Journal of International Technology and Information Management

Volume 25 | Issue 3 Article 4

10-1-2016

An Exploration of Mobile Device Security Artifacts At Institutions Of Higher Education

Amita Goyal Chin

Diania McRae

Beth H. Jones

Mark A. Harris

AN EXPLORATION OF MOBILE DEVICE SECURITY ARTIFACTS AT INSTITUTIONS OF HIGHER EDUCATION

Amita Goyal Chin, Ph.D.
Associate Professor
Department of Information Systems
School of Business
Virginia Commonwealth University
P.O. Box 844000
Richmond, Virginia 23284-4000
agchin@vcu.edu

Diania McRae
Assistant Professor
College of Business
Department of Accounting, Finance,
Information Systems and Business Law
Western Carolina University
Cullowhee, NC 28723
828-227-3724 (office)
828-227-7584 (fax)
dlmcrae@wcu.edu

Beth H. Jones, Ph.D.
Professor
College of Business
Department of Accounting, Finance,
Information Systems and Business Law
Western Carolina University
Cullowhee, NC 28723
828-227-3465 (office)
828-227-7584 (fax)
bjones@wcu.edu

Mark A. Harris, Ph.D.
Assistant Professor
University of South Carolina
Integrated Information Technology
IT-ology Tower, Suite 1010
1301 Gervais Street
Columbia, SC 29201
markaharris@sc.edu

ABSTRACT

The explosive growth and rapid proliferation of smartphones and other mobile devices that access data over communication networks has necessitated advocating and implementing security constraints for the purpose of abetting safe computing. Remote data access using mobile devices is particularly popular among students at institutions of higher education. To ensure safe harbor for constituents, it is imperative for colleges and universities to establish, disseminate, and enforce mobile device security artifacts, where artifacts is defined as policies, procedures, guidelines or other documented or undocumented protocols. The purpose of this study is to explore the existence of, specific content of, and the general current state of published mobile device artifacts at higher education institutions. Results show that such artifacts are only sparsely available through public university websites, and even when available, rarely address mobile device security specifically.

KEYWORDS: mobile device, security, higher education

INTRODUCTION

The growth of mobile devices, including smartphones, tablets, gaming consoles, and e-readers has rapidly increased in recent years (Harris & Patten, 2014). Ericson (2015) predicts that smartphone usage will double to 6.1 billion subscriptions and total mobile devices in use will reach 9.2 billion units by 2020. The most popular operating systems for mobile devices are Google's Android OS and Apple's iOS, which account for 62% and 25% of the world market respectively (StatCounter, 2015). The app markets associated with these platforms are amassing exponentially. Apple's App Store has nearly 2 million apps and is increasing at a rate of 1000 apps per day (IBT, 2015). Google's Google Play market has 1.8 million apps and is also hastily swelling (Statista, 2015).

  ISSN: 1941-6679-On-line Copy

In juxtaposition with this precipitous growth in mobile devices and associated apps are the intensifying concerns as to the security of these devices, particularly with regard to the malware that may be installed on them. The total number of malware variants for mobile devices is near 8.5 million samples as of mid-2015 and that number is rising at a rate of over 1 million new variants per quarter (McAfee, 2015). A primary target for mobile malware is user login credentials, which are stolen and used for accessing the victim's finances and email, as well as other personal information (Kaspersky, 2015a). Nearly 30% of mobile users know little or nothing about mobile malware (Kaspersky, 2015b), and therefore, are readily susceptible to such cyberattacks. In spite of this, many users fail to institute even the simplest of precautions, such as activating user authentication for device access (Kaspersky, 2015b).

Given the undeniable explosion and rapid proliferation of smartphones and other mobile devices coupled with their persistent, commonplace use, organizations must exercise vigilance in mobile device security. This necessity envelops not only commercial enterprises, but also institutions of higher education, which are a stomping ground for a nomadic population of fearless and voracious consumers of bleeding edge technology. College campuses face a challenging dilemma. Institutions of higher education pose increased temptation and increased security risk for these institutions "possess a large volume and variety of sensitive information on a wide range of individuals, and demands for this information are growing (Cate, 2006)." Mobile devices, particularly smartphones, inarguably have a powerful and significant presence on campuses and are used not just for social interaction (Gikas and Grant, 2013), but also increasingly so for access to academic material, submission of work, online research, and for financial transactions. Furthermore, these devices, even more so than desktop PCs (Wong et al., 2015), are used for surfing on and interacting with websites, where a variety of security breaches including cross-site scripting (Hydara et al., 2015; Johns, 2014) can occur.

This substantial usage and penetration into mainstream daily life renders knowledge of and adherence to appropriate security measures and practices imperative. To help protect the rich assortment of sensitive data, colleges and universities must publish mobile security artifacts, where artifacts is defined as policies, procedures, guidelines or other documented or undocumented protocols that clearly address use, connectivity, access, etc. of any and all mobile devices. In this research, policies are seen as mandatory practices that must be followed and guidelines are seen as suggested practices that should garner adherence. Many organizations employ centralized software, such as mobile device management (MDM), that enforces various security covenants on mobile devices that connect to important organizational systems. In a university setting, this is often accomplished at the time

  ISSN: 1941-6679-On-line Copy

a user connects to the university WiFi or at the time a user adds a university account, such as an email account, to their mobile device. Relying on MDM for security, some organizations forego establishing published security policies directed at end users. Instead, these organizations often implement internal mobile security policies focused on the security staff that manages MDM, as suggested by the National Institute of Standards and Technology (NIST) (Souppaya, 2013). However, the stark reality that must be addressed is that a plethora of higher education users connect to systems that do not fall within the purview of MDM, including educational learning systems akin to Blackboard. Furthermore, users often forward university email to personal email accounts and use web-based portals to register for classes and view grades. These multifarious methods of accessing sensitive higher education data from mobile devices essentially circumvent MDM control. The necessity of clearly enumerated artifacts for mobile device security is indisputable. While the specific enforcement of pedantic adherence to any such artifacts will surely prove onerous, especially for personal devices without MDM, organizations should nonetheless make concerted efforts to at least avail such artifacts to their user communities. The purpose of this study, then, is to explore the existence of, specific content of, and the general current state of published mobile device artifacts at higher education institutions.

The remainder of this paper is organized as follows. The next section provides a contextual background and vets the current research within the context of previous literature. The following section enumerates essential facets of mobile device security artifacts. Then, we develop our research questions regarding the existence and specific constitution of security artifacts in institutions of higher education. We also develop our research hypotheses stemming from the research questions. The next section outlines our research methodology for the selection of participant colleges and universities. Our results and associated discussions follow. Finally, we offer conclusions and directions for future research in this area.

CONTEXTUAL BACKGROUND AND LITERATURE REVIEW

Perhaps no prior technology has more expediently and more universally and pervasively usurped the landscape than mobile technology. Mobile technology includes phones, tablets, personal digital assistants (PDAs), gaming consoles, and e-readers (Harris & Patten, 2014). Through decades of refined iterations, these devices have become so powerful, sophisticated, and versatile that they can oftentimes be used in lieu of laptops and desktops for many routine tasks including email, internet surfing, online purchasing, and online banking (Shaikh & Karjaluoto, 2015). It is expected that by 2020, "90 percent of the world's population over six years old will have a mobile phone (Fried, 2014)." To capitalize on this

trend, a large base of software applications has been established specifically for these devices. However, these applications and their associated hardware devices "require extremely high levels of security and privacy protection to prevent fraudulent or unauthorized use (Gragnaniello et al, 2015)."

Several security measures have been implemented to protect mobile devices (Hu et al., 2011; Olalere, 2015) and data sharing, particular in the context of cloud computing (Kumar, 2014; Li, 2013). At a minimum, protection is available in the conventional form of user login id and password to gain access. More sophisticated security implementations include biometric evaluation for access (Chen et al., 2012). For example, Apple began implementing fingerprint ID for access to its iPhone 5 and continued such security scrutiny for all successive iPhone models. Biometric systems, which take advantage of physical or behavioral traits of the user – e.g., voice, keystroke dynamics, gait, signature, fingerprint, palm print, hand geometry, vein pattern, face, ear, iris, and retina (Unar et al., 2014) – help to enforce security with minimal invasiveness to the user and hence, minimize erroneous input. According to Kharif (2015), "by 2020, half of e-commerce transactions over mobile devices will be authenticated using biometrics." However, even biometric systems have their shortcomings. In response to the fragility of biometric security systems, Gragnaniello et al., (2014) propose a very-low complexity iris liveness detector to thwart malicious attacks intended to surpass iris detection security protocols. Mira et al., (2015) also use human irises for biometric identification while Ntantogian et al., (2015) propose a two-factor authentication scheme based on gait, which can be observed unobtrusively. Fingerprint image security is explored in (Hsiao, 2015) and an algorithm is proposed to circumvent brute-force attacks.

Despite the substantial security hazards associated with the massive exposedness of personally owned mobile devices, colleges are abound with students employing such technological gadgetry for daily activities and all the while, being remiss in their security practices (Jones & Chin, 2015; Kim, 2014; Padilla-Meléndez et al., 2013; Mensch & Wilkie, 2011; Jones & Heinrichs, 2012; Shropshire et al., 2015; Jones et al., 2014) and in the online exposure of personal privacy (Harris & Chin, 2016; Furnell & Phippen, 2012; Kelly & Rowland, 2000; Marett et al., 2015; Wu et al., 2012; Harris et al., 2016a; Harris et al., 2016b). Technology has become so pervasive and integrated into curriculum that using electronic devices is essential for access to academic resources such as Blackboard and online coursework, particularly since curriculums of higher education are increasingly incorporating new methods of teaching and learning that are based on mobile access (Minaie et al., 2011), including collaborative and open learning (Liao et al., 2015). This level of amalgamation of technology and instruction has been shown to be vital to

learning and comprehension. The Campus-Class-Technology (CCT) Theory, for example, attempts to "explain the relationships between student engagement and technology theoretically (Gunuc & Kuzu, 2015)." That is, does the infusion of technology into the learning process enhance student interest and involvement, and therefore, yield more effective learning? Gunuc & Kuzu (2015) conducted an empirical study to test the CCT theory and determine the influence of technology on student engagement. They concluded that the use of technology such as laptop, internet, tablet PC, interactive whiteboard, smartphone, and slideware presentations, in class and out of class increased student engagement. Another study explored the role of mobile technology for mobile-learning, or m-learning, in higher education and concluded that mobile technology can "complement and add value" to the current learning models (Motiwalla, 2007).

Given the ubiquitous inhabitance of mobile devices and their unmitigated infiltration into academia, institutions of higher education must establish concise and exhaustive mobile security policies and then, must actively adjudicate compliance from the university community. While previous research establishes that managing information security is critically important (Nazareth & Choi, 2015), mobile security policies in higher education are only sparsely existent (Ismail & Zainab, 2013), and even then, are typically embedded in general security policies and fail to clearly disseminate guidance on mobile security practices. Doherty et al., (2009) recognized this gap and critically examined information security policies for both structure and content and concluded that policies, when in existence, are rather diverse, disparate, and lacking in standards. Furnell and Phippen (2012) evaluated privacy policies in terms of their presentation and complexity and determined that such policies lack standardization and are rather difficult to understand. Knapp et al., (2009) surveyed certified information security professionals to propose an information security policy process model to help identify key external and internal factors that can impact organizational security process.

The purpose of the current study is to explore the availability and ready accessibility of mobile device security artifacts at institutions of higher education. In addition, if such artifacts are successfully located, we delve into the intricacies of these artifacts to determine the specific issues addressed, and the alignment of these issues with those recommended in the contemporary research literature for such artifacts. These mobile security artifacts are of particular importance for their purpose is to propagate dogma and meticulously guide the online behavior of college students, who represent a segment of the population that is generally pioneering and zealous adopters of mobile technology. Students use mobile technology to interact socially through email, text and social media sites, including Facebook and Instagram, and

for personal activities including banking and other financial transactions. Therefore, it is vitally important to "protect their information and systems from possible security attacks (Kim, 2014)."

MOBILE SECURITY ARTIFACTS

The National Institute of Standards and Technology (NIST) issued a draft paper discussing the normative content of mobile device security artifacts (Souppaya, 2013). According to this document, organizations should utilize a centralized management system, such as mobile device management (MDM) to forcibly secure mobile devices that connect to sensitive networks or data. However, MDM can only force security artifacts on mobile devices under certain circumstances, such as when the device attempts to access university WiFi, a university account is added to the device, or the device is otherwise registered with the university. But MDM does not account for mobile devices that access sensitive data through other means, such as web portals. Getting these non-MDM controlled mobile devices secured needs to be done through other mechanisms. One such mechanism is to publish mobile security artifacts that users can use on their own to better secure their devices.

The following list of mobile device security considerations was adapted from Harris & Patten (2014). These security considerations are the minimum of what we expect to find published and available at higher education institutions.
(1) Do not jailbreak or root the device.
(2) Use a passcode or passphrase.
(3) Use inactivity timeout/autolock.
(4) Apply operating system updates regularly (or auto-apply).
(5) Encrypt data on devices.
(6) Use VPN (or other specified access) when accessing sensitive data over any non-secure network.
(7) Install antivirus/spyware software. Antivirus is not available for iOS devices.
(8) Use backup software for device data.
(9) Install data wipe software with the capability to erase data on lost or stolen devices.
(10) Avoid storing usernames, passwords, and pins on the device.
(11) Do not click on links in text messages and emails or open attachments from unknown sources.
(12) Beware of applications that request more permissions than necessary.
(13) Avoid untrusted third-party markets or developers.

ISSN: 1941-6679-On-line Copy

The Federal Communications Commission (FCC) also publishes a list of 10 steps to smartphone security (FCC, 2015). The list was compared to the items above and two new items emerged, creating a total of 15 mobile device security artifacts.
(14) Factory reset devices before donating, selling, or recycling.
(15) Report a stolen device.

RESEARCH QUESTIONS AND HYPOTHESES

College students use their mobile devices for such activities as emailing, viewing course management software screens, and paying fees and other bills due their university. Professors and other university staff routinely access course management software and if hacked, run the risk of unauthorized alterations to student grades with the possible exposure of confidential student information, which may constitute a violation of the Family Educational Rights and Privacy Act (FERPA) (Family, 2015). Administrators and their assistants have access to even a broader variety of sensitive data. If any of these parties access university data via a mobile device that has been compromised with malware a priori, the data they access as well as all system-wide data they have access to may be compromised. Personal phones belonging to these employees may also be lost or misplaced. These devices may house confidential data or have pin numbers and passwords coded on them for automated access to sensitive university data. Lost phones are cited as the top concern of the Security for Business Innovation Council – a team composed of Global 1000 information security leaders (BYOD, 2015). Yet another security issue is the assessment of data breach exposure on unmanaged BYODs. To quote Dave Martin, Vice President and CSO at Hopkinton, Massachusetts-based EMC Corp., "It comes down to losing control of your data. When email is retrieved and opened on a BYOD, I lose visibility into data access. In a phishing attack, I'd have no idea it even happened and I [would] lose any chance of [forensic investigation] (BYOD, 2015)."

Universities are also not immune to such dangers. An important feature of any risk-management strategy includes having a stated artifact (What's, 2011; Every, 2015) specifically in this case, a mobile device security artifact. However, a brief investigation in 2009 (Jones and Heinrichs, 2010) showed a glaring lack of such artifacts at universities. Since that time, there has been an explosion in the technology; one study, for example, found that in Spring 2009, approximately 47% of college students had smartphones and by Spring 2014 this percentage had jumped to 90% (Jones & Chin, 2015).

ISSN: 1941-6679-On-line Copy

The enormous growth in mobile device usage, in juxtaposition with the immense risks associated with the improper use of this technology, leads us to the following research questions:

RQ 1: Do most universities have mobile device security artifacts published online?

RQ 2: What security considerations do university mobile device security artifacts address?

One might expect that IT departments in large universities have more funds available than smaller institutions, and therefore, have more personnel available for tasks such as writing and monitoring data security plans. They also tend to have a greater number of student users, which could raise more of an IT security concern. With their larger budgets, greater student numbers, availability of IT personnel, and most likely, more expertise than the smaller schools, we would expect to find more national universities with mobile device security artifacts online than regional universities, and furthermore, we would expect to find that their artifacts are more complete. Therefore, we posit the following:

H1: Mobile device security artifacts will be more readily available for national institutions than for regional institutions.

H2: Mobile device security artifacts of national institutions will list more security artifacts than those of regional institutions.

RESEARCH METHODOLOGY

A stratified random sample of 50 national and 50 regional universities was selected from U.S. News and World Report's 2015 Best College Ranking (Best, 2015). National Universities are those that offer a "full range of undergraduate majors, plus masters and doctoral programs, and emphasize faculty research. National Liberal Arts Colleges focus almost exclusively on undergraduate education. They award at least 50 percent of their degrees in the arts and sciences (How, 2014)." Regional Universities rarely have doctoral programs and may offer some masters degrees, but the focus is on their broad scope of undergraduate degree programs. Regional Colleges, like National Liberal Arts colleges, focus on undergraduate education, but do not grant 50% or more of their degrees in liberal arts disciplines (How, 2014).

For convenience, the sample was selected from ranked schools only. To select schools from the list, the rankings of the national universities and national liberal

  ISSN: 1941-6679-On-line Copy

arts colleges were put in one numeric listing (national universities, in rank order, followed by national liberal arts colleges in rank order) and a random number generator (http://random.org/sequences) was used to select 50 random numbers between one and 379 for the 379 ranked national universities. The process was repeated for the 634 ranked regional universities and regional colleges.

According to the U.S. Digest of Education Statistics, there were 3,026 4-year institutions in 2012-2013 (Digest, 2015). Assuming this number approximates the 2015 count, we sampled 3.3% of all 4-year institutions. The U.S. News and World Report ranked 1,365 of these schools, omitting those that do not use SAT or ACT test scores in admissions, too few respondents to the peer assessment survey, fewer than 200 students, no first-year students, and a few other reasons. We saw a total of 1,054 schools ranked online; the difference between this number and the "1,365 ranked schools" claimed on the website is presumably due to the fact that U.S. News has a "Rank Not Published" designation included in their 1,365 but not actually ranked online (How, 2014). Of the 1,054 published rankings, our sample of 100 represents about 9.5%.

The vast majority of schools did not have a set of security artifacts specifically for mobile devices (schools who stated that their technology security artifacts covered mobile devices were considered to have a mobile device artifact). When no reference to a mobile device security artifact could be found, the search continued to see if at least a set of computer security artifacts was published online by that university. If this search also failed to produce the desired results, the search continued for computer usage artifacts. In one national university instance, viewing computer artifacts online required a password; therefore, this school was deleted from the sample.

RESULTS AND DISCUSSION

Research Question 1: Do most universities have mobile device security artifacts published online?

As stated previously, the authors looked first for any specific mention of mobile device security, whether this was contained in a separate artifact or as part of an overall technology security artifact. Out of the 99 schools searched, only 16 (16%) addressed the mobile device issue in any type of security artifact statement (Table 1). Ten of these were national universities and the other six were regional institutions. The answer to the research question appears to be "very few."

	National Universities	Regional Universities	Total

	Observed	Observed	
Found mobile device artifact	**10**	**6**	**16**
No mobile device artifact, but found computer security artifact	**13**	**9**	**22**
No mobile device artifact, no computer security artifact, but found published computer usage artifact	**13**	**14**	**27**
No mobile device artifact, no computer security artifact, no computer usage artifact found	**13**	**21**	**34**
Total	**49***	**50**	**99**

*One not usable in the sample of 50 because that school required a password to view its online policies.

Table 1: Results

In 2009, Doherty et al. reviewed online technology artifacts of universities in several countries (Doherty et al., 2009). Their search included "mobile device security" and they found that 11 of the 61 (18%) university technology artifacts reviewed mentioned mobile security. Their published work did not offer a breakdown by country, and therefore, a direct comparison to our study cannot be made. Nevertheless, it is clear that the situation has not improved greatly, if at all, from 2009. All the while, growth in mobile device usage has expanded.

Perhaps such a stammering lack of mobile device artifacts should come as no surprise, given that approximately one-third of the universities sampled had no technology artifacts whatsoever in place. They did not even have a usage artifact available online. A usage artifact (Doherty et al., 2011) is one where basic rules are stated such as the disallowance of illegal activities, pornography, harassment, hacking, introducing malicious software, fraud etc. on the university network and/or computing facilities.

Research Question 2: What security considerations do university mobile device security artifacts address?

From the online artifacts reviewed, we created a detailed list of the security artifacts found, which appears in table 2 below. The artifact features presented in this table are sorted by the number of policies in which they appear. The artifacts in bold are the fifteen minimum mobile security artifacts previously determined and listed above. The most important safety features are passcode, encrypted data storage, and the use of a timeout/autolock feature where the phone locks down after a period of inactivity and requires a passcode before it can be used again. Many policies

instructed users to contact the IT department if their phone was lost, stating that it might be necessary to remotely wipe data off of the phone. One artifact simply suggested that users remotely wipe all of the data on a lost phone. Another common suggestion was for users to set their phones to automatically apply system updates if the phone was not already preset to do so.

Mobile Device Security Artifacts	**National Universities Total**	**Regional Universities Total**	**Overall Total**
Use passcode	**9**	**5**	**14**
Encrypt data	**7**	**5**	**12**
Use inactivity timeout/autolock	**5**	**3**	**8**
What to do when phone lost or stolen	**4**	**3**	**7**
Apply operating system updates regularly (or auto-apply)	**4**	**3**	**7**
Comply with data security restrictions applicable to data stored	**4**	**3**	**7**
Keep physically secure	**4**	**2**	**6**
Activate 'find my phone' feature or app/engrave contact info	**4**	**2**	**6**
Do not share password or use one easily guessed	**2**	**3**	**5**
Enable the ability to	**4**	**1**	**5**

remotely wipe data			
Use anti-virus/spyware software	**3**	**2**	**5**
Use VPN (or other specified access) when accessing sensitive data over any non-secure network	**3**	**2**	**5**
Increasing delay/lock out after incorrect attempts OR require/recommend automatic wipe after so many failed attempts	**5**	**0**	**5**
Do not store sensitive university data on device	**3**	**1**	**4**
Disable wireless networking features not in use (Bluetooth, WiFi)	**4**	**0**	**4**
No jail-breaking or rooting	**3**	**1**	**4**
Be sure app should have permissions it is requesting before granting them	**2**	**1**	**3**

Either use a secure password manager or do not store usernames, passwords, pins, etc. on device.	**2**	**1**	**3**
Use backup software for device data	**2**	**1**	**3**
Includes FAQ/instructions for user	**3**	**0**	**3**
Do not click on links in text messages and emails or open attachments from unknown sources	**1**	**1**	**2**
Do not download third-party applications from Internet sources you are not sure you can trust (third-party developers)	**2**	**0**	**2**
Document serial # and IEME # of your device	**1**	**1**	**2**
When connecting to public WiFi, use only	**2**	**0**	**2**

known, encrypted, password-protected networks			
Rather than use null, set new password when establishing connection via Bluetooth	**2**	**0**	**2**
The policy will be "applied to device" (download? By IT in person?)	**1**	**1**	**2**
Change passcode at least once/year	**1**	**0**	**1**
Use two-factor authentication on the device if available	**1**	**0**	**1**
Do not get device from third-party stores	**1**	**0**	**1**
Remove university data not being used	**1**	**0**	**1**
Remove/uninstall apps, services not necessary for performing assigned work duties	**1**	**0**	**1**
Disable auto-join of newly discovered	**1**	**0**	**1**

wireless networks			
Wipe clean or factory reset when disposing of the device	**1**	**0**	**1**
Only approved devices can be used (mainly, which Operative System version)	**1**	**0**	**1**

Table 2: Features Present in Mobile Device Security Artifacts

Many security artifacts categorized data based on its sensitivity, which shows users which artifacts to consider most important. Security artifacts also often mentioned the methods by which users need to keep mobile devices secure including: have unshared passwords, activate the 'find my phone' feature to aid in tracking the phone in the unfortunate event of loss or misplacement and use VPN or other secured network access. In addition to the above research questions, the following hypotheses were evaluated:

H1: Mobile device security artifacts will be more readily available for national institutions than for regional institutions. (NOT SUPPORTED)

Table 3 below summarizes the number of mobile device artifacts found. Only 10 security artifacts were located for national institutions out of the sample of 49 (there may have been 11 as one school required a password to view artifacts and had to be dropped from the sample); the sample of 50 regional schools produced only six mobile device artifacts. The Pearson's Chi-Square test run to determine whether or not this amounted to a significant difference concluded the difference was *not significant* (p=.026). What is significant is the miniscule quantity of artifacts that are in existence and readily available online.

	National Universities Observed	Regional Universities Observed	Total
Mobile device artifacts located	**10** (7.92)	**6** (8.08)	**16**

	[0.55]	[0.54]	
No mobile device artifacts found	**39** (41.08) [0.11]	**44** (41.92) [0.1]	**83**
Total	**49**	**50**	**99**

Table 3: Mobile Artifacts by University Size

As Table 4 below shows, mobile device artifacts could take several different forms. Most often, for national institutions, this was a stand-alone artifact specifically addressing mobile device security (8 out of the 10 artifacts found). In the case of regional universities, 4 out of the 6 artifacts located were contained within the general computer security artifact; one was a standalone mobile device artifact and one was in more of a pamphlet form prescribing how to 'stay safe' with your mobile device.

	Total National Schools	Total Regional Schools	**TOTAL**
Mobile subsumed within general IT security artifact	**1**	**4**	**5**
Artifact covering personally owned laptops, other devices	**1**	**0**	**1**
Specific mobile device artifact	**8**	**1**	**9**
"Stay safe" online pamphlet	**0**	**1**	**1**
Total artifacts/other references to mobile security found	**10**	**6**	**16**

Table 4: Mobile Security Artifact Sources

H2: Mobile device security artifacts of national institutions will list more security artifacts than those of regional institutions. (NOT SUPPORTED)

The sizes of the samples being compared, i.e., n=6 and n=10 does not lend itself well to statistical analysis. Nevertheless, a Mann-Whitney-U test (a non-parametric test to compare two independent samples) was used to compare the total number of security considerations per artifact for national institutions vs. regional institutions. The z-score was 0.5423, giving a p=0.29 which, not surprisingly, is not significant. Other than the fact that it appears that national universities are more likely to have standalone mobile device security artifacts than regional schools, no other differences between them were found.

SUMMARY AND CONCLUSIONS

Smartphones have rapidly proliferated across all aspects of society, as has their commonplace use for personal, academic, and professional tasks. This necessitates proper consideration for the physical security of these devices, the protection of the data that resides on them, and the protection of the data that they access. This infusion of mobile technology raises concerns for business organizations, for they must address, among other modes of data access, the prevalent BYOD phenomenon. Oftentimes, businesses are unaware that personal devices are even being used to access company information, which is an important business asset that "requires special protection (Mesquida et al., 2015)."

In addition to the business world, institutions of higher education must grapple with the saturation of college campuses with mobile devices, and the impact that the routine use of these devices has on the security of university data and university systems. Patten and Harris (2013) proposed integrating mobile security education into the IT curriculum to help educate current students who will become future IT professionals. In so doing, colleges will help secure data access on their systems and will help the businesses that employ their students and graduates maintain a more secure environment. Educating educators also becomes a priority if information security is to be accomplished in academia. Commencing with establishing specific security parameters, a proper organizational culture must be developed and propagated. Once promulgated, knowledge of and adherence to appropriate security measures and practices could become more of the norm.

The extant research literature is consistent in that information security is a major concern (Montesdioca & Macada 2015; Harris et al., 2016b) and that security artifacts are needed to advise constituents on appropriate security behavior and practices when using mobile devices. "Two of the most important documents for ensuring the effective deployment of information systems and technologies within the modern business enterprise are the strategic information systems plan (SISP) and the information security artifact (Doherty & Fulford, 2006)." However, the current study clearly shows that universities are lagging dangerously behind the technology in devising, disseminating, and enforcing germane security artifacts. Very few universities have security artifacts publicly available on their websites, and of these, even fewer actually contain provisions specifically for mobile device security. The efficacy of any non-online artifacts that may be available is arguable, for stakeholders are most likely not even aware of their existence. Mobile device security artifacts should be readily accessible online, include detailed required/recommended security measures in elementary, easily-comprehendible

language and should embed links to detailed instructions for implementing the appropriate security procedures on a mobile device (e.g., how to set a passcode, how to enable encryption, how to set up the phone for automatic updates if not already preprogrammed, how to enable 'find my phone', etc.). Of the 100 security artifacts that were researched in this study, a few were complete, easy to read, and included useful links. These artifacts could be used as guidelines and springboards, omitting the need for others to "reinvent the wheel."

The present exploratory study was limited only to the artifacts that could be located online for the participating universities. Given the dearth of these artifacts, an extensive statistical analysis was not feasible. While it behooves institutions of higher education to avail their mobile security artifact online, it is possible that some universities have artifacts in existence that were not posted online. A future research study may extend the current work to include these artifacts as well.

Vital, unanswered questions for practitioners and educators to explore as future research may be the intrinsic reasons for the deficiency of established mobile device security artifacts. We suspect the absence of such documents does not result from a dereliction of due diligence but rather is an unfortunate effect of time and cost constraints. The situation may be further exacerbated due to a lack of expertise within the organization, a lack of support from upper management, or possibly, a lack of recognition and acknowledgement of the severity of the situation that has resulted from the unstoppable assimilation of mobile technology.

Another avenue for future research is to quantify the costs associated with the development of a comprehensive security artifact. A good security artifact requires an understanding of and a meticulous enumeration of the possible risks of mobile device usage, and a well-constructed response to each possible infraction. The creation of such an exhaustive artifact requires communication and prioritization of security solutions among IT personnel and its publication implies adamant commitment from upper management. Artifacts provide a place of reference for both IT personnel and users. When users follow artifacts, the increase in compliance can decrease the number of security incidents and decrease litigation as well. Research providing concrete examples in the form of case studies where security artifacts have altered negative outcomes would present a convincing argument in their favor.

Finally, another future research direction could evaluate the potency and efficacy of implemented security artifacts. Previous research (Jones and Heinrichs, 2012; Jones & Chin, 2015) suggests a significant lack of compliance among university students to security artifact recommendations. Research exploring behavioral

  ISSN: 1941-6679-On-line Copy

patterns and including suggestions for increasing compliance to security procedures would prove valuable.

REFERENCES

Best College Rankings and Lists. (2015). Retrieved from http://colleges.usnews.rankingsandreviews.com/best-colleges/rankings

BYOD security strategies: Balancing BYOD risks and rewards. (2015). Retrieved from http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards

Cate, F. H. (2006). The Privacy and Security Policy Vacuum in Higher Education. Educause Review, 41(5), 18.

Chen, C. L., Lee, C. C., & Hsu, C. Y. (2012). Mobile device integration of a fingerprint biometric remote authentication scheme. *International Journal of Communication Systems*, *25*(5), 585-597.

Digest of Education Statistics. (2015). Retrieved from http://nces.ed.gov/programs/digest/d13/tables/dt13_317.10.asp

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25, 55-63. doi:10.1016/j.cose.2005.09.009

Doherty, N., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*, 201-209. doi:10.1016/j.ijinfomgt.2010.06.001

Doherty, N., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*, 449-457. doi:10.1016/j.ijinfomgt.2009.05.003

Ericson (2015). Ericsson Mobility Report: 70 percent of world's population using smartphones by 2020. Retrieved 12-7-15 from http://www.ericsson.com/news/1925907

Every company needs to have a security program. (2015). Retrieved from https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Family Educational Rights and Privacy Act (FERPA). (2015). Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FCC (2015). Ten Steps to Smartphone Security, Retrieved 12-8-15 from https://www.fcc.gov/sites/default/files/smartphone_master_document.pdf

Fried, Ina (2014). More Than 90 Percent of U.S. Households Have Three or More Devices Pinging the Internet. http://www.recode.net/2014/11/18/11632960/more-than-90-percent-of-u-s-households-have-three-or-more-devices

Furnell, S., & Phippen, A. (2012). Online privacy: A matter of policy? *Computer Fraud & Security, 2012*(8), 12-18. doi:10.1016/S1361-3723(12)70083-0

Gikas, J. & Grant, M. (2013). Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media. *Internet and Higher Education*, 19, 18-26.

Gragnaniello, D., Poggi, G., Sansone, C., & Verdoliva, L. (2014, November). Contact lens detection and classification in iris images through scale invariant descriptor. In *Signal-Image Technology and Internet-Based Systems (SITIS), 2014 Tenth International Conference on* (pp. 560-565). IEEE.

Gragnaniello, D., Poggi, G., Sansone, C., & Verdoliva, L. (2015). Using iris and sclera for detection and classification of contact lenses. *Pattern Recognition Letters*.

Gunuc, S., & Kuzu, A. (2015). Confirmation of Campus-Class-Technology Model in student engagement: A path analysis. *Computers in Human Behavior, 48*, 114-125. doi:10.1016/j.chb.2015.01.041

Harris, M. & Chin, A. (2016). "Consumer Trust in Google's Top Developers' Apps: An Exploratory Study," *Information and Computer Security*.

Harris, M., Brookshire, R., & Chin, A. (2016a). "Identifying Factors Influencing Consumers' Intent to Install Mobile Applications," *International Journal of Information Management*, Vol. 36, No.3, pp. 441-450, http://dx.doi.org/10.1016/j.ijinfomgt.2016.02.004

Harris, M., Chin, A., & Brookshire, R. (2016b). "Mobile App Installation: the Role of Precautions and Desensitization," *Journal of International Technology and Information Management*, Vol. 24, No. 4, Article 3, http://scholarworks.lib.csusb.edu/jitim/vol24/iss4/3

Harris, M., & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management and Computer Security*, *22*(1), 97-114. http://dx.doi.org/10.1108/IMCS-03-2013-0019

How U.S. News Calculated the 2015 Best Colleges Rankings. (2014). Retrieved from http://www.usnews.com/education/best-colleges/articles/2014/09/08/how-us-news-calculated-the-2015-best-colleges-rankings

Hsiao, H. I., & Lee, J. (2015). Fingerprint image cryptography based on multiple chaotic systems. *Signal Processing*, *113*, 169-181.

Hu, G., Venugopal, D., & Bhardwaj, S. (2011). *U.S. Patent No. 8,087,085*. Washington, DC: U.S. Patent and Trademark Office.

Hydara, I., Sultan, A., Zulzalil, H., & Admodisastro, N. (2015). Current state of research on cross-site scripting (XSS) – A systematic literature review. *Information and Software Technology, 58*, 170-186. doi:10.1016/j.infsof.2014.07.010

IBT (International Business Times) (2015). Apple App Store growing by over 1,000 apps per day. Retrieved 12-7-15 from http://www.ibtimes.co.uk/apple-app-store-growing-by-over-1000-apps-per-day-1504801

Ismail, R., & Zainab, A. (2013). Assessing the status of library information systems security. *Journal of Librarianship and Information Science, 45*(3), 232-247. doi:10.1177/0961000613477676

Johns, M. (2014). Script-templates for the Content Security Policy. Journal of Information Security and Applications, 19, 209-223. doi:10.1016/j.jisa.2014.03.007

Jones, B., Chin, A., (2015). On The Efficacy Of Smartphone Security: A Critical Analysis Of Modifications In Business Students' Practices Over Time. *International Journal of Information Management (IJIM)*, 35(5), pp. 561-571, http://dx.doi.org/10.1016/j.ijinfomgt.2015.06.003.

Jones, B., Chin, A., & Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, *58*(6), 73-83.

Jones, B., & Heinrichs, L. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems (JCIS), 53*(2), 22-30.

Jones, B., & Heinrichs, L. (2010). Exploring Mobile Device Security Policies in Higher Education. Issues in Information Systems, XI(1), 204-210.

Kaspersky (2015a). Kaspersky Lab Reporting: Mobile malware has grown almost 3-fold in Q2, and cyberespionage attacks target SMB companies. Retrieved 12-7-2015 from http://www.kaspersky.com/about/news/virus/2015/Kaspersky-Lab-Reporting-Mobile-malware-has-grown-almost-3-fold-in-Q2-and-cyberespionage-attacks-target-SMB-companies

Kaspersky (2015b). A Quarter of Users Don't Understand the Risks of Mobile Cyberthreats, Kaspersky Lab Survey Shows. Retrieved 12-7-15 from http://www.kaspersky.com/about/news/virus/2015/Quarter-of-Users-Do-Not-Understand-the-Risks-of-Mobile-Cyberthreats

Kelly, E., & Rowland, H. (2000). Ethical And Online Privacy Issues In Electronic Commerce. *Business Horizons, May-June*, 3-12. doi:10.1016/S0007-6813(00)89195-8

Kharif, O. (2015). Mastering the Art of Palm Reading, Criminals are figuring out how to fool biometric systems. https://www.bloomberg.com/news/articles/2015-03-12/criminals-work-to-fool-biometric-security-systems

Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security*, *22*(1), 115-126. http://dx.doi.org/10.1108/IMCS-01-2013-0005

Knapp, K., Morris Jr., R., Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*, 493-508. doi:10.1016/j.cose.2009.07.001

Kumar, R., Gupta, N., Charu, S., Jain, K., & Jangir, S. K. (2014). Open source solution for cloud computing platform using OpenStack. *International Journal of Computer Science and Mobile Computing*, *3*(5), 89-98.

  ISSN: 1941-6679-On-line Copy

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.

Liao, Q., Luo, X., Gurung, A., & Shi, W. (2015). A holistic understanding of non-users' adoption of university campus wireless network: An empirical investigation. *Computers in Human Behavior, 49*, 220-229. doi:10.1016/j.chb.2015.02.044

Marett, K., Pearson, A., Pearson, R., & Bergiel, E. (2015). Using mobile devices in a high risk context: The role of risk and trust in an exploratory study in Afghanistan. *Technology in Society, 41*, 54-64. doi:10.1016/j.techsoc.2014.11.002

McAfee (2015). McAfee Labs Threats Report August 2015. Retreived 12-7-15 from http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf

Mensch, S., & Wilkie, L. (2011). Information Security Activities of College Students: An Exploratory Study. *Academy of Information and Management Sciences Journal*, *14*(2), 91-116.

Mesquida, A., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers & Security, 48*, 19-34. doi:10.1016/j.cose.2014.09.003

Minaie, D., Sanati-Mehrizy, P., Sanati-Mehrizy,, A., & Sanati-Mehrizy,, D. (2011). Integration Of Mobile Devices Into Computer Science And Engineering Curriculum. Proceedings of the 118th American Society for Engineering Education Conference & Exposition. Vancouver, B.C. Canada.

de Mira Jr, J., Neto, H. V., Neves, E. B., & Schneider, F. K. (2015). Biometric-oriented Iris Identification Based on Mathematical Morphology. *Journal of Signal Processing Systems*, *80*(2), 181-195.

Montesdioca, G., & Macada, A. (2015). Measuring user satisfaction with information security practices. *Computers & Security, 48*, 267-280. doi:10.1016/j.cose.2014.10.015

Motiwalla, L. (2007). Mobile learning: A framework and evaluation. *Computers & Education, 49*, 581-596. doi:10.1016/j.compedu.2005.10.011

Nazareth, D., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*, 123-134. doi:10.1016/j.im.2014.10.009

Ntantogian, C., Malliaros, S., & Xenakis, C. (2015). Gaithashing: a two-factor authentication scheme based on gait features. *Computers & Security*, *52*, 17-32.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open*, *5*(2), 2158244015580372.

Padilla-Meléndez, A., Aguila-Obra, A., & Garrido-Moreno, A. (2013). Perceived playfulness, gender differences and technology acceptance model in a blended learning scenario. *Computers & Education, 63*, 306-317. http://dx.doi.org/10.1016/j.compedu.2012.12.014

Patten, K. & Harris, M. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education*, *24*(1), 41-52.

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, *32*(1), 129-142.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191. doi:.1016/j.cose.2015.01.002

Souppaya, M., & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. *National Institute of Standards and Technology,* (NIST SP - 800-124 Rev 1). doi:10.6028/NIST.SP.800-124r1

StatCounter (2015). StatCounter Global Stats. Retrieved 12-7-15 from http://gs.statcounter.com/

Statista (2015). Number of available applications in the Google Play Store from December 2009 to November 2015, Retrieved 12-7-15 from http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern recognition*, *47*(8), 2673-2688.

  ISSN: 1941-6679-On-line Copy

What's a Security Policy and why do I need one? I'm only a small business. (2011). Retrieved from https://fightinginsecurity.wordpress.com/2011/08/15/whats-a-security-policy-and-why-do-i-need-one-im-only-a-smb-small-business/

Wong, K., Wang, F., Ng, K., Kwan, R. (2015). Investigating Acceptance towards Mobile Learning in Higher Education Students, *Technology in Education. Transforming Educational Practices with Technology,* Volume 494 of the series Communications in Computer and Information Science,9-19.

Wu, K., Huang, S., Yen, D., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*, 889-897. doi:10.1016/j.chb.2011.12.008