic internal policies and not necessarily customer needs (McNeil, 1979). While customers can certainly make desired software modifications themselves, vendors typically deny software enhancement request due to the high development and maintenance costs (Brehm et al., 2001). Often the software as delivered does not fully meet the needs of the organization so frequent changes (customizations) and extensive maintenance are required (McNeil, 1979). Organizations can choose to have custom software built to meet their unique requirements but this imposes additional costs, risks, and implementation delays (Brehm et al., 2001; Fryling, 2010).

ERP systems differ from traditional software packages because they are neither "custom-built" nor "off-the-shelf" (Brehm et al., 2001, p. 2). ERP systems are, in theory, designed based on industry best practices and are intended to meet the needs of all similar organizations (Kumar & Van Hillegersberg, 2000). Since ERPs are developed to meet the needs of a variety of institutions, they are inherently generic and often reflect the vendor's perception of best practices; these will likely contradict many of the implementing organization's notions of best practices (Crumbly & Fryling, 2012; Dong, 2000; Orlikowski, 2002). This is further complicated by the integrated nature of ERP. In the pre-ERP environment functional offices could work fairly autonomously and developed specialized unit business practices (Frantz, Southerland, & Johnson, 2002); hence, technology-wise they were decentralized. Pre-ERP information system implementations did not require cross-functional collaboration and in fact necessitated little functional user involvement at all; they were principally IT initiatives (Frantz et al., 2002).
While ERP systems are generic in nature, they do have some flexibility built in and are configurable to meet some of the specific requirements of each institution. This configuration is not technical in nature but requires functional business process expertise. Therefore, implementation requires technical and functional communication, collaboration, and active project participation. "Because ERP software has to be implemented rather than simply installed, it requires a paradigm shift for most functional users" (Frantz et al., 2002, p. 40). "ERP implementations usually require people to create new work relationships, share information…, and make business decisions they were never required to make" (Appleton, 1997, p. 52). Often it is the case that in the pre-ERP environment there were more efficient ways to do business that were simply impossible with disparate information systems. For example, in a higher education environment without ERP the financial aid office must wait for nightly interfaces to run in order to make decisions regarding a student's financial aid eligibility. With an ERP the financial aid staff can access student account and student records information in real time; thus, improving customer service. These improved business practices can be exploited with ERP only if functional and technical project stakeholders communicate and collaborate effectively.

The major challenge for the organization implementing an ERP is instituting a major paradigm shift for executive leadership. "CFOs approach business processes from a practical orientation, whereas CIOs tend to be more technically oriented" (Frantz et al., 2002, p. 40). "ERP systems are really about closely integrating different business functions; this is what sets them apart from many other IT efforts" (Akkermans & van Helden, 2002, p. 36). This tight integration provides an information system with increased access to real-time data and a significant reduction of data redundancy, yet those same benefits impose significant complexity. The complex design of ERP systems makes them difficult to understand, implement and modify (Dodds & Spencer, 2007).

Information system failures and cost overruns have plagued organizations for decades (Peterson, 2003; Tapp, Hesseldenz, & Kelley, 2003). In order to take full advantage of ERP systems, ERP implementations require drastic structural and cultural changes within the organization including business process reevaluation and reengineering. These changes are difficult to accomplish and organizations continue to struggle with change management of ERP systems.

ERP implementations have distinct phases. Each of these phases involve a variety of stakeholders, with different levels of perceived understanding (Besson & Rowe, 2001). Stakeholder involvement and perceptions regarding the ERP system change over time (Besson & Rowe, 2001). Understanding evolving perceptions may lead to improved long-term ERP system management and reduced costs. This study focuses on the perceptions of ERP project stakeholders in the post-implementation phase, shortly after a major system upgrade.

2. METHODOLOGY

Research Questions and Objectives

The purpose of this research is to gain dynamic insight into the software project management of pre-packaged enterprise-wide information systems. This study seeks to better understand the technical and functional perceptions regarding customization versus business process reengineering to satisfy pre-packaged information system (i.e. ERP) functionality gaps.

Primary questions to be addressed are:

- Are customizations perceived a "slippery slope" such that the more they are implemented, the more they are desired?
- How likely are customizations to be reevaluated once created?
- What impact does top management support have on business process reengineering versus customization?
- Is there a perception that business process reengineering is more time consuming than customization?
- Is there a perception that customizations are an easier fix for functionality gaps than business process reengineering?
- Are customizations perceived as more costly than business process reengineering?

Case Study

This research employed a case study methodology with interviews of key functional and technical ERP project participants. The case study institution is a state research university consisting of approximately 13,000 undergraduate students, 5,000 graduate students and 4,300 employees. The institution implemented its first ERP system in 2004 and conducted its first major upgrade of that system in 2008.

System Dynamics and Casual-Loop Diagrams

Because ERP management consists of dynamic problems arising from complex social, managerial and economic systems, the system dynamics methodology is ideally suited to study ERP project management (Richardson, 1996). In order to address the challenges of ERP management, practitioners need a tool that will help them understand the complexities of the system they are attempting to control. System dynamics is a useful methodology for this type of research because it helps individuals understand the dynamics occurring in the real world (Meadows, 1989) and explore the impact of alternative decision options.

Causal Loop Diagrams (CLDs) are visual representations used to explain the interactions/influences within a system and help provide insight into a system's structure. CLDs explicitly show the complex interdependence and circular causality between components in the system (Sterman, 2000). The use of causal loop diagrams in the interview setting allowed for a focused discussion regarding model elements. Based on the research questions, a CLD was created for use during the interviews (see Appendix A, Figure 1).

Interview Administration

The interview protocol was developed and piloted with two case study employees; one from a functional department and one from the centralized technical department. The interview structure was modified based on the feedback from these pilot tests. To further improve the interview structure and consistency between interviews, a comprehensive administrative script was created. A solicitation to participate was sent to 9 case study project participants. A purposive sampling frame was used because it was important that the researcher interview key project participants who are able to provide information relevant to the research focus (Bryman, 2004). In addition a solicitation was sent to a technology in higher education listserv. Individuals were selected based on their role and level of experience on the ERP implementation/maintenance project. Of particular importance was the recruitment of a sampling frame with a balanced mix of functional and technical stakeholders as well as executive leadership. The results of the recruitment were positive with 8 of the 9 case

study individuals solicited actually participating. In addition, three listserv respondents from three institutions were interviewed.

Based on the timing of the pilot tests, all interviews were scheduled for 90 minutes. The Introduction and Model Overview sections of the booklet were sent to the interviewee ahead of time and interviewees were asked to review these documents prior to the interview. At the start of the interview the participant was given a complete Interview Booklet and the Model Overview section was reviewed together.

The use of both open ended questions and Likert-scale questions followed by open discussion was well received by the participants and provided rich data. Although the notation used in the causal loop diagrams was new to the interviewees, a fairly short explanation at the beginning of the interview seemed to clear up any questions. In addition, interviewees were given an introduction packet before the interview so questions were minimal.

Since this was a case study, the population was small enough that all of the functional and technical project leads could be including in the interviews. A larger sample of external experts could have been reached had surveys been used instead of interviews but the resulting data would lack homogeneity, making it difficult to compare the case study interview findings with the external data. In addition, the answers given in the Likert-type questions were sometimes different than the statements made during the structure review discussion. The ability of the researcher and the interviewee to ask questions regarding Likert-type questions reduced the possibility of misinterpretation by both the parties.

Data Capture and Coding

Interview lengths varied between 45 minutes and 2.5 hours. Data collected included open-ended discussion regarding the model concepts and causal structure. Additionally, participants were asked to answer Likert questions related to the model structure, indicating one of the following choices: strongly disagree, disagree, neither, agree, or strongly agree. Interviewees were encouraged to ask questions and offer comments/suggestions while answering the questions. Again following the Likert items, participants were asked if they would like to elaborate and/or offer additional explanation for their answers. Much discussion was generated during this time and dynamic insights were identified. After each interview all data was transcribed, coded and summarized.

3. FINDINGS

Expert Reaction to Model Structure

Semi-structured interviews for this study were conducted with eight case study institution project stakeholders, including executive project leadership and functional/technical leads. Additionally, three external interviews with experts from other higher education institutions were conducted. This section provides an overview and preliminary analysis of these data.

Case Institution Interviews

All interviewees, technical and functional, agreed that there is a customization "slippery slope" phenomenon where when an office sees that other units are getting a customization approved they want the same. Additionally, as customizations are approved for a specific office that office is more likely to request more customizations. As one functional participant explained, "[t]he more you customize, the more they want!" Also adding "once you customize something [the users] will always want it." Despite this agreement during the open ended discussions, there was remarkable divergence on the related Likert items.

While in general there was agreement that as gaps between existing business practices and delivered software functionality are discovered there is an increased pressure from the user community to customize the ERP, technical respondents agreed overall more than functional respondents (see Appendix B, Table I, Question 1). Technical respondents also agreed that users tend to prefer a customization solution over a business process reengineering solution, while functional respondents were more neutral (see Appendix B, Table I, Question 2).
One functional participant explained that the "[i]nitial reaction is to customize but if there is someone with good knowledge of the system [the office] can be persuaded to use existing functionality." Another functional participant added that the pressure to customize comes from the office level staff and that the executive level did encourage business process reengineering. A technical interviewee further

elucidated, "…the reflexive response of the community is to customize but you can change with framing, communication, and leadership."

A functional respondent added that even when the existing functionality satisfies the business requirement, but in a different way than current business practices, there is often an initial pressure to customize. He/she felt that despite the origin of the push (IT or not), there is simply a resistance to change. Even when a new process is more efficient, the functional community is uncomfortable with doing things differently. They also added that the more users are educated about the long-term implications of customizing the less likely they are to request customizations.

While interviewees agreed that clerical level users might not consider the time/resources required to maintain customizations/add-ons, one functional interviewee felt this was a consideration to functional offices. This interviewee reported that there "…is more awareness these days thanks to the IT priority list but there still isn't a handle on the time it will take for each task to implement and/or maintain; thus, making it difficult to prioritize." The interviewee felt their office is more concerned with improvement for the students' benefit versus improvement simply to benefit the administrative end-users.

The largest divergence between the functional and technical groups of participants was in response to the theory that once a customization has been developed to satisfy functionality gaps it is unlikely that gap will be reviewed in the future as a business reengineering candidate (see Appendix B, Table I, Question 3). One functional participant explained that they felt there is more of a willingness to explore delivered functionality and conduct business process reengineering than the model suggests. They also added that as familiarity with the software grows, willingness to conduct business process reengineering improves. Technical participants were overall in agreement that the need for customizations decreases as understanding of the ERP functionality increases, while functional participants were generally between neutral and agree (see Appendix B, Table I, Question 6).

Technical respondents agreed that it is difficult to retire a customization once it has been implemented, while functional participants were more neutral (see Appendix B, Table I, Question 4). Again, technical interviewees generally agreed that the more customizations that exist, the more difficult it is to encourage business process reengineering options for new fit gaps, while functional participants were in the neutral to disagree range (see Appendix B, Table I, Question 5). Two technical interviewees indicated that while customizations should be reviewed regularly they often are not unless IT pushes for it. Participants all agreed that willingness to explore business process reengineering and delivered functionality changes over time. The primary drivers reported by participants were real experience using the system, changes in leadership and changes in institution missions/goals. With each bundle/upgrade "…part of the challenge is to remember to re-explore functionality that didn't work before."

Two interviewees pointed out during the model segment review that they did not agree that business process reengineering always takes longer upfront than a customization and that it really depends on the task. 62.5% of the respondents agreed with the Likert question that business process reengineering typically takes longer to implement than customizations, while 35.5% were neutral (see Appendix B, Table I, Question 7).

There was a divergence between technical and functional participants in response to the theory that it is easier to customize to fix functionality gaps than conduct business process reengineering (see Appendix B, Table I, Question 8). What was surprising about this divergence was that the technical interviewees generally agreed, while functional participants were largely neutral. One technical interviewee expressed that they agreed but only that this was true initially and not over time. Another technical interviewee explained that business process reengineering necessitates consultation with a large group of constituents in the university community and often requires policy changes; thus, it may seem easier upfront to customize. Nonetheless, there was overall agreement that customizations have a greater long-term cost than business process reengineering (see Appendix B, Table I, Question 9). There was also agreement among all participants that strong top management support increases business process reengineering (see Appendix B, Table I, Question 10).

Overall interviewees were neutral regarding the theory that business process reengineering leads to improved functional productivity (see Appendix B, Table I, Question 11). As one technical participant stated, "[b]usiness process reengineering should lead to improved productivity but it doesn't always." Another functional interviewee agreed and stated that it "…depends on user attitude." Adding that adjustment time is needed because "…users are going from a totally customized legacy system to a mostly vanilla delivered with some customizations."

A participant pointed out that the functional perspective changes over time with policy changes, market changes, and technology changes; causing users to look back at the system and say what can the system do to help me.

Non-Case Study Institution Interviews

The non-case study institution interviewees came from three different higher education institutions. Both of the technical interviewees were the project manager for their institution's ERP implementation and are now CIOs at their respective institutions. The functional participant is an administrative office department director. These participants, similarly to the case study institution interviewees, were in high agreement with the model structure/description section of the interview, while there was some disagreement with the related Likert Items. This section will explore the similarities and differences.

One technical participant explained that it was important to gain the trust of functional leads (module managers group). Their organization agreed institutionally that they did not want to customize; they incurred the upfront costs to hire consultants. The interviewee also stated that communication and collaboration are important because the implementation group needs to roadmap the project collectively. The team needs to work together to discover what the options are and then make a decision. Another interviewee explained that "[t]here is a normal predictable resistance to change." Trust and willingness to conduct business process reengineering can be built over time based on early successes. The interviewee stated that these early successes are accomplished via strong leadership and communication.

One participant explained that the pressure to customize depends somewhat on how much the community as bought into the change. If they are not well informed about the big picture and do not have an understanding of what is going to happen, the pressure to customize is high. They added that "most people are not big picture people" and that the community ultimately wants to know, "How is this going to impact me?" The initial reaction for users is to say, "we must have what we had before" because they are afraid. It will take effort to get them to explore, to think about things from a different perspective and to agree on solutions. After the users gain system exposure they loosen up and are more open to change.

Another interviewee added that the pressure to customize depends on maturity level such that it changes over time. They strongly agreed that at the beginning of the implementation as gaps between existing business practices and delivered software functionality are discovered there is an increased pressure from the user community to customize the ERP. After the implementation is mature and the community gains experience with the system, the participant's answer changed from strongly agree to agree (see Appendix B, Table II, Question 1). The interviewee also stated that they strongly agreed that users tend to prefer a customization solution over a business process reengineering solution at the beginning of the implementation but felt that over time with increased exposure to the system this was less the case (see Appendix B, Table II, Question 2).

Two interviewees agreed that once a customization has been developed to satisfy functionality gaps it is unlikely that gap will be reviewed in the future as a business reengineering candidate, while one strongly disagreed (see Appendix B, Table II, Question 3). The individual that strongly disagreed explained that their institution has been able to reduce customizations by 50% in the past 2 upgrades (25% each upgrade) but admitted this took a significant effort initiated by the technical leadership and accomplished via a strong technical/functional partnership.

One of the participants explained that once you give people a customization that makes the system work exactly as it did before they will never explore business process reengineering even if things could work better. "You've put people back in their happy place and when

people get comfortable they don't move…" and are less likely to look back to see if they really need the customization. They also added that functional users need motivation and free time to re-explore delivered functionality, especially when there is a customization that is already filling the gap. It should be noted that this participant made the preceding statements before they viewed/answered Question 3 (see Appendix B, Table II). When reading Question 3 they stated, "[t]hat's exactly what I was saying."

In response to the statement that it is difficult to retire a customization once it has been implemented, one interviewee indicated that it depends on the vendor (see Appendix B, Table II, Question 4). Adding that their ERP vendor is constantly improving the product and their customer base is willing to look at the new functionality because they have asked for changes. Two interviewees agreed that the more customizations that exist, the more difficult it is to encourage business process reengineering options for new fit-gaps. One participant explained that once you have set an expectation that functionality gaps will go away with customizations, users will assume future gaps will be managed this way (see Appendix B, Table II, Question 5).

One interviewee explained that a major problem with ERP is that people suffer from small-world mentality and with ERP systems it is necessary to have a larger worldview; it is necessary to think about the community as a whole. In their institution they have no overseer of the enterprise (e.g. steering committee), which has been a challenge in developing clear goals. The organization did conduct a strategic assessment and the end result was a report indicating that the project stakeholders were not getting along. They added that as CIO you know that the dynamics will happen whether you like it or not. In order to be successful, an organization needs an open-minded group and this attitude needs to be injected into the blood of the university (culture). The interviewee stressed the importance of a roadmap so that there are no customizations made to the system that do not fit with the larger strategic mission of the project.

All interviewees agreed that the need for customizations decreases as understanding of the ERP functionality increases (see Appendix B, Table II, Question 6). However, one participant added that "[t]here are some existing business practices that people are going to hold on to even if they understand the delivered functionality."

One interviewee explained that if users find something good in the new system they get excited and are willing to explore further. He/she added that the "good find" (positive early experience) might need to be facilitated (e.g. consulting) as users might get frustrated on their own, depending on each individual's level of experience.

Another participant felt that capability maturity, how far down the ERP path they are, is a factor in determining how receptive an organization will be to business process reengineering. The interviewee explained that it is important to weed out noise in the system (the naysayers).

An organization needs a critical mass of people that can tell a good story (positive experience). They stated that a minimal common vocabulary is required in order to foster technical/functional communication. Finally adding this it is important to remember that "there are no IT projects, they are all business projects…everything is about the business!" The non-case study interviewees were more in agreement that business process reengineering leads to improved functional productivity than case study participants (see Appendix B, Table II, Question 11).

One interviewee stated that training (functional, technical and end-user) is critical and the key to success. Training is an investment and as such "[i]t is reckless to treat training/development as a cost…[training] is highly associated with a successful outcome." This participant added that the timing of training is important in addition to the strategic use of consulting. Another interviewee explained that user training is "not a self-guided tour." Generic vendor delivered training is good but it is important to get training that is related to what the users do every day. The final interviewee also indicated that training needs to be more than just how the software works; real-life exposure is what makes the difference.

One interviewee explained that business process reengineering does not necessarily take longer than customization solutions (see Appendix B, Table II, Question 7); "the key is whether or not you are good at [reengineering processes]." Another participant explained that an

organization needs to commit to business process reengineering in a disciplined way; focusing on goals of the university and not just departmental objectives. Another interviewee pointed out that customizations do have a recurring cost at the functional office end as each time a customization is reapplied it must be tested, which is very time consuming (see Appendix B, Table II, Question 9).

All interviewees agreed with the statement that "strong top management support increases business process reengineering" (see Appendix B, Table II, Question 10). However, two participants stated they really felt strong management support does not necessarily increase business process reengineering but improves the capacity for it. Unlike the case study institution participants, all non-case study interviewees agreed that business process reengineering leads to improved functional productivity (see Appendix B, Table II, Question 11). One interviewee added a comment that seemed to support the case institution's more neutral stance on this theory, stating "[y]ou would hope the reason you changed was to improve productivity but in some cases this may not be true." The non-case study interviewees were less in agreement than the case study interviewees that it is easier to customize to fix a functionality gap than conduct business process reengineering (see Appendix B, Table II, Question 8).

Indicated Changes to the Model

Based on the interview findings, changes were made to the model structure (see Appendix A, Figure 2). The following table summarizes the relationships eliminated or replaced in the model and the reasons for elimination/replacement:

Additionally, several additions of variables and relationships were added to the model (see Appendix C). Interview findings indicated that willingness to explore business process reengineering changes over time based on system exposure, so the variable needs to reflect this dynamic behavior. System exposure is more than just generic training but a combination of focused training as well as real use of the system. The mean rating for the theories "once a customization has been developed to satisfy functionality gaps it is unlikely that gap will be reviewed in the future as a business reengineering candidate" and "the more customizations that exist, the more difficult it is to encourage business process reengineering options for new fit gaps" was 3.55, indicating neutral to low agreement (see Appendix B, Table II, Questions 3 & 5). Participants explained during the related model segment discussion that there are a variety of factors that influence the likelihood that customizations will be reevaluated, including system exposure and time available to reevaluate customizations.

Relationship Eliminated	**Reason(s) for Elimination**
"Willingness to explore business process reengineering" → (-) "Cumulative customizations"	Willingness alone does not reduce customizations; business process reengineering actually needs to take place. The relationship between "Cumulative business process reengineering" and "Gaps in delivered functionality" is more appropriate and already exists in the model structure.
"Cumulative customizations" → (-) "Willingness to explore business process reengineering"	There was not overall agreement with the related Likert items (see Appendix B, Table II, Questions 3 & 5) and statements made during the open-ended discussion supported elimination of relationship.

Model review discussions indicated that as the technical and functional stakeholders learn to work together effectively the pressure to customize reduces, which in turn opens the door for business process reengineering and increased use of delivered functionality. Therefore, the relationship between interdepartmental collaboration and pressure to customize was added to the model.

4. CONCLUSIONS

The pressure to customize an ERP system is driven by real or perceived functionality gaps in a pre-packaged information system. Some gaps are resolved via business process reengineering or software configuration changes, while others

are resolved via customizations or add-ons. Additionally, there are a certain percentage of gaps that will never be resolved.

A fraction of customizations and add-ons will need to be reviewed each time a software bundle is applied (i.e. typically 4 times per year in higher education institutions). For upgrades, all customizations and add-ons need to be reviewed (i.e. typically every 3-4 years). Therefore, the more customizations and add-ons that exist, the more new work will be generated for each bundle/upgrade. While there is certainly real costs associated with business process reengineering and configuration, interviewees were in agreement that customizations have a greater long-term cost than business process reengineering.

As gaps are discovered in system functionality there is an increased pressure to customize. There is often an initial preference to customize the system rather than change business processes to fit the embedded processes in the software. This can be mitigated via top management support, including a formal process to review and approve/deny customization requests based on a real business need.

Interviewees agreed that there is a customization "slippery slope" reinforcing loop where the more customizations that exist, the greater the pressure to customize. Interviewees stressed the importance of system exposure, and not just generic training, to improve functional understanding, increase willingness to explore business process reengineering, and increase the likelihood that customizations will be reevaluated. Top management can also ensure proper communication channels are nurtured and appropriate time is allocated to review customizations and conduct business process reengineering, factors which were all identified by interviewees as important components that can reduce customizations and total cost of ownership.

5. REFERENCES

Akkermans, H. A., & van Helden, K. (2002). Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors. *European Journal of Information Systems, 1*, 35-46.

Appleton, E. L. (1997). How to Survive ERP. *Datamation, 43*(3), 50-53.

Bansal, V., & Negi, T. (2008). A Metric for ERP Complexity. In W. Abramowicz & D. Fensel (Eds.), *Business Information Systems* (Vol. 7, pp. 369-379). Innsbruck, Austria: Springer Berlin Heidelberg.

Besson, P., & Rowe, F. (2001). ERP Project Dynamics and Enacted Dialogue: Perceived Understanding, Perceived Leeway, and the Nature of Task-Related Conflicts. *The DATA BASE for Advances in Information Systems, 32*(4), 47-66.

Brehm, L., Heinzl, A., & Markus, M. (2001). *Tailoring ERP Systems: A Spectrum of Choices and their Implications*. Paper presented at the 34th Annual Hawaii International Conference on System Sciences, Maui, Hawaii. http://portal.acm.org/citation.cfm?id=821999

Bryman, A. (2004). *Social Research Methods (2nd edition)* (2nd ed.). New York: Oxford University Press.

Crumbly, J., & Fryling, M. (2012, November 1-4). *Rocky Relationships: Enterprise Resource Planning and Supply Chain Management.* Paper presented at the Conference on Information Systems Applied Research (CONISAR), New Orleans, LA.

Dodds, T., & Spencer, R. (2007). Next-Generation Administrative Systems: Philosophy, Principles, and Technology *ECAR* (Vol. 2007, pp. 1-12). Boulder, CO: EDUCAUSE.

Dong, L. (2000, August 10-13). *A Model for Enterprise Systems Implementation: Top Management Influences On Implementation Effectivenes.* Paper presented at the Americas Conference on Information Systems (AMCIS), Long Beach, CA.

Frantz, P. S., Southerland, A. R., & Johnson, J. T. (2002). ERP Software Implementation Best Practices. *Educause Quarterly, 25*(4), 38-45.

Fryling, M. (2010). Estimating the impact of enterprise resource planning project management decisions on post-implementation maintenance costs: a case

study using simulation modelling. *Enterprise Information Systems, 4*(4), 391–421.

Kumar, K., & Van Hillegersberg, J. (2000). ERP experiences and evolution. *Communications of the ACM, 43*(4), 23-26.

McNeil, D. H. (1979). Stabilizing an MIS. *MIS Quarterly*, 31-36.

Meadows, D. (1989). *Gaming to Implement System Dynamics Models.* Paper presented at the The 7th International Conference of the System Dynamics Society, Stuttgart, Germany.

O'Brien, J. A., & Marakas, G. (2006). *Management Information Systems* (7th ed.). New York: McGraw-Hill/Irwin.

Orlikowski, W. J. (2002). Knowing in practice: Enacting a collective capability in distributed organizing. *Organization Science, 13*(3), 249-273.

Peterson, S. (2003). Lost Signals: How Poor Communication and Other Nontechnical Issues Hampered Arkansas' Innovative Statewide ERP Implementation. *Government Technology, February*. Retrieved from http://www.govtech.com/e-government/Lost-Signals.html

Rashid, M. A. (2005). Evolution of ERP Systems *Encyclopedia of Information Science and Technology (II)* (pp. 1138-1143).

Richardson, G. P. (1996). System Dynamics. In S. Gass & C. Harris (Eds.), *Encyclopedia of Operations Research and Management Science*. Norwell, MA: Kluwer Academic Publishers.

Sammon, D., & Adam, F. (2005). Defining and Understanding ERP Systems *Encyclopedia of Information Science and Technology (II)* (pp. 772-778).

Somers, T., & Nelson, K. (2001, January 3-6). *The impact of critical sucess factors across the sages of enterprise resource planning implementations.* Paper presented at the 34th Hawaii International Conference on Information Systems (HICSS-3), Maui, Hawaii.

Sterman, J. D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*. New York: McGraw-Hill Higher Education.

Tapp, R. M., Hesseldenz, J., & Kelley, G. (2003, August 4-6). *The Role of Project Acceptance in the Successful PeopleSoft Human Resources Management System Implementation for the Kentucky Community an Technical College System.* Paper presented at the 9th Americas Conference on Information Systems (AMCIS), Tampa, FL.

Appendix A – Casual Loop Diagrams

Figure 1: Pre-Interview Casual Loop Diagram

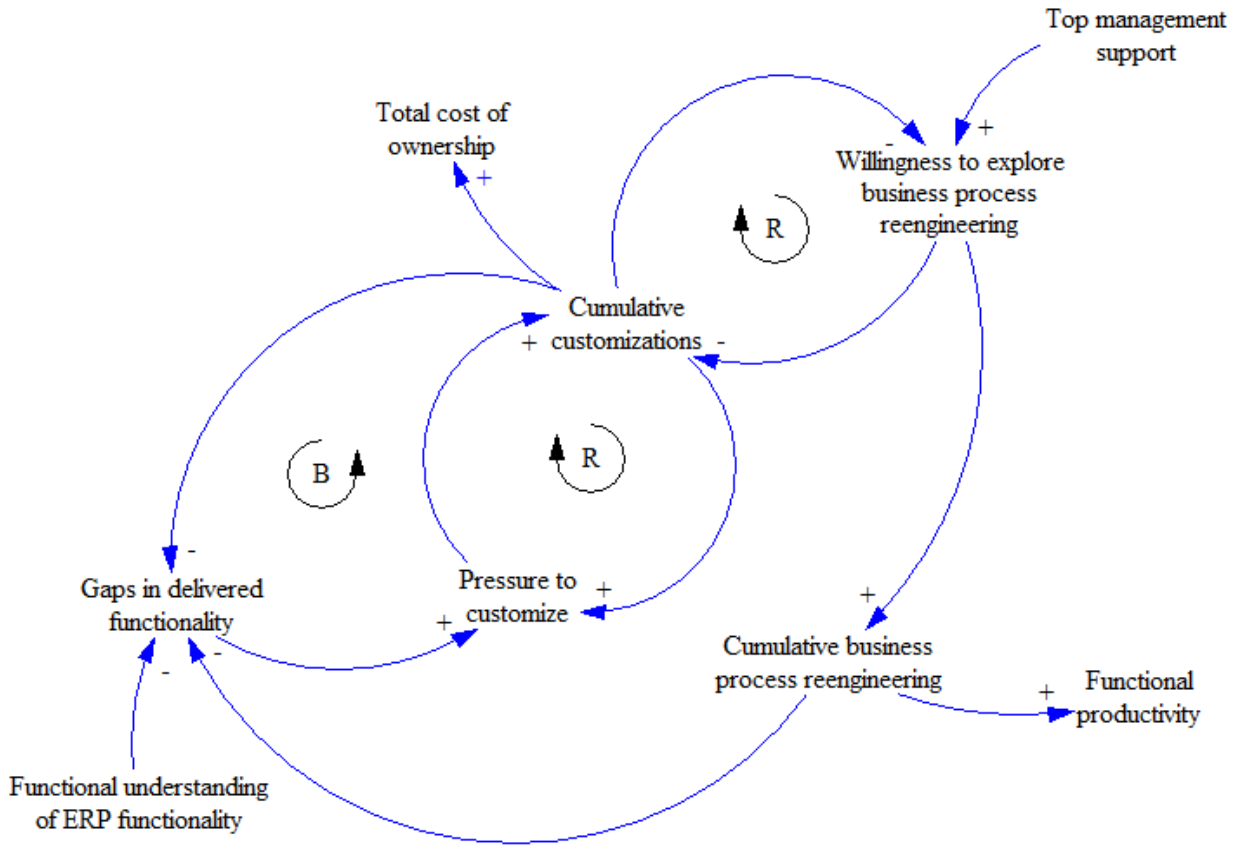
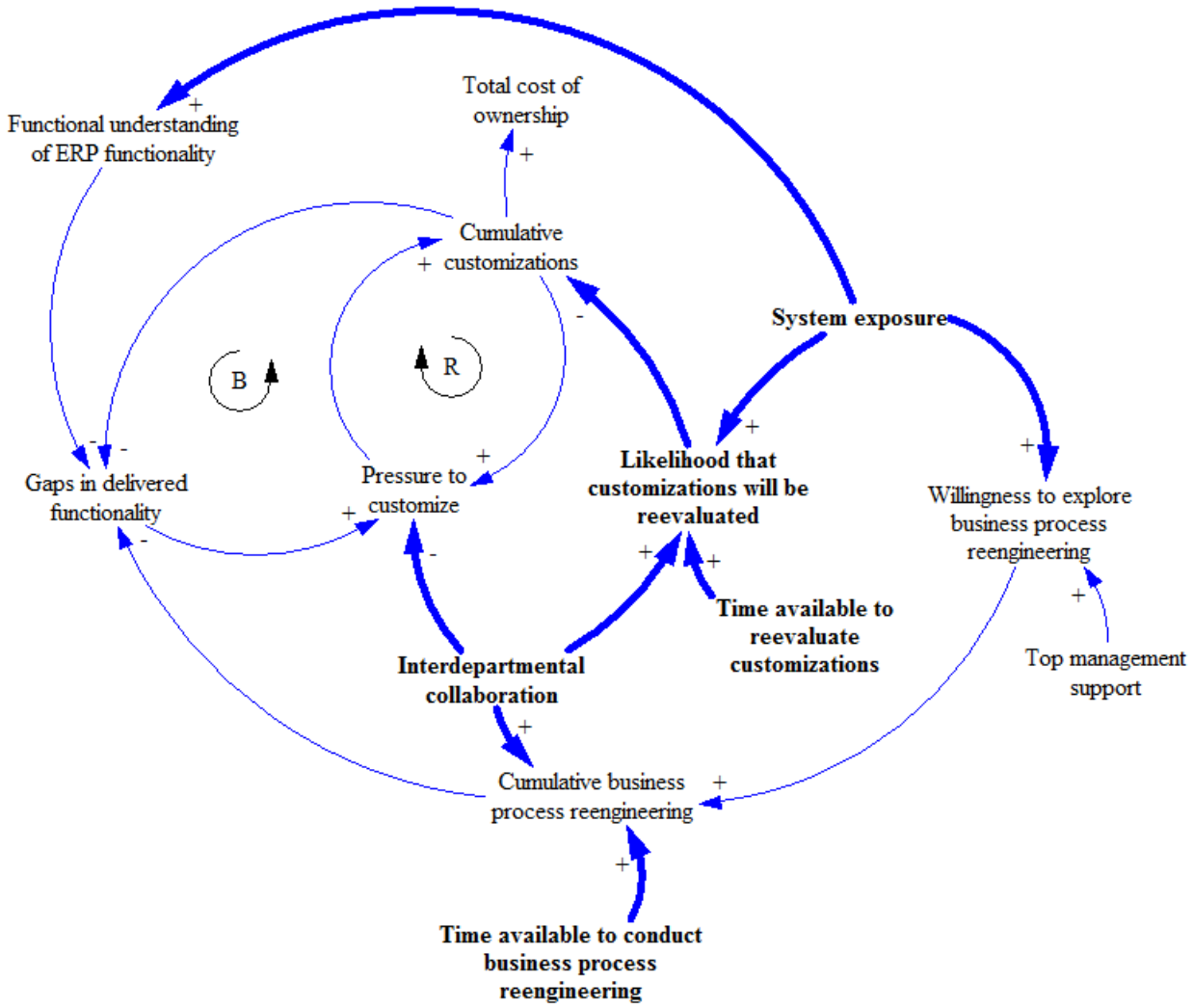


Figure 2: Post-Interview Casual Loop Diagram



Appendix B. Likert Question Results

Table I: Case Study Interviewees Only

	Rating Mean (All)	SD (All)	Rating Mean (Tech only)	SD (Tech only)	Rating Mean (Func only)	SD (Func Only)
1. As gaps between existing business practices and delivered software functionality are discovered there is an increased pressure from the user community to customize the ERP.	4.13	0.99	4.50	0.58	3.75	1.26
2. Users tend to prefer a customization solution over a business process reengineering solution.	3.88	0.99	4.00	0.00	3.75	1.50
3. Once a customization has been developed to satisfy functionality gaps it is unlikely that gap will be reviewed in the future as a business reengineering candidate.	3.75	1.17	4.50	0.58	3.00	1.16
4. It is difficult to retire a customization once it has been implemented.	3.88	1.25	4.25	0.50	3.50	1.73
5. The more customizations that exist, the more difficult it is to encourage business process reengineering options for new fit gaps.	3.50	1.07	4.00	0.00	3.00	1.41
6. The need for customizations decreases as understanding of the ERP functionality increases.	4.13	0.64	4.50	0.58	3.75	0.50
7. Business process reengineering typically takes longer to implement than customizations in order to satisfy fit-gaps.	4.13	0.99	4.50	1.00	3.75	0.83
8. It is easier to customize to fix a functionality gap than conduct business process reengineering.	3.50	0.76	4.00	0.00	3.00	0.71
9. Customizations have a greater long-term cost than business process reengineering.	4.25	0.46	4.50	0.58	4.00	0.00
10. Strong top management support increases business process reengineering.	4.38	0.74	4.50	0.58	4.25	0.83
11. Business process reengineering leads to improved functional productivity.	3.38	0.52	3.25	0.50	3.50	0.50

Table II: All Interviewees

	Rating Mean (All)	SD (All)	Rating Mean (UA)	Rating Mean (Non-UA)
1. As gaps between existing business practices and delivered software functionality are discovered there is an increased pressure from the user community to customize the ERP.	4.14	0.84	4.13	4.17
2. Users tend to prefer a customization solution over a business process reengineering solution.	3.91	0.83	3.88	4.00
3. Once a customization has been developed to satisfy functionality gaps it is unlikely that gap will be reviewed in the future as a business reengineering candidate.	3.55	1.29	3.75	3.00
4. It is difficult to retire a customization once it has been implemented.	3.82	1.08	3.88	3.67
5. The more customizations that exist, the more difficult it is to encourage business process reengineering options for new fit gaps.	3.55	0.93	3.50	3.67
6. The need for customizations decreases as understanding of the ERP functionality increases.	4.18	0.60	4.13	4.33
7. Business process reengineering typically takes longer to implement than customizations in order to satisfy fit-gaps.	3.73	1.04	4.13	3.33
8. It is easier to customize to fix a functionality gap than conduct business process reengineering.	3.36	0.81	3.50	3.00
9. Customizations have a greater long-term cost than business process reengineering.	4.27	0.47	4.25	4.33
10. Strong top management support increases business process reengineering.	4.27	0.65	4.38	4.00
11. Business process reengineering leads to improved functional productivity.	3.64	0.67	3.38	4.33

Appendix C. Variable and Relationship Additions to the Model

Variables Added	Relationships Added
• System exposure • Time available to reevaluate customizations • Time available to conduct business process reengineering • Likelihood that customizations will be reevaluated • Interdepartmental Communication	• "System exposure" → (+) "Willingness to explore business process reengineering" • "System exposure" → (+) "Likelihood that customizations will be reevaluated" • System exposure" → (+) "Functional understanding of ERP functionality" • "Time available to reevaluate customizations" → (+) "Likelihood that customizations will be reevaluated" • "Time available to conduct business process reengineering" → (+) "Cumulative business process reengineering" • "Likelihood that customizations will be reevaluated" → (-) "Cumulative customizations" • "Interdepartmental collaboration" → (-) "Pressure to customize" • "Interdepartmental collaboration" → (+) "Likelihood that customizations will be reevaluated" • "Interdepartmental collaboration" → (+) "Cumulative business process reengineering"

A Cloud Computing Methodology Study of Platform-as-a-Service (PaaS) in the Financial Industry

James Lawler
lawlerj@aol.com

H. Howell-Barber
h.howell@verizon.net

Anthony Joseph
ajoseph2@pace.edu

Pace University
Seidenberg School of Computer Science and Information Systems
163 William Street
New York, New York 10038 USA

Abstract

The financial industry is a frequent client of cloud computing systems. Firms in this industry are gradually implementing more of Platform-as-a-Service (PaaS) as a new paradigm of this technology. In this study, the authors evaluate business, procedural and technical factors in the implementation of PaaS, as to their significance on projects and on a larger strategy. The authors learn from financial firms innovating in PaaS that procedural and business factors manifested more significance on PaaS projects than technical factors, which may facilitate an optimal strategy with this technology if the firms pursue such a strategy. The findings and the methodology of this study benefit educators enhancing curricula of information systems for current evolutions of cloud computing systems in the financial industry and in generic industry.

Keywords: cloud computing, financial industry, information systems, platform-as-a-service (PaaS), strategy

1. DEFINITION OF PLATFORM-AS-A-SERVICE (PaaS)

Platform-as-a-Service (PaaS) "is a broad collection of application infrastructure (middleware services including application platform, business process management, database and integration) … [consisting largely] of application PaaS (aPaaS) …" (Gartner, Inc., 2013) and an operating system (Zhang, Cheng, and Boutaba, 2010). Essentially PaaS is a platform on which firms deploy or develop projects and software solutions without having to buy, or having the complexity of hosting, the infrastructure technology (Marston, Li, Bandyopadhyay, Zhang, and Ghalsasi, 2011, and Murphy, 2013). Firms may have mainframe (Acquia, Inc., 2011) and mobile systems (Sartain, 2013) managed on PaaS by a cloud service provider (CSP) - the extent of providers (Emison, 2013a) is depicted in Figure 1 in the Appendix of this paper. PaaS CSPs include Amazon Database Service, Google App Engine, IBM Smart Cloud, Microsoft Azure Services and Salesforce Force.com (Butler, 2013, Cloud Connect – Information Week, 2013, and Emison,

2013b). Literature forecasts global growth to be $27 billion or 5.3 zettabytes in PaaS by the end of 2016 (Sartain, 2013) and $241 billion in cloud computing overall by 2020 (Engineyard, 2013).

The benefits, especially for financial firms (Zimmerman, 2013), are in accessibility of agile development environments and in agility, efficiency and flexibility of infrastructure performance (McCaffrey, 2013). The fast provisioning of resources and scalability of services are considered critical features of infrastructure PaaS (Pearlson and Saunders, 2013). Financial firms are enabled to immediately implement innovations in products and services from hosted hardware and software for mainframe and mobile systems and for network operations systems. Financial firms are further interested in the cloud because of cost pressures (Crosman, 2014) and in outsourced PaaS because of infrastructure investment savings (Crosman, 2013b) in shared technology. Literature indicates 80% of firms leveraging cloud computing, such as PaaS, in 2014 (Thibodeau, 2013).

The benefits of PaaS are accompanied by concerns however. The control of customized resources by a CSP inevitably inhibits instant migration of services to a different CSP in the event of issues, such as non-fulfillment of services (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Naslund, and Pourzandi, 2012) or non-interoperability of non-CSP systems (Kress, 2014). The outages in the performance of PaaS resources inhibits proper response of services (Addis, Ardagna, Panicucci, Squillante, and Zhang, 2013) – an issue negative to that which is strategic about this technology (Distefano, Puliafito, and Trivedi, K., 2013). The perceived problems as to proper protection, risk management, and security of the systems are frequently indicated in the financial firm (Lipman, 2013a) and generic (Nanavati, 2014) literature. The PaaS may not realize savings (The Economist, 2013). These problems of PaaS pose a risk to financial firms and to generic industry (Vignos, Kim, and Metzer, 2013), such that the implementation of PaaS projects may be initiated slowly without a strategy. For financial firms, the risk may be managed with a methodology for a PaaS strategy. Given PaaS as the last segment of cloud computing to be initiated by industry (McAfee, 2011), a methodology may offer optimal potential with the technology.

2. INTRODUCTION TO PAPER

In the study, the authors apply a cloud computing methodology model to evaluate dimensions of business, procedural and technical factors on the implementation of PaaS projects in financial firms. The model is customized from earlier studies on Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) in financial firms by the authors (Howell-Barber, Lawler, Joseph & Narula, 2013, and Howell-Barber, Lawler, Desai, & Joseph, 2013). The emphasis of this holistic model in this study is on the factors, or the impacts, on the implementation of PaaS projects and on significance on strategy. This methodology is important to financial firms in the management of PaaS (and IaaS and SaaS) projects and strategy, inasmuch as increased investment in the technology in 2014 - 2016 is indicated in the literature (Camhi, 2013, Crosman, 2013a, and Stine, 2013). Though financial firms may be increasing investment in the technology, few may have a methodology model for business professionals and cloud technologists on projects that might proceed in a productive strategy.
The methodology model of the study is enhanced from the models on the IaaS and Saas studies by the authors (Howell-Barber, Lawler, Joseph, & Narula, 2013, and Howell-Barber, Lawler, Desai &, Joseph, 2013), but is essentially homogenous in the hosted similarity of the technologies.

Business Factors of Model
The business factors on the implementation of PaaS projects are below:

Agility and Competitiveness – Extent to which improved agility in initiating new products and services and increased competitiveness in the industry market were significant on the PaaS project;

Cost Benefits – Extent to which expense savings were significant on the PaaS project;

Executive Involvement of Business Organization – Extent to which participation of senior managers from the internal business client organization was significant on the PaaS project;

Executive Involvement of Information Systems Organization – Extent to which participation of senior managers from the internal information systems organization was significant on the PaaS project;

Globalization – Extent to which international impacts were significant on the PaaS project;

Organizational Change Management – Extent to which internal organizational change management processes were significant on the PaaS project;

Participation of Business Client Organization – Extent to which participation of internal business client organizational staff were significant on the Paas project;

Regulatory Requirements – Extent to which governmental or industry regulatory rules were significant on the PaaS project; and

Strategic Planning and Cloud Computing – Extent to which integration of overall strategic planning was significant on the project.

Procedural Factors of Model
The procedural factors on the projects are below:

Education and Training – Extent to which internal PaaS training was significant on the project;

Estimation of Expense and Planning and Procurement – Extent to which internal expense planning and procurement techniques were significant on the PaaS project;

Process Management – Extent to which internal process improvement responsibilities and tasks were significant on the PaaS project;

Program and Project Management – Extent to which internal program and project management teams, in partnership with the external cloud service provider (CSP) teams, were significant on the PaaS project;

Risk Management – Extent to which the CSP service level agreements (SLAs) integrated into internal risk management techniques were significant on the PaaS project;

Service-Oriented Architecture (SOA) – Extent to which purchased services of SOA were significant on the PaaS project;

Standards – Extent to which open standards, participation in standard organizations or processes of standards were significant on the project; and

Technology Change Management – Extent to which technology change management including CSP selection were significant on the project.

Technical Factors of Model
The technical factors are below:

Cloud Computing Center of Excellence – Extent to which a designated internal information systems team knowledgeable in best-of-class practices of cloud technology including PaaS were significant on the project;

Cloud-to-Cloud Interoperability – Extent to which PaaS integration with other internal or external cloud systems or technologies were significant on the project;

Cloud-to-Non-Cloud Interoperability – Extent to which PaaS integration with other internal or external non-cloud systems or technologies were significant on the project;

Continuous Processing – Extent to which 365/7/24 resource availability of services were significant on the PaaS project;

Data – Extent to which data governance, including "big data" management services, were significant on the PaaS project;

Elasticity of Processing Resources – Extent to which resource synchronization with internal processing requirements were significant on the PaaS project;

Infrastructure Architecture – Extent to which PaaS integration with internal organizational processing requirements were significant on the project;

Multiple Cloud Service Providers (CSPs) – Extent to which multiple CSPs were significant on the PaaS project;

Networking Implications – Extent to which the internal networking infrastructure was significant on the PaaS project;

Platform of Cloud Service Provider (CSP) – Extent to which the CSP platform of specialized technologies was significant on the project;

Privacy and Security – Extent to which CSP and internal organizational protection and security requirements were significant on the project;

Cloud System Problem Management – Extent to which problem management monitoring tools were significant on the project; and

Tools and Utilities – Extent to which CSP lifecycle management and system utilities were significant on this project.

This methodology offers a model on Paas projects that may proceed progressively in a strategy with PaaS technology.

The study attempts to evaluate the factors of the model as to immediate implementation significance and to significance to strategy. How might financial firms be best in identifying and implementing PaaS projects with external CSPs, but also be best in concurrently implementing other projects with internal organizational staff? How might the firms be integrating PaaS projects non-disruptively with internal services, and even IaaS and SaaS projects and services? How might they be integrating private and public PaaS services? How might they be managing external CSP PaaS systems integrating with internal organizational processes and systems? How might financial firms be managing PaaS systems in a PaaS strategy, if not an integrated SaaS, PaaS and IaaS strategy, with internal staff? Few in the field of information systems furnish a methodology model to answer these questions – answers that might be helpful to instructors in information systems in informing students of industry practices with this technology.

3. FOCUS OF STUDY

The focus of the authors is to evaluate the aforementioned business, procedural and technical factors in financial firms, as to significance in implementation on PaaS projects and as to significance on a PaaS strategy. Though firms in the industry have frequently hesitated in cloud computing innovation due largely to issues of reliability and security, the perceived processing savings is inexorably pressuring them to pursue PaaS systems (Melvin, 2013). The investment in PaaS is manageable with not only a methodology to minimize project risks but also with a strategy to maximize the benefits of PaaS systems (Subramanian, 2013). The maximization of on premise systems and outsourced PaaS systems, if not of further IaaS and SaaS technologies, is probable in a strategy (Greengard, 2013a). Financial firms may benefit from the guidance of the methodology of the study, and instructors in information systems may learn new practices in the shift to PaaS technology. In short, this study of PaaS contributes insight into a striding technological trend.

4. RESEARCH METHODOLOGY

The research methodology of this study consisted of a case study of 5 financial firms, chosen by the authors from among cloud computing first-mover innovators in Platform-as-a-Service (PaaS) identified in reputed practitioner publications (e.g., *Bank & Systems Technology*, *Bank Technology News*, and *Wall Street & Technology*) in the 4-month September – December 2013 period. The projects and systems of PaaS in the firms were evaluated by the authors from a checklist definition instrument of the aforementioned business, procedural and technical factors in the 4-month January – April 2014 period. The factors were evaluated on evidence of factor project significance, and significance on strategy, on a six-point Likert-like rating scale:

5 – Very high in significance;
4 – High in significance;
3 – Intermediate in significance;
2 – Low in significance;
1 – Very low in significance; and
0 – No significance.

These evaluations were based on in-depth observation of middle-management stakeholders in the financial firms; informed perceptions of observation PaaS rationale by the third author, an industry practitioner of 35 years; and research reviews of secondary industry practitioner studies by the first author, which were filtered for hype of marketing by also the third author. The checklist instrument of this study was evaluated in the context of construct, content and face validity and content validity, measured in sample validity, by the second author.

Overall, the research methodology of this study of PaaS was consistent in creditability and proven reliability with that of the earlier original studies of the authors on cloud SaaS and IaaS technologies (Howell-Barber, Lawler, Joseph, & Narula, 2013, and Howell-Barber, Lawler, Desai, & Joseph, 2013) and on related service-oriented architecture (SOA) technology (Lawler, & Howell-Barber, 2008); and with that of information systems syllabi taught by instructors in the Seidenberg School of Pace University.

5. ANALYSIS OF DATA

From the case study of the financial firms, the authors interpreted the data from the evaluations of the factors, and of the strategies, in the MATLAB 7.10.0 Statistics Toolbox (McClave & Sincich, 2006), for the following sub-section and Tables 1 and 2 in the Appendix.

Detailed Analysis of Financial Firms*
Firm 1: **Banking Institution**
Project: **Application Processing Platform**
Type: **Public Cloud System**

Financial Firm 1 is (in revenue) a small-sized northeast banking institution that focused on an application for processing and routing of customer services initiated at its international retail offices. The objective of the project was to discontinue antiquated and disparate internal systems that were not current with executed transactions; enable faster management of the transactions, especially problematic transactions; and integrate organizational processes for faster monitoring of the transactions. The project resulted in an external public cloud, performance reporting for senior management and service staff, and full security of the system.

The business factors of *Executive Involvement of Business Organization* (5.00 / 5.00), *Executive Involvement of Information Systems Organization* (5.00) and *Participation of Business Client Organization* (5.00) were significant in ensuring that the business requirements of the retail offices were met by the CSP. The procedural factors of *Process Management* (5.00) and *Risk Management* (5.00), and the technical factors of *Data* (5.00) and *Privacy and Security* (5.00), were especially significant in ensuring that *Regulatory Requirements* (4.00) were met by the CSP. Inasmuch as the processes of the system were managed mostly by the CSP, the technical factors of *Cloud-to-Non-Cloud Interoperability* (5.00), *Continuous Processing* (5.00) and *Cloud System Problem Management* (5.00) were of further significance. The very high reliance of the firm on the CSP was evident in the internal procedural factor of *Education and Training* (1.00) and the technical factor of *Cloud Computing Center of Excellence* (0.00). The project was the first initiation of the firm into the cloud, in the context of a plan in *Strategic Planning and Cloud Computing* (4.00), with the intent of further migration of internal systems to the CSP in 2015 – 207.

Firm 1 is an example of a small-sized organization that is cautiously piloting PaaS for a few applications in a public cloud with a CSP vendor.

Firm 2: **Financial Services Institution - Domestic**
Project: **Application Infrastructure Platform**
Type: **Private Cloud System**

Firm 2 is a large-sized northeast financial services institution that focused on an application infrastructure for development systems staff. The objective of the project was to discontinue expensive and inefficient localized infrastructures; and enable a faster infrastructure institutionalized for software teams. The project resulted in a private cloud with a CSP that improved platform services and productivity of the staff for next generation systems, at a lower investment than the multiple platform services.

Though the business factor of *Agility and Competitiveness* (5.00) and *Cost Benefits* (5.00) were significant in initiating the project, the procedural factors of *Estimation of Expense and Planning and Procurement* (5.00), *Standards* (5.00) and *Technology Change Management* (5.00) were significant in managing the technology. The technical factor of *Cloud-to-Non-Cloud Interoperability* (5.00) was especially significant on this project, inasmuch as the financial firm was initiating a private cloud PaaS that was also managed by the internal information systems organization. This project was significantly technical, such that *Continuous Processing* (5.00), *Elasticity of Processing Resources* (5.00) and *Infrastructure Architecture* (5.00) were of notable significance to the internal systems staff. The reliance on internal systems teams was evident in the procedural factor of *Education and Training* (4.00) and the technical factor of *Cloud Computing Center of Excellence* (5.00). The project was migrating the firm into the cloud with informed knowledge of a strategy in *Strategic Planning and Cloud Computing* (5.00).

Firm 2 is an example of a large-sized organization that is piloting core infrastructure on PaaS in a private cloud with a CSP, in order to be competitive and efficient on projects, but the firm is limiting integration of in-house on premise systems with the vendor.

Firm 3: **Financial Services Institution - Global**
Project: **Database "Big Data" Platform**
Type: **Private Cloud System**

Firm 3 is a large-sized global proprietary services organization that initiated an enhanced database platform for international offices. The objective of this project was to enable expandable features of an existing PaaS hardware platform for predictive analytic services. The project included a few more CSPs that resulted in an improved private cloud platform that increased scalability of the services and interoperated internal legacy systems.

The business factors of *Agility and Competitiveness* (5.00) and *Cost Benefits* (5.00) were again significant, but they included more of *Participation of Business Client Organization* (5.00) on the project. The procedural factors of *Education and Training* (5.00) and *Standards* (5.00), and the technical factor of *Cloud Computing Center of Excellence* (5.00), were especially significant on this project – the inclusion of open source standards in the technical factor of *Tools and Utilities* (5.00) was notable significantly for ensuring independence of the CSP vendors. The reliance on the internal management of systems was again evident in *Executive Involvement of Information Systems Organization* (5.00). This project was mainly managed by the internal organizations, in the procedural factors of *Estimation of Expense and Planning and Procurement* (5.00) and *Technology Change Management* (5.00). In fact, the technical factors of *Cloud-to-Non-Cloud Interoperability* (5.00), *Data* (5.00), *Elasticity of Processing Resources* (5.00), *Infrastructure Architecture* (5.00) and *Multiple Cloud Service Providers* (5.00) were prominent on this project – the hosted *Multiple Cloud Service Providers* (5.00) integrating into internal processes of the organization were notably significant to project success. Interestingly, the factor of *Privacy and Security* (2.00) was not as evident in the planning of the technologists. Overall, this project was further in migrating into the PaaS platform in an incremental strategy, in *Strategic Planning and Cloud Computing* (5.00), than the projects in Firms 2 and 1.

Firm 3 is another example of a large-sized organization that is independently migrating into the PaaS paradigm, pioneering critical infrastructure on PaaS in a private cloud, but limiting the optimization of the technology in initial internal training.

Firm 4: **Global Insurance Organization**
Project: **Elastic Grid Platform**
Type: **Public Cloud System**

Firm 4 is an international medium-sized insurance organization that needed a faster and flexible data center platform for international regulatory reporting requirements. The objective was to implement a high performance platform for the processing stochastic systems of the offices of the organization. The project resulted in a new public cloud platform with a first comer CSP that increased the frequency and intelligence of the reporting and the interoperability of the systems at less expense than previous.

The business factors on this project were especially significant in European Union *Regulatory Requirements* (5.00) that involved more of *Executive Involvement of Business Client Organization* (5.00) and *Participation of Client Organizations* (5.00) than on the projects previously, though the information systems organization in *Executive Involvement of Information Systems Organization* (5.00) managed the project, again similar to the projects previously. The factor of *Cost Benefits* (5.00) was of project significance. The procedural factors of *Process Management* (5.00), *Program and Project Management* (5.00) and *Risk Management* (5.00), and also *Education and Training* (5.00), were of notable significance, inasmuch as the PaaS platform was a higher-risk public system. The technical factors of *Cloud-to-Non-Cloud Interoperability* (5.00), *Data* (5.00), *Elasticity of Processing Resources* (5.00), *Privacy and Security* (5.00) and *Tools and Utilities* (5.00) were of significance in insuring the performance and protection of the non-private technology. Overall, the project was planned in a sole strategy for the specific technology, but was not positioned for a PaaS strategy of subsequent technologies.

Firm 4 is an illustration of an organization that is leveraging a PaaS public cloud platform on a limited number of projects with a CSP vendor, but the organization will not probably pursue the technology unless perceived urgent.

Firm 5: **Customer Loan Management Organization**
Project: **Loan Management Platform**
Type: **Public Cloud System**

The final firm is a small-sized Midwest organization that needed to replace an expensive external system hosted by a non-cloud vendor. The objective of the organization was in fully outsourcing and processing payment transactions on a less expensive public cloud

system of a CSP vendor. The project resulted not only in a less expensive PaaS processing and reporting system, but also in PaaS utilities and tools furnished by the vendor that increased organizational profit margins.

The business factors of *Agility and Competitiveness* (5.00) and *Cost Benefits* (5.00) were notably significant on this project. This project was managed by the business organization in *Executive Involvement of Business Client Organization* (5.00) and *Participation of Client Organizations* (5.00), inasmuch as the firm as a small-sized organization was without a technologist team. The procedural factor of *Process Management* (5.00), in negotiating processing requirements with the CSP, was of significance. The technical factors were limited to *Data* (5.00), *Privacy and Security* (5.00) and *Tools and Utilities* (5.00) in project significance. In short, neither the organization nor the project was positioned for a PaaS *Infrastructure Architecture* (0.00) plan or strategy in *Strategic Planning and Cloud Computing* (0.00) – outsourcing of specific technologies was the pure and simple target.

Firm 5 is an illustration of small-sized organizations having few funds for internal systems that are initiating investment in limited PaaS platform technologies that are often public not private utilities.

*Financial Firms are classified as confidential due to competitive imperatives in the industry.

Summary Analysis of Financial Firms

The analysis of the data findings from the financial firm projects is disclosing business factors (3.51 summary) as essentially significant. Even though the PaaS projects were mainly managed by the information systems organizations (4.00), the justification for the projects was not merely technical. The procedural factors (3.60) were significant insofar as the organizations were managing the migration of processing requirements (4.60) to the CSP vendors. Internal technologist training (3.60) was significant in instances of interoperability of non-PaaS systems and observable performances of PaaS technologies (Stewart and Slisinger, 2012). The technical factors (3.18) frequently were manifested more and were notably significant in interoperability (4.00) of non-PaaS systems and in the performances (4.00) and protections (4.40) of PaaS technologies, especially in the large-sized organizations sharing PaaS technologies. Few of organizations were migrating systems to multiple CSP vendors (1.00). Privacy and security (4.40) was of notable significance. The large-sized organizations were migrating systems to private cloud vendors; and the small-sized organizations were migrating the systems to public cloud vendors. The organizational planning of the projects in a bona fide PaaS strategy was not positioned prominently in the study, but the potential of pursuing a strategy was strong at times. The planning of IaaS, PaaS and SaaS strategy was not a result of this study.

(The correlations of the factor ratings between pairs of the firms indicated in Table 3 that positive correlations between Firms 1 and 4 (0.5132), Firms 1 and 5 (0.5920) and Firms 4 and 5 (0.5187) were statistically significant at the $p<0.01$ level of significance. The frequency distributions of the 0 -5 ratings of each of the firms indicated in Table 4 that except for Firm 5 factor ratings across Firms 1-4 were concentrated in the 5 (very high in significance) rating. The concentrations of the 5 rating in Firms 1, 2, 3 and 4 were 43.33%, 63.33%, 66.67% and 63.33% respectively – in Firm 5 the 0 rating (no significance) had the highest concentrations of ratings of 40.00%.)

6. DISCUSSION AND IMPLICATIONS OF STUDY

The evaluations of the financial firms denote encouragingly that the PaaS projects were funded and implemented from business factor justification. Though the projects were mainly managed by the information systems organization, in partnership with the CSP PaaS staff, the internal technologists were motivated by business organizational requirements (Greengard, 2013b), not the provider technologies. The importance of internal organizational requirements as a PaaS prerequisite is an immediate implication.

The evaluations of the firms by the authors find that the PaaS projects were implemented mainly in private cloud systems by the large-sized organizations and in public cloud systems by the small-sized organizations. The management of internal non-PaaS and external PaaS metric processing and protection requirements was notable regardless of the systems. Risk and security of the external systems were notable in the study. Though external private secure systems on the cloud will be the probable technologies of large-sized organizations (Lipman, 2013b), the risk and security of private and public systems were equivalently of prominent significance in the study. The

importance of non-PaaS and PaaS processing requirements in private and public secure systems is an implication of the study.

The evaluations of the authors highlight the governance importance of integration of internal non-PaaS and external PaaS systems in mostly the large-sized organizations with the most systems. The focus on the interoperability of the systems, and even of localized so-called ready technologies (Andriole, 2014), is noted in the literature (Greengard, 2013a) and was of prominent significance in the study. The importance of interoperability and openness of the processing of non-PaaS and PaaS systems, as a required responsibility of the CSP and the internal systems organization, is another implication.

Even though the cloud model of PaaS is an outsourcing paradigm, the findings in the financial firms indicate that knowledge of cloud PaaS in the internal systems organizations is of importance in the migration of the systems to the CSP vendor. The importance of cloud knowledge in PaaS, SaaS and IaaS is noted often in the literature (Eddy, 2013, Florentine, 2013, and Kress, 2014) and was also of prominent significance in this study. Firms need professionals skilled in the business and technical perspectives of these technologies (Gabriel, 2013 and Rubin, 2013). Forward-looking instructors in information systems might enhance programs for students, in order to help them in learning these state-of-the-art technologies, in tandem with traditional theories (Linthicum, 2013). The importance of internal skilled systems teams in the interface integration and migration of on premise systems and PaaS provider technologies is a further implication.

Finally, the findings of the study indicate the locus of the financial firms to be more on PaaS projects at minimal risk (Subramanian, 2013) than on strategy. The gains of the projects were more incremental than integrated or optimized in a strategy (Greengard, 2013a). Though PaaS projects are the smallest of the cloud technologies (Butler, 2013), firms may proactively pursue a strategy if PaaS furnishes an increased edge in their industry beyond expense infrastructure savings with these technologies. PaaS may be eventually integral to the firms (Sardet, 2012), necessitating a strategy. The importance of practitioners and researchers in information systems pursuing the potential of a PaaS strategy is the last implication of this study.

7. LIMITATIONS AND OPPORTUNITIES

Implications of this study are from a limited number of financial firms, inasmuch as investment is limited in this segment of the technology. This study is exclusive of external cloud service provider (CSP) PaaS processes and is limited to internal interoperating processes of the PaaS systems and technologies of the financial firms. The methodology of this study furnishes nevertheless an opportunity for pursuing project research and significance of strategy, inasmuch as practitioner and scholarly research is limited on PaaS if not on IaaS and SaaS technologies (Zhang, Cheng, and Boutaba, 2010). The methodology may even be improved for researching CSP risks and reviewing CSP services for specialized PaaS technologies. The opportunities for PaaS study will increase as investment increases in this technology.

8. CONCLUSION OF STUDY

The authors conclude that the financial firms analyzed in this study are benefiting from Platform-as-a-Service (PaaS) projects, but not as frequently as other cloud platform technologies. Firms in this industry are concerned about risks and are generally hesitant in implementing outsourced PaaS systems. For the firms implementing PaaS private or public systems, the authors learn that business, procedural and technical factors from the framework of a management methodology model are significant on PaaS technologies.

The business factors were a definite justification for the projects, in efficiencies and savings, even though the projects were managed mostly by the information systems organizations. The procedural factors, such as risk management, were significant in the migration of processing and protection requirements to the cloud service provider (CSP) PaaS technologies. The technical factors were more manifested than the procedural and business factors and were prominent and of significance in the interoperability of non-PaaS systems and PaaS technologies in tandem.

At the same time, the findings indicate that the financial firms initiated investment in the CSP PaaS technologies separate from a strategy. Though the firms might be hesitant about further investment due to lingering issues, such as security, they might be more motivated to pursue a PaaS strategy beyond tactical once the benefits are more prevailing than the issues. In the interim period, the study contributes findings

that are beneficial to instructors in information systems, in helping students learn practices in PaaS state-of-the-art technologies. The study is beneficial to practitioners, in learning of proven solutions. In conclusion, this study contributes a methodology model for instructors and practitioners that may be applied in the evolution of PaaS technologies not only in the financial industry, but also in generic industry.

9. REFERENCES

Addis, B., Ardagna, D., Panicucci, B., Squillante, & Zhang, L. (2013). A hierarchical approach for the resource management of very large cloud platforms. *IEEE Transactions on Dependable and Secure Computing*, 10(5), 253.

Andriole, S.J. (2014). Ready technology: Fast-tracking emerging business technologies. *Communications of the ACM*, 57(2), 40-41.

Butler, B. (2013, June 19). Forrester: PaaS makes developers happy. *Infoworld*, 1,2.

Camhi, J. (2013, October 16). Gartner: Majority of banks will turn to cloud for processing transactions by 2016. *Bank Systems & Technology*, 1-3.

Crosman, P. (2013a, August 12). Why banks are finally embracing cloud computing. *American Banker*, 1-2.

Crosman, P. (2013b, November 1). Bankers put cost concerns first when contemplating cloud computing. *Bank Technology News*, 2.

Crosman, P. (2014, March 10). Banks pushed toward cloud computing by cost pressures. *American Banker*, 2-3.

Distefano, S., Puliafito, A., & Trivedi, K.S. (2013). Cloud computing assessment: Metrics, algorithms, policies, models, and evaluation techniques. *IEEE Transactions on Dependable and Secure Computing*, 10(5), 251.

Eddy, N. (2013, May 23). Chief information officer (CIO) challenges: IT skills gap, growing cloud, mobile demands. *Eweek*, 2.

Emison, J.M. (2013a, March). PaaS buyer's guide. *Information Week*: *Reports*, 2.

Emison, J.M. (2013b, April 22). Change platform: Here is why we give PaaS a vote of confidence. *Information Week*, 26.

Florentine, S. (2013, November 1). Demand for cloud skills still outpaces supply of workers. *CIO*, 36.

Gabriel, A.R. (2013, June 12). Seven must-have skills for chief information officers (CIOs). *Wall Street & Technology*, 1-3.

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Naslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing*: *Advances, Systems and Applications*, 1(11), 16.

Greengard, S. (2013a, August 22). Integrating clouds into IT infrastructure. *Baseline*, 2,4.

Greengard, S. (2013b, October 1). Cloud adoption grows despite new challenges. *CIO Insight*, 3.

Howell-Barber, H., Lawler, J., Desai, S., & Joseph, A. (2013). A study of cloud computing software-as-a-service (SaaS) in financial firms. *Journal of Information Systems Applied Research*, 6(3), 4-17.

Kress, J. (2014). Cloud computing and service-oriented architecture (SOA). *Service Technology*, March, 1-5.

Howell-Barber, H., Lawler, J.P., Joseph, A., & Narula, S. (2013). A study of cloud computing infrastructure-as-a-service (IaaS) in financial firms. *Proceedings of the Information Systems Educators Conference*, San Antonio, Texas, November, 6(2804), 1-14.

Lawler, J.P., & Howell-Barber, H. (2008). Service-oriented architecture: SOA strategy, methodology and technology. Boca Raton, Florida: Auerbach Publications – Taylor & Francis Group.

Linthicum, D. (2013, September 13). Want a good cloud job? Better know traditional IT too. *Infoworld*, 1-5.

Lipman, B. (2013a, October 31). Will public cloud come of age in 2014? *Wall Street & Technology*, 1,2.

Lipman, B. (2013b, November 11). OneMarketData releases cloud adoption survey. *Wall Street & Technology*, 1-4.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing – The business perspective. *Decision Support Systems*, 51, 178.

McAfee, A. (2011). What every chief executive officer (CEO) needs to know about the cloud. *Harvard Business Review*, November, 4.

McCafferty, D. (2013, June 6). Cloud's benefits outweigh perceived negatives. *Baseline*, 2.

McClave, J., & Sincich, T. (2006). A first course in statistics, ninth edition. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Melvin, M. (2013, December 19). Cloud services: Five key questions before you buy. *Information Week*, 4.

Murphy, A. (2013, September 10). Cloud computing: The private versus the public cloud. *Wall Street & Technology*, 2.

Nanavati, M., Colp, P., Aiello, B., & Warfield, A. (2014). Cloud security: A gathering storm. *Communications of the ACM*, 57(5), 78.

Pearlson, K.E., & Saunders, C.S. (2013). Managing & using information systems: A strategic approach, fifth edition. Hoboken, New Jersey: John Wiley & Sons, Inc., 184.

Rubin, H. (2013, June 21). Do not fall into the technology skills gap. *Wall Street & Technology*, 1-3.

Sardet, E. (2012, October). Clouds could save banks: Use of cloud technology can be a way to help banks bundle products and price them accordingly. *Bank Technology News*, 38.

Sartain, J.D. (2013, November 27). Cloud traffic poised to quadruple by 2017, challenge chief information officers (CIOs). *CIO*, 1,2.

Stewart V., & Slisinger, M. (2012). Virtualization changes everything: Storage strategies for wmware & cloud computing. New York, New York: Vaughn Stewart, 114,165,192.

Stine, E. (2013, December 4). Four bank technology predictions for 2014. *Bank Systems & Technology*, 1-3.

Subramanian, K. (2013, December 5). Five pillars of enterprise PaaS strategy. *Information Week*, 3,4.

Thibodeau, P. (2013, December 11). One in four cloud providers will be gone by 2015. *Infoworld*, 2.

Vignos, J., Kim, P., & Metzer, R. (2013). Let's look at the cloud from a risk management perspective. *Journal of Information Systems Applied Research*, 6(3), 26.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services Applications*, 1, 9,14.

Zimmerman, D. (2013, November 26). Cloud accelerates competitive advantage to banking and financial markets. *Bank Systems & Technology*, 1-3.

_____ (2011). The payoffs of PaaS: Four ways cloud platform-as-a-service offerings can improve performance while reducing operational costs. *Acquia, Inc*., December, 1.

_____ (2013, March 20). Cloud computing comparison: PaaS providers. *Cloud Connect – Information Week*, 2,4.

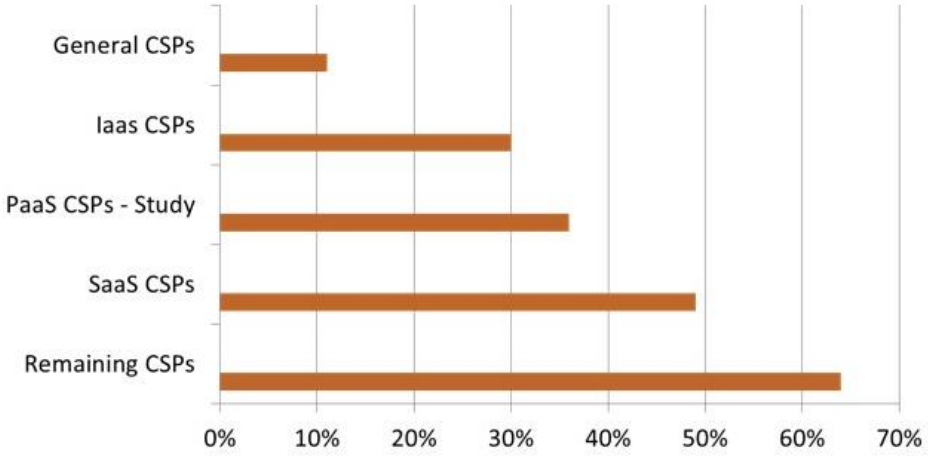
_____ (2013, July 20). Silver linings: Banks big and small are embracing cloud computing. *The Economist*, 65.

_____ (2013). Platform-as-a-service (PaaS): What is platform-as-a-service? *Engineyard*, November, 2.

_____ (2013). IT Glossary: Platform-as-a-service (PaaS). *Gartner, Inc.*, November, 1.

APPENDIX

Figure 1: Cloud Service Providers (CSPs) – Platform-as-a-Service (PaaS) in Industry



2013 Organizational Percentage Usage

Source: Emison, J.M. (2013a, March). PaaS buyer's guide. *Information Week*: *Reports*, 2.

Table 1: Summary Analysis of Factors of Financial Firms of PaaS Study

Categorical Factors of Methodology Model	Means	Standard Deviations
Business Factors	3.51	2.00
Procedural Factors	3.60	1.84
Technical Factors	3.18	2.14

Legend: 5 – Very High in Significance, 4 – High in Significance, 3 – Intermediate in Significance, 2 – Low in Significance, 1 – Very Low in Significance, and 0 – No Significance, on Projects of Study

Table 2: Detailed Analysis of Factors of Financial Firms of PaaS Study

	Firm 1 Means	Firm 2 Means	Firm 3 Means	Firm 4 Means	Firm 5 Means	Summary Means	Standard Deviations
Business Factors							
Agility and Competitiveness	5.00	5.00	5.00	1.00	5.00	4.20	1.79
Cost Benefits	3.00	5.00	5.00	5.00	5.00	4.60	0.89
Executive Involvement of Business	5.00	0.00	3.00	5.00	5.00	3.60	2.19

Organization							
Executive Involvement of Information Systems Organization	5.00	5.00	5.00	5.00	0.00	4.00	2.24
Globalization	5.00	4.00	3.00	0.00	0.00	2.40	2.30
Organizational Change Management	2.00	4.00	0.00	4.00	0.00	2.00	2.00
Participation of Business Client Organization	5.00	3.00	5.00	5.00	5.00	4.60	0.89
Regulatory Requirements	4.00	0.00	0.00	5.00	3.00	2.40	2.30
Strategic Planning and Cloud Computing	4.00	5.00	5.00	5.00	0.00	3.80	2.17
Procedural Factors							
Education and Training	1.00	4.00	5.00	5.00	3.00	3.60	1.67
Estimation of Expense and Planning and Procurement	4.00	5.00	5.00	5.00	3.00	4.40	0.89
Process Management	5.00	5.00	3.00	5.00	5.00	4.60	0.89
Program and Project Management	3.00	3.00	4.00	5.00	2.00	3.40	1.14
Risk Management	5.00	5.00	5.00	5.00	3.00	4.60	0.89
Service-Oriented Architecture (SOA)	0.00	5.00	5.00	0.00	0.00	2.00	2.74
Standards	0.00	5.00	5.00	0.00	0.00	2.00	2.74
Technology Change Management	3.00	5.00	5.00	5.00	3.00	4.20	1.10
Technical Factors							
Cloud Computing Center of Excellence	0.00	5.00	5.00	0.00	0.00	2.00	2.74
Cloud-to-Cloud Interoperability	0.00	0.00	5.00	0.00	0.00	1.00	2.24
Cloud-to-Non-Cloud interoperability	5.00	5.00	5.00	5.00	0.00	4.00	2.24
Continuous Processing	5.00	5.00	2.00	3.00	3.00	3.60	1.34
Data	5.00	0.00	5.00	5.00	5.00	4.00	2.24

Elasticity of Processing Resources	0.00	5.00	5.00	5.00	0.00	3.00	2.74
Infrastructure Architecture	3.00	5.00	5.00	0.00	0.00	2.60	2.51
Multiple Cloud Service Providers (CSPs)	0.00	0.00	5.00	0.00	0.00	1.00	2.24
Networking Implications	4.00	3.00	2.00	3.00	3.00	3.00	0.71
Platform of Cloud Service Provider (CSP)	2.00	5.00	5.00	5.00	2.00	3.80	1.64
Privacy and Security	5.00	5.00	2.00	5.00	5.00	4.40	1.34
Cloud System Problem Management	5.00	5.00	2.00	5.00	3.00	4.00	1.41
Tools and Utilities	5.00	5.00	5.00	5.00	5.00	5.00	0.00

Legend: Refer to Legend in Table 1

Table 3: Correlations between Pairs of Financial Firms of PaaS Study

	Firm 1	**Firm 2**	**Firm 3**	**Firm 4**
Firm 2	0.0844			
Firm 3	-0.2811	0.2019		
Firm 4	0.5132*	0.0640	-0.1584	
Firm 5	0.592*	-0.0967	-0.1404	0.5187*

*Correlations between Firms 1 and 4, between Firms 1 and 5 and between Firms 4 and 5 were significant statistically relative to zero at the 0.01 level of significance.

Table 4: Frequency of Ratings across Factors of PaaS Study

	Firm 1	**Firm 2**	**Firm 3**	**Firm 4**	**Firm 5**
Ratings					

0	20.00%	16.67%	6.67%	23.33%	40.00%
1 – Very Low	3.33%			3.33%	
2 – Low	6.67%		13.33%		6.67%
3 – Intermediate	13.33%	10.00%	10.00%	6.67%	26.67%
4 – High	13.33%	10.00%	3.33%	3.33%	
5 – Very High in Significance	43.33%	63.33%	66.67%	63.33%	26.67%

Use of Preventative Measures to Protect Data Privacy on Mobile Devices

Jamie Pinchot
pinchot@rmu.edu

Karen Paullet
paullet@rmu.edu

Robert Morris University
Moon Township, PA 15108, USA

Abstract

This study examined mobile data privacy concerns as demonstrated by the use of preventative measures for protecting privacy on mobile devices among university students and alumni. Several preventative measures were explored, including techniques for browsing the mobile web anonymously, use of mobile apps that collect or share personal or private data, use of mobile apps that connect to social accounts, such as Facebook, use of social account logins for access to mobile apps, and use of location tracking device controls. A total of 187 participants were surveyed, including undergraduates and doctoral students and alumni at a mid-Atlantic university. The study found that among the preventative data privacy measures explored, participants were not as aware of anonymous mobile web browsing techniques and also tended to use social account logins for convenient access to other mobile apps despite the risk, even though concern for explicit connections to social accounts via mobile apps was displayed.

Keywords: mobile privacy, data privacy, mobile security, mobile apps, mobile devices

1. INTRODUCTION

The use of mobile devices has become common practice in the United States and around the world. As of December 2013, there were 345.2 million mobile subscriptions in the U.S ("Global mobile statistics", 2014). The increase in mobile devices has led to an increase in security threats. Only a small percentage, approximately 4%, of mobile devices are protected by security and anti-malware software. Protecting personal information has become an area of concern as increasing numbers of people use mobile devices. People commonly use their mobile devices to log into bank accounts, social networking sites and personal email accounts while connecting to free Wi-Fi or Bluetooth at the risk of exposing personal information.

Privacy is essential while communicating through mobile devices. As stated by Dotzer (2006), "Once privacy is lost, it is very hard to re-establish that state of personal rights." In order to protect personal information, users must become aware of the risks associated with using mobile devices.

2. RELATED RESEARCH

Mobile Privacy Concerns

One area of concern when thinking about privacy issues is the increase in popularity of mobile Online Social Networks (mOSNs) (Krishnamurthy & Wills, 2010). Facebook has announced that a quarter of their users visit online social networks via their mobile devices (Palihapitiya, 2010). As defined by Krishnamurthy and Wills (2010), there are two

classes of mobile OSNs. The first is the traditional OSN such as Facebook and Twitter, and the second is the growing list of mobile applications that were created to deal with mobile content. Even though mobile OSNs provide privacy settings, the nature of the environment makes it more difficult to protect personal information. Traditional pieces of personally identifiable information (PII), such as name, age, and gender have always been easy to track. With the increased use of mobile devices, user locations are now being exposed. Even when a user's exact location is not shown, information such as nearby gas stations, airports and restaurants can be found which can reveal the approximate location of the user. When connecting to mobile OSNs, personal information is being leaked to third party providers. This type of information can be used to link the user's browsing behavior with their actual identity (Krishnamurthy & Wills, 2010).

A study directed by Futuresight ("User perspectives", 2011) on mobile privacy sought to determine if users of mobile devices had privacy concerns when using Internet services and applications. The study was conducted for the Group Special Mobile Association (GSMA), which represents the interests of the worldwide mobile communications industry comprised of 219 countries. The study revealed that 92% of participants expressed concern about applications collecting personal information and 81% were concerned about location sharing applications or services.

Aldhafferi, Watson, and Sajeev (2013) conducted a study on personal information privacy settings for mobile devices. The researchers measured user awareness of protecting their personal information and the methods used to modify privacy settings when using social networks while connecting to the Internet on mobile devices. The results showed that most respondents use their mobile devices to check email, chat, and communicate via social network accounts. Over 67% of mobile users were interested in controlling privacy settings for their online accounts, while 59% actually took the time to change their settings in order to protect their privacy. Additionally, the study revealed that 66% of respondents were worried about the misuse of their personal information (Aldhafferi, et al., 2013).

The Advancement of Social Sciences Research Center (CASR) (2012) surveyed 838 smartphone users in regard to their habits and awareness of personal data privacy while using their device. The results showed that 57% of respondents had no idea what information was being obtained by third-party vendors when downloading applications to their smartphones. Approximately 56% of iPhone users and 51% of Android users were not aware that their contact lists stored on the device might be uploaded to the vendor's server. Forty-seven percent of users had not taken a single step on their smartphones, such as enabling screen locks, setting passwords, or installing anti-malware software, to protect the device and their privacy.

In February 2014, McAfee released their third mobile security report revealing that privacy-invading applications (apps) are on the rise. A staggering 82% of applications downloaded to mobile devices are tracking the end user. Of those downloaded apps, 35% contain malware. Malware is short for "malicious software" which can contain viruses, worms, spyware, and Trojan horses which can be launched on mobile devices. Most applications collect detailed information such as the user's exact location (GPS, longitude, and latitude), the user's general location via Wi-Fi or cell tower, as well as the user's last known location. Approximately 80% of apps collect location information, 55% continuously track location while the device is turned on, 26% know the user's SIM card number, 57% track when the device is in use and 36% know the user's mobile device account information (Asrar, et al., 2014). Users of mobile devices need to realize that their personal information is at risk when downloading mobile applications.

Many mobile applications now offer the ability to login with an existing social media account, such as Facebook, Google, or Twitter. The benefit of this approach is that the user can conveniently login with a username and password that already exists and that they presumably use regularly, so it will be easy to remember. However, using a social account to login to another mobile app essentially weakens the security for your social account as well as the security for the other app. If a social account is hacked, the hacker will then automatically gain access to all apps where the user utilized that same login. In addition, by linking accounts between social sites and other mobile apps, a user is adding to their public dossier. Data mining and other graph search techniques can

more easily track a user if their activities on multiple apps are tied together (Dale, 2013).
Barkhuus and Day (2003) studied users' privacy concerns when using location based services on their smartphones. The researchers analyzed location tracking services which are used by third parties for tracking an individual's movements and position awareness services that rely on the device's knowledge of its location. Research indicates that privacy is an essential issue when using location-based services (Snekkenes, 2001; Barkhuus, 2003), especially in determining how sensitive information is stored in the application.

A 2012 study set forth to measure users' confidence in smartphone security and privacy. Sixty smartphone users were interviewed about the actions they perform on their smartphones. The researchers found that users were less willing to shop, bank, provide their social security numbers, and access their health information on their smartphones compared to using their laptops (Chin et al., 2012). Participants were asked an open-ended question in regard to their primary concerns about using their smartphones. Some of the factors mentioned were theft and loss of the actual phone, data loss, physical damage, and trusting applications. The study found that users are more concerned about privacy on their smartphones than laptops. Installing applications on mobile devices has become an area of concern. The study explored how participants discovered the applications they installed on their smartphones. Approximately 80% of participants reported that they read customer reviews prior to installing the applications, while others reviewed the brand status. Very few participants read the privacy policies, end user agreements and terms of service prior to installing applications (Chin et al., 2012).

Protecting Privacy on Mobile Devices
Web surfers, including those using the mobile web, can use anonymous browsing to ensure that their activity on the web cannot be traced. People use anonymous browsing for both privacy and safety. If tracked, a person's search term history, web site use history, and other browsing habits could be used without their consent by profilers, Internet marketers, or even by people with criminal intent. Anonymous browsing allows the user to hide some actions on the web from marketers, profilers and other parties interested in collecting their data ("Anonymous browsing", 2014).

Anonymous browsing can be accomplished through proxy servers, which send information through a group of routers to prevent others from viewing a person's web history and activity. Many browsers such as Firefox and Chrome provide users an option to browse anonymously without leaving history or data such as cache or cookies behind after browsing ("Anonymous browsing", 2014).

Tor software is another option for anonymous browsing. Anonymity makes Tor an attractive tool for criminals (Dredge, 2013). Tor distributes transactions over several places on the Internet so that no single point can link users to its destination. Instead of taking a direct route to the end destination, packets on the Tor network take random paths to reach the final destination. This prevents the Internet Service Provider (ISP) and other people from monitoring the network to view what is being accessed.

Anonymous browsing can also be accomplished through the use of a personal virtual private network (VPN), which provides users with a secure connection over the Internet. Information sent using a VPN will encrypt the communication being transmitted from the user's device (Grueter, 2013). A VPN can connect a public network such as the Internet, to a secure private network. Mobile users can protect their privacy online while securing their communication. It is one of the best methods of protecting information since the user's IP address remains hidden and Internet traffic is encrypted. Many companies offer VPN services to their employees needing to connect to company networks. But, a growing use of VPNs is in the personal VPN area. An individual can purchase a VPN service for a very low monthly cost and then connect to their personal VPN from all mobile devices when they are accessing the Internet from a public Wi-Fi connection or another unprotected connection. Many personal VPN services also allow the user to connect through servers in a variety of countries, allowing the user to appear as a web browser from a different location when surfing the web. This can also help to protect the user's privacy, particularly by keeping their location private.

3. PURPOSE OF STUDY

The literature reviewed makes it clear that there is a high level of concern regarding privacy of data on mobile devices. This exploratory study sought to explore the use of common

preventative measures to protect data privacy on mobile devices among university students and alumni.

The following primary research question was explored:

Do university students and alumni use preventative measures to mitigate risk factors for the loss or compromise of private data on mobile devices?

4. RESEARCH METHODOLOGY

This exploratory study examined concern for mobile privacy issues as demonstrated by the use of preventative measures for protecting privacy on mobile devices among university students and alumni.

A quantitative method was utilized. The researchers implemented an anonymous electronic questionnaire to survey a convenience sample of undergraduate students, doctoral students, and doctoral alumni at a mid-Atlantic university in March and April of 2014.

Due to the exploratory nature of this study, the researchers wished to include as much diversity in the sample as possible. Undergraduate students were selected from core course sections required by the university or electives known to be taken by students in a variety of majors in an effort to capture a diverse group of students within the sample. Doctoral students and alumni from the information systems and communications areas were selected to be part of the sample to maximize diversity as well. The students and alumni of the doctoral program represent a variety of ages, ethnicities, and occupational industries and they live in a variety of locations across the United States. Responses were received from 138 undergraduates and 76 doctoral students and alumni. Participants were first asked if they owned a smartphone or tablet. Any participants who did not own a smartphone or tablet exited the survey, and these responses were discarded. After participants without a mobile device were removed from the data set, there were 114 undergraduate and 73 doctoral student and alumni responses, for a total of 187 (n = 187) participants. A pilot test was conducted with 61 adult participants prior to survey administration in order to test the validity and reliability of the questionnaire questions.

The anonymous electronic questionnaire included a variety of questions relating to mobile device usage, privacy concerns, and use of preventative security measures. Basic demographics were captured first, including age, gender, and occupational affiliation. Then, participants were asked about the types of smartphones and tablets that they own, broken down by device platform. The choices for smartphones were iOS, Android, BlackBerry, Windows Phone, Symbian and Other. The choices for tablets were iOS, Android, Kindle and Other. Next, participants were asked about their habits regarding the downloading of mobile apps, including whether they had ever downloaded an app, how often they download free and paid apps, and how often they download financial, health-related, social media, and productivity apps. These four categories of apps were chosen because of the sensitive nature of the data that is typically stored in these types of apps.

The next set of questions was targeted toward understanding the participants' usage habits regarding several preventative security measures related to mobile device privacy identified from the literature. First, participants were asked if they have ever used a special mobile web browser or setting, a personal virtual private network (VPN), or Tor software to access the web anonymously from a mobile device.

Some mobile apps allow users to login with an existing social account (such as Facebook or Google) rather than creating a new account specifically for the app. This can weaken the security of private data because a breach of one account can potentially allow access to many accounts. Participants were asked if they have ever used their Facebook or Google account to login to a (different) mobile app.

Next, participants were asked if they had ever decided not to install a mobile app because they found that personal information would have to be shared in order to use it. They were also asked if they had ever uninstalled a mobile app because it needed to connect to a social account (such as Facebook) or if they had ever uninstalled a mobile app because it was collecting personal information they did not want to share. Another question asked whether participants had ever turned off the location tracking feature on their mobile device because they were worried about other people or companies accessing that information. These

four questions were adapted from a previous Pew study (Boyles, Smith, & Madden, 2012).

Lastly, several questions relating to other mobile malware and security concerns were asked, but not utilized for this study.

5. FINDINGS

Of the 187 participants, ages ranged from 18 to 72, with a mean age of 32 years. The largest age group represented included 18-20 year-olds, at 31% of the sample. This skew toward the younger end of the age spectrum can largely be attributed to the 114 undergraduates included in the sample. Participants aged 21-30 comprised 25% of the sample, those aged 31-40 comprised 11%, those aged 41-50 comprised 18%, those aged 51-60 comprised 10%, and the remaining 5% included participants aged 61-72. The sample included more males, 66%, than females, 34%.

In terms of occupational affiliation, 36% of participants worked in industry (for profit), 30% worked in education, 17% indicated "other," 10% worked for government (local, state or federal), 4% worked in health care, and 3% worked for a non-profit organization. Nearly all of the responses in the "other" category came from undergraduates and can perhaps be attributed to the fact that many undergraduates were not working while attending school. In retrospect, a "not applicable" response was not included for this question but would have been useful.

All participants who were kept in the data set owned at least one mobile device. A majority of the participants, 94%, owned a smartphone and 63% owned a tablet. Nearly all of the participants, 96%, had downloaded a mobile app to their device. Of those who had downloaded a mobile app, the majority tended to download free apps more frequently than paid apps. More than half, 53%, downloaded free apps frequently or very frequently, 40% occasionally, 6% rarely, and 1% never. Only 7% downloaded paid apps frequently or very frequently, 19% occasionally, 43% rarely, and 31% never downloaded a paid app. Regarding types of apps downloaded, participants who had downloaded an app were asked how often they downloaded financial, health-related, social media, and productivity apps, since these categories of apps are the most likely to involve the use of private information. For financial apps, 39% downloaded them frequently or very frequently, 17% occasionally, 15% rarely, and 29% never. For health-related apps, 21% downloaded frequently or very frequently, 28% occasionally, 17% rarely, and 34% never. For social media apps, 71% downloaded frequently or very frequently, 13% occasionally, 10% rarely, and 6% never. And lastly for productivity apps, 36% downloaded frequently or very frequently, 28% occasionally, 18% rarely, and 18% never.

The research question asked, "Do university students and alumni use preventative measures to mitigate risk factors for the loss or compromise of private data on mobile devices?" To answer this question, the researchers looked at the responses to eight questions related to preventative measures for protecting data privacy on mobile devices.

The eight questions related to preventative measures focused on use of anonymous web browsing, use/installation of mobile apps perceived or known to be sharing private data, use/installation of mobile apps that require connections or logins linked to social accounts, and control of device location tracking features. Participants were asked if they had ever attempted to access the Web anonymously via their mobile device by using a special mobile web browser or setting, a personal virtual private network (VPN), or Tor software. They were also asked if they had ever decided not to install a mobile app because it required sharing personal information, or if they had ever uninstalled a mobile app because it was collecting personal information they did not want to share or required a connection to a social account such as Facebook, and if they had ever connected to another app using a social account login. Lastly, participants were asked if they had ever turned off location tracking on their device due to concerns about other people or companies accessing location information.

Use of Anonymous Web Browsing

Twenty-five percent (25%) of participants indicated that they have used a special web browser or setting on their mobile device to access the web anonymously, while 65% had not, and 10% responded that they did not know. Sixteen percent (16%) indicated that they had used a personal VPN to browse the web anonymously, while the majority, 76%, had not, and 8% said they did not know. Only 6% of the participants responded that they had used Tor software to access the web anonymously, while

84% indicated that they had not and 10% responded that they did not know.

In terms of understanding anonymous browsing, results show that among the sample population, use of basic techniques for anonymous access of the web is in the minority. In fact, the high responses indicating "I don't know" to each of the questions may point to an underlying lack of awareness of anonymous web browsing in general among the participants surveyed. It is unclear from the results whether participants may be unaware of the need for anonymous web browsing, or if they are aware of the need but have not been exposed to these common methods for accomplishing anonymity when browsing the web. Future studies could further explore this issue to pinpoint a level of awareness.

Use/Installation of Mobile Apps Perceived or Known to be Sharing Private Data

The majority of participants, 81%, responded that they had decided not to install a mobile app because they found out that they had to share personal information in order to use it. Sixteen percent (16%) indicated that they had never decided not to install a mobile app for this reason and 3% responded that they did not know.

More than half of the participants, 67%, said that they had uninstalled a mobile app because it was collecting personal information that they did not want to share. Twenty-nine percent (29%) indicated that they had never uninstalled a mobile app for this reason, and 4% responded that they did not know.

A clear majority of the sample indicated an understanding of the risks of using mobile apps that access or share private data. This is evident from their choice to not use or to uninstall any mobile apps that appeared to be sharing data in an undesirable way.

Use/Installation of Mobile Apps that Require Connections to Social Accounts

Most of the participants, 73%, responded that they had uninstalled a mobile app because they found out that they would need to connect to a social account, such as Facebook, to use it. Twenty-five percent (25%) noted that they had never uninstalled a mobile app for this reason, and 2% responded that they did not know.

Conversely, the majority of participants, 61%, displayed risky behavior, responding that they had used a social account, such as Facebook or Google, as a login for a different mobile app. Thirty-eight percent (38%) had never logged in to a different mobile app using a social account, and 1% indicated that they did not know.

The results in this area are mixed. Participants do demonstrate awareness of the risks involved with connecting to a social account such as Facebook or Google from a mobile app, but more than half of them have used a social account as the login to a different mobile app, effectively opening a possible connection to any personal data contained in their social account. Perhaps the convenience of a simple login without having to create another username and password for a different app prevailed over privacy concerns. Or perhaps participants are not aware that the use of their social account login could potentially allow a connection to their private social data. Future studies could specifically address the convenience factor of these types of logins versus the privacy risk.

Control of Device Location Tracking Features

The majority of participants, 76%, indicated that they had turned off the location tracking feature on their device due to a concern that other people or companies could access that information. Twenty-two percent (22%) responded that they had never turned off location tracking for this reason, while 2% said that they did not know.

Participants in the sample have clearly demonstrated a high level of awareness regarding the risks of sharing location data by indicating that they have turned off location tracking particularly due to privacy concerns.

6. LIMITATIONS

The primary limitation of this study was the small sample size. Due to the exploratory nature of this study, the convenience sample provided a good foundation for exploring this topic. Future work should consider incorporation of more participants from a variety of locations.

7. CONCLUSION

The majority of participants in this study demonstrated use of preventative measures to mitigate the privacy risks posed by mobile

location tracking, as well as mobile apps that access or share personal data. However, most participants did utilize the convenience of tying a social media account login to another mobile app, demonstrating either a lack of concern or awareness of the risks associated with this behavior. In addition, few participants demonstrated use of anonymous web browsing or anonymous web connection techniques, such as the use of a personal VPN.

The majority of participants were savvy enough to have uninstalled, or chosen not to install, mobile apps that appear to use or share personal data. This includes, in particular, mobile apps that require a connection to a social account such as Facebook in order to function. However, when other mobile apps ask to use a social account's login for access to the app, the majority of participants in this sample did use this convenience feature despite the privacy risk it could pose to any private data stored in their social account. This could indicate a preference of convenience over privacy concerns or a lack of awareness of the privacy risks taken when a connection is made between a social account and another mobile app.

Participants also demonstrated privacy concerns related to location tracking, with the majority noting that they had turned off tracking features on their mobile device due to a concern that others could access this information.

Finally, participants in this sample did not appear to be savvy about anonymous web browsing from a mobile device. Only 25% of the participants had ever used an anonymous web browser or setting to access the web, 16% had ever used a personal VPN, and 6% had ever used Tor software. It is possible that participants in the sample are not aware of the privacy risks related to browsing the web without the cloak of anonymity. Almost every action that you take, every search term entered, every web site surfed, is tracked. Without an anonymous browsing technique, all of a person's actions on the web could be collected and used for internet marketing, profiling, or perhaps even criminal uses. This study identified a lack of awareness of anonymous web browsing techniques. Future studies could further explore this issue to pinpoint whether the lack of awareness surrounds the need for anonymous browsing or the technical skills to accomplish it.

8. REFERENCES

Aldhafferi, N, Watson, C., & Sajeev, A.S.M. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. DOI: 10.5121/ijsptm.2013.2011

Anonymous Browsing. (2014). Retrieved April 22, 2014, from: http://cybersecurityprivacyfoundation.org/Anonymous%20Browsing.pdf

Asrar, I., Hinchliffe, A., Kay, B., & Verma, A. (2014, February 2014). Who's watching you? McAfee Mobile Security Report. Retrieved May 8, 2014, from www.mcafeemobilesecurity.com

Barkhuus, L. & Dey, A. (2003). Location-based services for mobile telephony: a study of users' privacy concerns. *Proceedings of Interact, 2003,* 709-712, Zurich, Switzerland, ACM Press

Bharti, A. K., Goyal, M., & Chaudhary, M. (2013). A Review on Detection of Session Hijacking and Ip Spoofing. *International Journal of Advanced Research in Computer Science*, *4*(9).

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and Data Management on Mobile Devices. Pew Internet & American Life Project. Retrieved June 30, 2014 from: http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

Centre for Advancement (2012, November). Privacy awareness survey on smartphones and smartphone apps. Office of the Privacy Commissioner for Personal Data. Retrieved from: http://www.pcpd.org.hk/english/publications/files/smartphone_survey_e.pdf

Chin, E., Felt, A.P., Sekar, V., & Wagner, D (2012). Measuring user confidence in smartphone security and privacy. *Symposium on Usable Privacy and Security (SOUPS)*, Washington DC.

Dale, K.Z. (2013). Log in with Facebook, Google+ or Twitter: Pros and cons. Retrieved March 2, 2014, from: http://www.chicagonow.com/listing-toward-

forty/2013/02/log-in-with-facebook-google-plus-twitter/

Dotzer, F. (2006). Privacy issues in vehicular and ad hoc networks. *Lecture Notes in Computer Science,* Vol. 3856, Springer 197-209.

Dredge, S. (2013, November 5). What is tor? A beginner's guide to the privacy tool. *The Guardian.* Retrieved May 8, 2014, from: http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

Escobar, E. (2013, March 6). The dangers of unsecured Wi-Fi hotspots. Retrieved May 2, 2014, from Quick and Dirty Tips website: http://www.quickanddirtytips.com/tech/mobile/the-dangers-of-unsecured-wifi-hotspots

Fedewa, J. (Ed.). (2014, May 6). Android antivirus: 6 truths about smartphone malware. Retrieved May 8, 2014, from Phandroid website: http://phandroid.com/2014/05/06/android-virus-malware-scan/

Global mobile statistics 2014 part A: Mobile subscribers, handset market share; mobile operators. (2014). Retrieved July 2, 2014, from MobiThinking website: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#mobilesecurity

Grueter, E. (2013, September 19). VPN Services: How they work, and why you're crazy for not using one. Retrieved April 21, 2014, from: http://www.doctrackr.com/blog/bid/336596/VPN-Services-How-They-Work-And-Why-You-re-Crazy-For-Not-Using-One

Krishnamurthy, B. & Wills, C.E. (2010). Privacy leakage in mobile online social networks. In *Proceedings of the 3rd Wonference on Online social networks* (WOSN'10). USENIX Association, Berkeley, CA, USA, 4-4. Retrieved May 9, 2014, from: http://web.cs.wpi.edu/~cew/papers/wosn10.pdf

Palihapitiya, C. (2010, February 10). Facebook Mobile: 100 Million and Growing. Facebook. Retrieved May 9, 2014, from: https://www.facebook.com/notes/facebook/facebook-mobile-100-million-and-growing/297879717130

Ruggiero, P., & Foote, J. (2011). Cyber threats to mobile phones. Retrieved April 29, 2014, from United States Computer Readiness Team (US-CERT) website: https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Skoudis, E. (n.d.). Defining mobile device security concerns. Retrieved May 9, 2014, from SearchSecurity website: http://searchsecurity.techtarget.com/answer/Defining-mobile-device-security-concerns

Snekkenes, E. (2001). Concepts for personal location privacy policies. *Proceedings of Electronic Commerce,* pp. 91-102, Tampa, Florida. Retrieved March 5, 2014, from: https://www.ansatt.hig.no/einars/papers/ACM_EC01_13_09_2001.pdf

Stern, A. (2013, April 15). Bluetooth connectivity threatens your security. Retrieved March 5, 2014, from Kaspersky Lab website: http://blog.kaspersky.com/bluetooth-security/

User perspectives on mobile privacy. (2011). FutureSight. Retrieved April 21, 2014, from Group Special Mobile Association (GSMA) website: http://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011

Cyber Security Best Practices: What to do?

Howard Kleinberg
kleinbergh@uncw.edu
Information Systems and Operations Management Dept.
University of North Carolina Wilmington
Wilmington, NC 28403

Bryan Reinicke
Rochester Institute of Technology
Saunders College of Business
Rochester, NY 14623

Jeff Cummings
cummingsj@uncw.edu
Information Systems and Operations Management Dept.
University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

While cyber security is an increasingly important topic for organizations globally, it is also a confusing one for both researchers and practitioners. A great deal has been written about cyber security, but there is comparatively little written about how to actually implement cyber security – specifically, who should actually do what. There also tends to be an assumption made that cyber security is simply something that the networking group will take care of, and is therefore put out of mind by most users and IT professionals. In this paper, we examine some of the suggested best practices for cyber security and suggest a framework for thinking about these practices. We also examine how cyber security tasks can be broken out by area of responsibility within an organization.

Keywords: security; cyber security; best practices.

1. INTRODUCTION

Information security has been a hot topic in the popular press, with revelations about the NSA's various programs (Gorman, 2008) and data breaches at large retailers in the US (Rawlings, 2013) being covered extensively. There has been an increasing level of interest on the topic, as the general public has realized that their data is, in fact, at risk in these types of incidents.

Information security, however, is a broad term that covers a wide range of topics and areas. One area receiving increased focus has been cyber security. Cyber security is a sub-set of information security that focuses specifically on those computing devices that are connected to the network, and how to secure them. Cyber Security is, without a doubt, one of the most critical aspects of the computer information systems world today. However, questions inevitably arise as to how to go about providing cyber security. For instance, how does one know what to protect? How does one go about determining how to protect one's information and information assets? What kinds of

measures, both technological and human, must be taken to safeguard both presence in and access to (and from) the Internet? How does one even know where to begin to do so effectively yet affordably and manageably?

In at least partial response to these "how to" questions, many standards and advisory bodies exist today. These organizations provide full 'bodies of knowledge' that enable organizations of almost any size and type to defend their information and systems, while operating in cyberspace. However, these bodies are all separate organizations, and incorporate entirely separate systems of thought and operation, oftentimes embodied in large volumes of guidelines, standards, and recommendations. In addition, these standards and recommendations are not presented in any type of standard format, leading to confusion for those trying to implement cyber security policies.

The purpose of this paper is to try to bring these various sets of best practice recommendations for cyber security together into a more approachable format for both practitioners and researchers in this field.

2. LITERATURE REVIEW

Information security is a very broad area of research, spanning any number of sub branches. The purpose of this paper is not to review and summarize every possible area of information security. Rather, this paper focuses specifically on aspects of cyber security. This choice was made to narrow the field of study to one that was both manageable and applicable for both researchers and practitioners. Recent reports of cyber-attacks against major retailers in the United States have emphasized the need for work in this area.

Cyber Security

There is surprisingly little academic research in the area of cyber security. This is likely because most of the focus in this area has been on the practical "how to" aspects of the field, rather than any sort of theoretical justification for performing certain tasks. This is an area that needs to be addressed, and we have presented some thoughts in the closing section of the paper on this.

While there is little academic research in the area, there are many practitioner articles and textbooks available (e.g. (Whitman & Mattord, 2010)). The attention to cyber security in industry press is understandable, as it has been called out as critical by heads of the NSA and CIA in the United States (Panchak, 2014). There are also frameworks dedicated to information security broadly, with applications to cyber security that are examined here.

Some of the notable frameworks in this area are the Control Objectives for Information and Related Technology (COBIT), the Information Technology Infrastructure Library (ITIL) and the ISO/IEC 17799 standards for Information Security Management (Saint-Germain, 2005).

COBIT is a framework for managing enterprise IT created and managed by the Information Systems Audit and Control Association (ISACA) and, as such, goes well beyond just information security. COBIT does have specific modules that deal with Information Security, Assurance and Risk (ISACA, 2014), and the framework is used extensively in industry (Turner, Oltsik, & McKnight, 2008).

The ISO/IEC 17799 standards are set by the International Organization for Standardization (ISO), and are the most complete framework available for information security management (Saint-Germain, 2005). The overall goal of the standards is to give companies standards for information security to allow them to comply with various regulations, and to allow them to create security that can be audited.

ITIL was originally developed by the British government to manage the IT resources for that nation. Since then, it has developed into an approach for aligning information systems services with the business processes they support. While it is not focused specifically on information systems security, security of information is one of the components for the framework.

In addition to these formal bodies of knowledge, there are other cyber security guidelines that are issued by companies like Invensys and Symantec's IT Policy Compliance Group. Each of these groups have different suggestions, but they all relate to cyber security. A summary of their recommendations is presented in the table found in the Appendix.

The table shows a compilation of very specific steps that organizations and individuals can take to implement cyber security measures. This is to be expected as many of these citations are based on practical experience, and an analysis of

security breaches in the public domain. As you can see from the citations in the table, many of their recommendations are overlapping, but are unstructured so that they are easily approachable from a research, or practice standpoint.

3. MAKING SENSE OF CYBER SECURITY

The literature review found a large number of cyber security best practices from numerous sources. What it did not find was a way to organize these items into an approachable list of best practices (see Appendix A for list). In this section, we will present two ways of organizing and approaching these best practices.

Area of Threat

While the list of possible actions to take to ensure some level of cyber security is broad, it is possible to organize and examine them in a logical way. For this paper, we have taken the approach of examining the policies, procedures and technology affected by the specific recommendations. After reviewing the best practices, we have broken them down by Hardware (HW), Software (SW), Antivirus (AV), Network (NW) and finally People, Policies and Procedures (P3).

Item	Best Practice	Tech Type
1	Inventory of Authorized and Unauthorized Devices	HW
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
7	Wireless Device Control	HW
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
23	Physical Facilities Security	HW, P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 2 – Hardware related best practices

We chose this method for several reasons. First, it provides a grouping for the best practices that naturally follows the breakdown of tasks in both industry and education for approaching technology. This, in turn, allows us to focus on how to approach the implementation or teaching of these best practices. This also has allowed us to reduce the best practices list down to manageable pieces. The original list of 30 is more than a little unwieldy – breaking it down by area makes it much more approachable. We have kept the item numbering the same as in Appendix A to make it easier to refer between the tables. There are a number of the best practices that reach across the different distinctions. For example, Information System Security Systems Design and Planning deals with multiple technology types including hardware, software, network, and people, policies and procedures. The best practices for Hardware are shown in table 2.

Many times when the topic of security arises the focus is on the user and what the user interacts with, i.e. applications. However, hardware plays a critical role in security and should be examined more closely as a tool for cyber security (Smith, 2004). Hardware includes various devices used within an organization that may be affected by cyber threats. Ensuring security of hardware devices is critical as this includes workstations and laptops containing organizational data as well as servers potentially containing customer data.

It is interesting to note that implementing hardware security is not simply configuring the hardware for access control – actually controlling the location of the hardware plays a role as well. Making sure that devices are physically secured (#23) plays a part. This is, obviously, made significantly more difficult due to the proliferation of mobile devices like smart phones that have enormous computing power, and incredible portability.

Security for hardware goes beyond how it is used. Security must be taken into account when hardware is being designed and built as well. There is a stream of research on how to design in security from the beginning with hardware (Smith, 2004). Clearly this isn't something that the average user will know about, but hardware plays a critical role in security and should be examined more closely as a tool for cyber security.

Table 3 shows the best practices that are related to software. Once again, the item numbering is the same as on the original table to facilitate comparisons between the different tables.

Some of these software best practices are items that are recommended for everyone (#8 Data Recovery – everyone should have a backup!), while others are oriented towards security professionals. This list again shows that there is

a range of tasks that need to be done to secure software.

Item	Best Practice	Tech Type
2	Inventory of Authorized and Unauthorized Software	SW
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3
8	Data Recovery Capability	SW
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 3 – Software Related Best Practices

One of the things that these cyber security best practices for software shows is that we need to build these security practices into the software while it is being built. We believe that this is important both for practitioners and educators. The practitioners need to create software with security in mind. Educators need to teach students to think about security when building software.

Item	Best Practice	Tech Type
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	NW
11	Limitations and Control of Network Ports, Protocols, and Services	NW
12	Controlled Use of Administrative Privileges	NW, P3
13	Boundary Defense	NW
19	Secure Network Engineering	NW
20	Penetration Tests and Red Team Exercises	AV, NW, P3
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 4 – Network related best practices

Table 4 shows the networking related best practices for cyber security. Not surprisingly, this list is longer than it was for either hardware or software.

Item	Best Practice	Tech Type
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3
9	Security Skills Assessment and Appropriate Training to Fill Gaps	P3
12	Controlled Use of Administrative Privileges	NW, P3
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	P3
15	Controlled Access Based on the Need to Know	P3
16	AccountMonitoring and Control	P3
18	Incident Response and Management	P3
20	Penetration Tests and Red Team Exercises	AV, NW, P3
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
22	Top-Down Implementation is Essential	P3
23	Physical Facilities Security	HW, P3
24	Combine Major Cyber Security Frameworks	P3
25	Centralized InfoSec Design, Planning & Implementation	P3
26	InfoSec Department Separated from IT Department	P3
27	InfoSec Department Reports Directly to CISO	P3
28	Compliance with All Required or Applicable Regulations	P3
29	InfoSec Implementation must be Consistent w. the Organization's Culture	P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 5 – People, Policies and Procedures best practices.

Security surrounding networks at organizations tend to be the primary focus of cyber security discussions. This is because attacks on networks tend to be the most publicized. Thus, as networks are at the heart of cyber space, their configuration plays a critical role in cyber security as well. Many of the recommendations for the networks deal with testing and remediation of issues for the network. This is to be expected as these threats evolve over time, and can change as hackers find new ways to breach security.

Table 5 shows the People Policies and Procedures best practices for cyber security. This is, by far, the longest list. What is interesting is that this seems contrary to expectations. Most people tend to focus on technology when cyber security is mentioned. However, when best practices are reviewed, it is policies and procedures that are most common.

This actually goes to something that has been noted in earlier research on security in general – your people are the weakest link (Ames, 2013). While part of this can be attributed to education and training for users, it also emphasizes the need for policies to be in place for enforcement. For example, many users continue to use weak passwords, despite the increase risk from hacking (Rashid, 2011), even though they are told not to. While we can't keep users from always doing this, we can put policies in place that force users to choose more secure passwords.

Level of Implementation

While breaking out the best practices by area of impact is useful, it highlights something else about the best practices. Having a secure company requires the efforts of every employee. After all, it only takes a single person clicking on a malicious link to compromise security. However, these best practices are clearly not going to be approachable by everyone. For example, how likely is it that an individual will run penetration testing on their home network?

This leads us to a second way of approaching the best practices: By level of implementation. Specifically, is this something that individuals should realistically be concerned with doing? Or is this something that would require trained professionals? We present a suggested breakdown at two levels. The first is at the individual level (what should each person do) in table 6. The second is at the organizational level in table 7.

Individual	
Item	**Best Practice**
5	Malware Defenses
6	Application Software Security
7	Wireless Device Control
8	Data Recovery Capability
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
15	Controlled Access Based on the Need to Know

Table 6 – Individual Level best practices

Many best practices for cyber security are suggested across multiple levels making it difficult for the layman user to understand what he/she should implement. While not everyone is a technical expert, everyone who has devices that connect to the internet is impacted by concerns with cyber security. This was the mindset that the authors used when trying to determine which best practices could reasonably be implemented by individuals.

For example, as most best practices would suggest, everyone should be running antivirus and antimalware software (practice #5) and you should always keep your software patched and up to date (practice #6). In addition, users should run frequent backups (#8), make sure their home wireless network are password protected (# 7 and 10) and passwords are not lying around as well as access to files are limited to the user (#15). This provides a very reasonable list that even individuals without extensive technical knowledge can perform on most modern operating systems fairly easily. If each individual followed these practices, there will be fewer security breaches at organizations, and fewer horror stories from users. Many of the other practices, however, are best left to the experts.

It should be noted that the assumption made here is that if the individuals should be doing it, then the organizations should as well. Thus, table 7 represents those best practices that should be implemented by organizations. Here, the authors tried to divide out those practices that were identified that should be done, but that are not reasonable to assume an individual user could or should do. While it is reasonable to assume that a large organization would audit their security procedures to ensure compliance with regulations (#28), it's probably not reasonable to assume that an individual could do this.

Organization	
Item	**Best Practice**
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
4	Continuous Vulnerability Assessment and Remediation
9	Security Skills Assessment and Appropriate Training to Fill Gaps
11	Limitations and Control of Network Ports, Protocols, and Services
12	Controlled Use of Administrative Privileges
13	Boundary Defense
14	Maintenance, Monitoring, and Analysis of Security Audit Logs
16	Account Monitoring and Control
17	Data Loss Prevention (DLP)
18	Incident Response and Management
19	Secure Network Engineering
20	Penetration Tests and Red Team Exercises
21	Information System Security Systems Design and Planning
22	Top-Down Implementation is Essential
23	Physical Facilities Security
24	Combine Major Cyber Security Frameworks
25	Centralized InfoSec Design, Planning & Implementation
26	InfoSec Department Separated from IT Department
27	InfoSec Department Reports Directly to CISO
28	Compliance with All Required or Applicable Regulations
29	InfoSec Implementation must be Consistent with the Organization's Culture
30	Maximize Use of Automation in InfoSec Implementations

Table 7 – Organizational level best practices

As noted in the previous section, many of these best practices are policies and procedures that the organization should put into place. This is to be expected, but it also is indicative of a need within organizations to have someone or some group that is responsible for creating these policies and monitoring their implementation. While this has been a constant recommendation, the sheer number of cyber security failures that make the news indicates that it is not a suggestion that is always followed by organizations.

4. CONCLUSIONS AND FUTURE RESEARCH

This article has pulled together suggested cyber security best practices from multiple sources and given two possible frameworks to examine them in. It is believed that this gives both researchers and practitioners a good base to build on when either teaching or implementing cyber security programs.

While conducting this research, we noticed a few gaps in the cyber security literature. One of the current gaps in cyber security research is that there is no theoretical basis on which to build upon. The research in this area has, to date, been primarily applied. While this makes sense, as cyber security is a very applied area, we also believe that this creates a problem for research in the area.

We believe that this is something that should be addressed by future research: the creation of a theoretical base for cyber security research to build on. This theoretical base could potentially be used to help organizations understand which cyber security practices would be most applicable to them. In the current research, we have provided a framework to categorize many of the best practices provided by practitioners.

Also, while this paper has presented a dividing line between organizations and individuals in this paper, additional refinement is required. After all, high net worth individuals, or those in great positions of responsibility, would likely need to implement additional security measures beyond the suggested individual measures presented here. Further research should be done to develop more of a "sliding scale" approach to determining when a given best practices should be put into place both for individuals and for organizations. This could potentially be linked with the theoretical basis for research that was mentioned earlier, thus providing theoretical justification for the sliding scale.

5. REFERENCES

Ames, J. (2013). Cyber security: Lawyers are the weakest link. [Article]. Lawyer, 27(44), 1-1.

Gorman, S. (2008). NSA's Domestic Spying Grows As Agency Sweeps Up Data. [Article].

Wall Street Journal - Eastern Edition, 351(57), A1-A12.

Invensys. (2012). Cyber Security Best Practices. Retrieved June 4, 2014, from http://iom.invensys.com/EN/pdfLibrary/ServicesProfile_Invensys_CyberSecurityBestPractices_06-12.pdf

ISACA. (2014). COBIT 5. Retrieved June 4, 2014, from https://cobitonline.isaca.org/about

Nicho, M. E. (2013). An Information Governance Model for Cyber Security Management. In D. Mellado, L. E. Sanchez, E. Fernandez-Medina & M. Piattini (Eds.), Cyber Security Governance Innovations: Theory and Research (pp. 155-185): AISPE.

Ortbal, J. (2010). Best Practices for Managing Information Security. ITpolicycompliance.com, 22. Retrieved from http://eval.symantec.com/mktginfo/enterprise/other_resources/b-best_practices_for_managing_information_security-february_2010_OR_2876547.en-us.pdf

Panchak, P. (2014). American CyberSecurity is a Big, Dangerous Deal for Business, IndustryWeek.

Rashid, F. Y. (2011). Password Security Remains the Weakest Link Even After Big Data Breaches. [Article]. eWeek, 28(11), 38-39.

Rawlings, N. (2013). Data Breach at Target Impacts Up to 40 Million Customers. [Article]. Time.com, 1-1.

Rembiesa, B. (2013). How to reduce IT security risk with IT asset management. Retrieved June 4, 2014, from http://searchsecurity.techtarget.com/tip/How-to-reduce-IT-security-risk-with-IT-asset-management

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. The Information Management Journal, 39(4), 6.

Smith, S. (2004). Magic Boxes and Boots: Security in Hardware. [Article]. Computer, 37(10), 106-109.

Team, V. R. (2013). 2013 Data Breach Investigations Report. 63. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Turner, M. J., Oltsik, J., & McKnight, J. (2008). Security Management Survey: ISO, ITIL and COBIT Triple Play Fosters Optimal Security Management. Retrieved June 4, 2014, from http://www.bsmreview.com/security_best_practice_survey.shtml

Whitman, M. E., & Mattord, H. J. (2010). Management of Information Security (3rd ed.). Boston, MA: Course Technology.

Editor's Note:

This paper was selected for inclusion in the journal as a CONISAR 2014 Meritorious Paper. The acceptance rate is typically 15% 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 2014

Appendix

Item	Best Practice	Cite
1	Inventory of Authorized and Unauthorized Devices	(Rembiesa, 2013)
2	Inventory of Authorized and Unauthorized Software	(Team, 2013)
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	(Rembiesa, 2013; Team, 2013)
4	Continuous Vulnerability Assessment and Remediation	(Invensys, 2012; Ortbal, 2010; Saint-Germain, 2005; Team, 2013)
5	Malware Defenses	(Invensys, 2012; Team, 2013)
6	Application Software Security	(Rembiesa, 2013; Team, 2013)
7	Wireless Device Control	(Rembiesa, 2013)
8	Data Recovery Capability	(Nicho, 2013; Team, 2013)
9	Security Skills Assessment and Appropriate Training to Fill Gaps	(Rembiesa, 2013; Team, 2013)
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	(Invensys, 2012; Team, 2013)
11	Limitations and Control of Network Ports, Protocols, and Services	(Invensys, 2012; Team, 2013)
12	Controlled Use of Administrative Privileges	(Saint-Germain, 2005; Team, 2013)
13	Boundary Defense	(Team, 2013)
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	(Invensys, 2012; Team, 2013)
15	Controlled Access Based on the Need to Know	(Rembiesa, 2013; Team, 2013)
16	Account Monitoring and Control	(Team, 2013)
17	Data Loss Prevention (DLP)	(Invensys, 2012; Team, 2013)
18	Incident Response and Management	(Saint-Germain, 2005; Team, 2013)
19	Secure Network Engineering	(Team, 2013)
20	Penetration Tests and Red Team Exercises	(Team, 2013)
21	Information System Security Systems Design and Planning	(Saint-Germain, 2005)
22	Top-Down Implementation is Essential	(Saint-Germain, 2005)
23	Physical Facilities Security	(Saint-Germain, 2005; Team, 2013)
24	Combine Major Cyber Security Frameworks	(Nicho, 2013; Turner, et al., 2008)
25	Centralized InfoSec Design, Planning & Implementation	(Ortbal, 2010)
26	InfoSec Department Separated from IT Department	(Ortbal, 2010)
27	InfoSec Department Reports Directly to CISO	(Ortbal, 2010)
28	Compliance with All Required or Applicable Regulations	(Saint-Germain, 2005; Turner, et al., 2008; Whitman & Mattord, 2010)
29	InfoSec Implementation must be Consistent w. the Organization's Culture	(Nicho, 2013; Ortbal, 2010)
30	Maximize Use of Automation in InfoSec Implementations	(Ortbal, 2010)

Table 1 – Summary of Cyber Security Best Practices