https://doi.org/10.48009/1_iis_2010_204-210

EXPLORING MOBILE DEVICE SECURITY POLICIES IN HIGHER EDUCATION

Beth H. Jones, Western Carolina University, bjones@email.wcu.edu
Lynn R. Heinrichs, Elon University, lheinrichs@elon.edu

ABSTRACT

With the explosive growth of smart phones and other mobile devices, mobile device security is now one of the top network security threats. Organizations must be vigilant in protecting sensitive data that might be stored on a device or transmitted to/from a device. Higher education communities have special challenges when it comes to preventing data exposure; they serve multiple audiences that dictate the need for numerous security profiles and have little control over end user devices. To ensure the protection of sensitive data, colleges and universities need security policies that specifically address the use of mobile devices. The purpose of this study is to explore the current state of mobile device security policies at institutions of higher education.

Keywords: mobile devices, security, policy

INTRODUCTION

The growth of mobile Internet computing has been no less than astounding. The mobile Internet is expected to be bigger than the desktop Internet by 2015 [11]. According to a Gartner forecast, 6.5 billion mobile connections are expected by 2014, and more than 3 billion people across the globe will bank and shop online [14]. Smart phones will continue to permeate our lives. They will replace wallets and keys. Smart phones and other mobile Internet devices (e.g. e-readers) will converge [8].

The growth of mobile Internet computing brings with it rising concern over mobile device threats and security issues. Gregg identified the growing number of smart phones and other mobile devices that connect with the Internet as the worst network security threat for 2010 [6]. The Georgia Tech Information Security Center (GTISC) identified "threats to VoIP and mobile devices" as one of the top five threats to information security [7] from problems such as malware, eavesdropping, phishing, and stolen or lost devices. Ogren [12] sees the real mobile security issues as "protecting the data that sits on the device for those inevitable occasions when it is left in the backseat of a taxi, protecting business applications from malicious activity, and reducing the cost of extending the infrastructure to include these phones."

Concerns over mobile security are gaining attention at institutions of higher education. Universities and colleges are among the most aggressive adopters of wireless technology as collaboration and open learning is fueled by the presence of mobile devices. One of the unique challenges that higher education institutions face is the need to accommodate access policies for many different groups including students, faculty, staff, visiting researchers, and members of the local community [1]. Lev Gonick, CIO of Case Western University, identified a top ten IT trend for 2010 as the year in which mobile security hits college campuses. "It's not a matter of 'if' mobile security headaches will bring down the wrath of audit committees and public exposures in the headlines of local and national media. It's only a matter of 'when'. My bet is 2010 [5]."

One tool in the battle to establish a secure mobile environment is implementation of a mobile device security policy. While most institutions probably have some type of policy that covers mobile devices, the policies can differ in terms of scope, specific recommendations, and availability. The purpose of the current study was to explore the status of mobile device security policies at institutions of higher education in spring 2010. The results of this preliminary study will serve as the basis for a broader study of mobile device policies in higher education, and also establish a data point for comparison in future studies.

BACKGROUND

The April 19, 2010, *Computerworld* headline, "Gizmodo paid $5K for next-gen iPhone [9]" was yet another reminder of how vulnerable organizations are to mobile device mishaps and why policies governing their use are a necessary component of any security strategy. Anybody can lose or misplace a cell phone, exposing a wealth of data such as credit card pin numbers, account numbers, customer emails, and so on.

Security Policy Components

A policy should contain three components [13]:

- Security.
- Responsibility and education.
- Enforcement.

"Security" should protect sensitive data that is at rest or in flight. *At rest* refers to data contained on the mobile device itself. *In flight* refers to data in transmission. "Responsibility and education" outlines specific roles and responsibilities of both the enterprise and the users, and educates employees on the content of the policy. Finally, enforcement specifies how policies will be carried out and the consequences of violations.

Security Practices

Specific practices for protecting data will vary from institution to institution, but guidelines and recommendations are not hard to find. Many of these practices can be incorporated into a mobile device policy.

Baseline Magazine [2] reports the following ten best practices recommended by security gurus, Tom Cross and Paul DeBeasi:

1. Select devices carefully.
2. Turn on encryption.
3. Require authentication.
4. Utilize remote wipe.
5. Set up a lost phone hotline.
6. Control third party apps.
7. Set unique firewall policies.
8. Use intrusion prevention software.
9. Keep an open mind about anti-virus software.
10. Shore up Bluetooth.

The first practice, selecting devices carefully, is underscored in a Computerworld article "Should Your IT department support the iPhone? [4]" While iPhones are popular smart phone choices, organizations that are concerned about HIPAA regulations have restricted iPhone access to sensitive data. Yet, it is often difficult for an organization to control the personal use of such devices. An approved list of devices can be included as part of a mobile policy.

Tauschek emphasizes the use of encryption (item two in the Cross and DeBeasi list) both for data at rest and in flight. To protect data at rest, a mobile policy should mandate 128-bit encryption for all devices that have the ability to store data. To protect data in flight, devices used for business purposes should be required to use encrypted network connections. A sample template for a mobile device encryption policy can be found at the SANS Institute Web site [3].

The use of software to beef up security (items four, six, eight, and nine in the Cross and DeBeasi list) is gaining momentum. Hackers can attack mobile devices through e-mails and on-line application stores. A wide-range of software options such as virus-protection, remote wiping, are available to organizations to thwart such attacks [10]. Deployment of such software can be specified as part of a mobile device security policy.

The bottom line is that a mobile device security policy can incorporate many different practices. The extent to which specific practices play a role in a particular policy depends on the organization. Colleges and universities are uniquely challenged because of their multiple constituencies and commitment to open learning. The purpose of this research was to conduct an exploratory study into the current state of mobile device security policies at institutions of higher education.

RESEARCH QUESTIONS AND METHODOLOGY

Colleges and universities typically publish their information technology policies on their Web sites. The authors were interested in the following basic questions regarding mobile device security policies specifically:

1. Are mobile device security policies typically included with the published IT policies?
2. What does the typical policy cover?
3. What similarities are there in policies? What differences?
4. Have policies been updated recently?

For this exploratory study, the authors chose to look at a small sample of 10 institutional policies.

DATA ANALYSIS AND FINDINGS

Data analysis began with a Google search using the keywords "mobile device security" (searched April 17, 2010; see Table 1). The plan was to examine the security policies of the first 10 U.S. institutes of higher education returned by the search. As it turned out, many of the links returned by Google pointed to

cell phone usage policies that covered such things as the circumstances under which the university will pay for employee cell phones, what the reimbursement procedures are, limits of reimbursement, if a carrier can be chosen by employee or if one is dictated by the policy, and so on.

Due to these 'usage' links, finding 10 security policies required visiting the first 18 university sites returned by the Google search (Table 1). The first 18 links returned by the search did include eight mobile security policy links. These university sites were visited to be sure these were the most recent policies (all eight were). The first 18 links also returned 10 'usage' policies. These 10 university sites were then searched for security policies. In two cases "best practices" related to mobile device security were found online for that university; in the other eight no mobile security policy was found. In these cases "Did not find security policy online" was noted in Table 2. The fact that a policy was not found does not guarantee one is not in existence at that university. It does mean that the policy could not be located using the university's search engine and links from its IT page.

After locating 10 mobile device security policies, the next step was to examine the policies to get an idea of their stage of development. Table 3 lists the 10 universities with security policies and gives an overview of the topical content of each policy.

To summarize the data in another way, Table 4 shows the number of university policies in our study that address selected security practices referred to by Cross and DeBeasi [9], Tauschek [3], or Kharif [10].

Table 4. Summary of Policy Content

Security Practice	No. of Policies (out of 10)
Approved devices	2
Encryption	5
Authentication	9
Anti-virus/malware software	5
Remote wipe/lost phone	8
Third party apps	4

It was not surprising to see that almost all (9 out of 10) security policies required password authentication. Perhaps more surprising was that the next most common practice was for policies to include lost device procedures and/or mention remote wipe capabilities. Universities seem reluctant to include a list of acceptable devices in their security policy. Perhaps this is because available devices change frequently, or universities are reluctant to favor certain devices over others, or they may not have the resources to spend time creating and maintaining such lists.

It was clear from reading these policies that some institutions' policies leave much to be desired. Two security policies seemed to be directed more at users with university-issued devices, did not cover all security aspects, and were not as clearly written as the more detailed policies. One policy only detailed what platform and devices would be supported; one put into place a password requirement only; one disclaimed with "*Should you wish to use a third-party client for advanced e-mail management, you do this at your own risk and assume your own support",* with no further discussion of security issues.

CONCLUSIONS

The purpose of the study was to explore the current status of mobile device security policies at institutions of higher education and seek answers to four basic questions.

1. Are mobile device security policies typically included with the published IT policies?
2. What does the typical policy cover?
3. What similarities are there in policies? What differences?
4. Have policies been updated recently?

While the sample selected for this study cannot be generalized to the entire population of U.S. universities due to its small size and potential selection bias, we can still glean useful information from the findings. First, it is clear that not all universities have a published mobile device security policy in place at the present time. This is a reasonable conclusion to draw given the fact the web search using the key words "mobile device security" returned more higher education usage policies than security policies, and it took searching 18 university sites to find 10 security policies. The answer to the first research question is: "when the policy exists, it does tend to be included with the published IT policies, but at the present time not all universities have such a policy".

There does not appear to be a "typical" policy at the present time. In our sample, half of the ten universities' policies had what the authors considered to be comprehensive policies covering such elements as passwords, anti-virus, encrypting data at rest and in flight, lost device policies and other best practices mentioned earlier in this manuscript.

In terms of policy dates, four were undated and six dated from 2007 to 2010. There did not appear to be any correlation between policy coverage and date; some of the most thorough were from 2007.

While the information gleaned by examining 18 sites and 10 policies does not provide a comprehensive look at the current state of mobile security policies, it does provide the context for developing a survey instrument that can be used for a more extensive study. The authors see the next step in this research focus as creating such an instrument that can be sent to chief information officers at colleges and universities.

REFERENCES

1. Brocade. (2009). *Wireless LANs in Higher Education (White Paper).* Retrieved 05 11, 2010, from Brocade Communications Systems: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1379874,00.html.
2. Chickowski, E. (2009, 02 26). *10 Best Practices for Mobile Security.* Retrieved 05 11, 2010, from Baseline Magazine: http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/.
3. Conrad, E. (2008, March). *Mobile Device Encryption Policy.* Retrieved 05 13, 2010, from SANS: http://www.sans.org/security-resources/policies/#template.
4. Faas, R. (2010, 01 12). *Should your IT Department Support the iPhone?* Retrieved 01 22, 2010, from ComputerWorld: http://www.computerworld.com/s/article/9142860/Should_your_IT_department_support_the_iPhone.
5. Gonick, L. (2010, 01). *2010: The Year Ahead for IT in Higher Education*. Retrieved 05 11, 2010, from Bytes from Lev: http://blog.case.edu/lev.gonick/2008/12/14/top_10_it_trends_for_higher_education_in_2009.
6. Gregg, M. (2010, January 28). *2010 Predictions: What's the Worst Network Security Threat This Year?* Retrieved 05 11, 2010, from SearchNetworking.com: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1379874,00.html.
7. GTISC. (2008, 10 15). *Emerging Cyber Threats Report for 2009.* Retrieved 05 11, 2010, from Georgia Tech Information Security Center: http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf.
8. Kavur, J. (2009, 12 04). *20 Mobile Trends and Future Technologies.* Retrieved 05 11, 2010, from CIO: http://www.cio.com/article/510076/20_Mobile_Trends_and_Future_Technologies.
9. Keizer, G. (2010, 04 19). *Gizmodo Paid $5K for Next-gen iPhone.* Retrieved 04 19, 2010, from Computerworld: http://www.computerworld.com/s/article/9175819/Gizmodo_paid_5K_for_next_gen_iPhone.
10. Kharif, O. (2009, 11 17). *Smartphones: A Bigger Target for Security Threats.* Retrieved 16 2010, 02, from Business Week Online.
11. Meeker, M., Devitt, S., & Wu, L. (2010, 04 12). *Internet Trends.* Retrieved 05 11, 2010, from Morgan Stanley: http://www.morganstanley.com/institutional/techresearch/internet_trends042010.html.
12. Ogren, E. (2008, 10 24). *Getting Enterprises Ready for Smartphone Security*. Retrieved 05 11, 2010 from Computerworld: http://blogs.computerworld.com/getting_enterprises_ready_for_smartphone_security.
13. Tauschek, M. (2008, 09 09). *Developing and Instituting Corporate Mobile Device Policies.* Retrieved 05 11, 2010, from SearchMobileComputing: http://searchmobilecomputing.techtarget.com/feature/Developing-and-instituting-corporate-mobile-device-policies.
14. Whitney, L. (2010, 14 01). *Smartphones to Dominate PCs in GartnerForecast.* Retrieved 05 11, 2010, from CNET.com: http://news.cnet.com/8301-1001_3-10434760-92.html?tag=mncol.

Table 1. Results of Google Search

	Universities Returned	Policy Links Returned
1	N. Mexico State U	http://ict.nmsu.edu/Guidelines/cell_policy12112007.shtml
2	Indiana University	http://www.indiana.edu/~vpcfo/policies/accounting/i-480.html
3	Villanova U	http://www.villanova.edu/unit/policies/mobiledevices.htm
4	Purdue U	http://www.purdue.edu/POLICIES/pages/information_technology/v_4_2.html
5	North Carolina Central U	http://www.nccu.edu/formsdocs/proxy.cfm?file_id=436
6	U of Kansas Medical Center	http://www2.kumc.edu/ir/operationalprotocols/mobilesecurity.asp
7	Tufts U	http://finance.tufts.edu/purchasing/?pid=16
8	Bradley U	http://www.bradley.edu/controller/docs/Mobile_Device_Policy.pdf
9	Central Florida U	http://policies.ucf.edu/documents/4-007SecurityofMobileDevicesFINAL.pdf
10	Towson U	http://www.towson.edu/adminfinance/OTS/aboutots/otspolicies/mobilecomputing.asp
11	Stanford U	https://itservices.stanford.edu/service/mobiledevice/cellular
12	N. Georgia College	http://www.ngcsu.edu/uploadedFiles/Administration/Human_Resources/845.0%20Mobile%20Communication%20Device%20Policy.pdf
13	U of New Mexico Health Science Center	http://hsc.unm.edu/library/kmit/docs/Procedures%20to%20comply%20w%20Mobile%20Device%20Standard%20TMG.pdf
14	Azusa Pacific U	http://www.apu.edu/imt/policiesandprocedures/mobile/
15	U of Portland U	http://www.up.edu/showimage/show.aspx?file=12520
16	Rockhurst U	http://help.rockhurst.edu/mail/phones/security
17	U of Detroit, Mercy	http://it.udmercy.edu/documentation/third_party_client_settings.htm
18	U of Tennessee	http://security.tennessee.edu/pdfs/SMDBP.pdf

Table 2. Type of Policy and Online Availability

	University	Type of Policy Google search returned	If Usage, could mobile device security policy be located online?
1	N. Mexico State U	Usage	Did not find security policy online.
2	Indiana U	Usage	Did not find security policy online.
3	Villanova U	Security	
4	Purdue U	Usage	Yes http://www.purdue.edu/securepurdue/bestPractices/mobileDevice.cfm
5	North Carolina Central U	Usage	Did not find security policy online.
6	U of Kansas Medical Center	Security	
7	Tufts U	Usage	Did not find specific security policy online. One reference within their Info. Security policy: **13. Laptop & Mobile Device Encryption:** All personal information stored on laptops or other portable devices, and all records and files transmitted across public networks or wirelessly, shall be encrypted to the extent technically feasible. (http://uit.tufts.edu/?pid=717)
8	Bradley U	Usage	Did not find security policy online.
9	Central Florida U	Security	
10	Towson U	Usage	Yes http://www.towson.edu/adminfinance/ots/gettingconnected/infosecandvirus/infsectraining/mobile.asp
11	Stanford U	Usage	Did not find security policy online.
12	N. Georgia College	Usage	Did not find security policy online.
13	U of New Mexico, Health Science Center	Security	
14	Azusa Pacific U	Security	
15	U of Portland	Usage	Did not find security policy online.
16	Rockhurst U	Security	
17	U of Detroit, Mercy	Security	
18	U of Tennessee	Security	

Table 3. Security Policy Content Summary

	University	Policy Date	Topical Coverage
1	Villanova U	Not dated	Per website: • Develop a clear policy on supported platform and mobile devices. • Identify the standard platform and set of supported devices. • Review current University policies on acceptable use and security to address mobile device issues. • Recognize mobile devices as compliment to PC / laptop. • Email on mobile devices (recommend reading/sending email on PC/laptop because of attachment compatibility). Policy only discussed first two points; no discussion of encryption, remote wipe, use of passwords or other security measures.
2	Purdue U	October 2008	Fairly thorough list of "best practices" for mobile devices. Use of passwords, encryption (both at rest and in flight), what to do if device is lost, wireless access disabled if not in use, confirm before connecting to network. No mention of remote wipe or virus protection.
3	U of Kansas Med Center	Not dated	Very detailed, lengthy, thorough security policy covering laptops as well as PDAs and smart phones. Encryption, passwords, what data can and cannot be stored on device, virus protection, etc.
4	Central Florida U	July 15, 2007	Another thorough policy; discusses five areas of risk: physical, unauthorized access, network, operating system or application, and mobile data storage device risk. Procedures addressing each risk are identified in the policy, including encryption, passwords, anti-virus/spyware/firewalls if available, who to notify if lost, etc.
5	Towson U	Sept 4, 2007	Like Purdue, Towson's mobile device security measures were listed under "best practices" rather than a university "policy" statement. Like all policies, much of the security is the responsibility of the user. Towson's list includes seven best practices for locking down Bluetooth and 14 best practices to protect mobile devices (passwords, firewall, anti-virus, encrypt transmissions and data on hard drive, turn off wireless if not used, etc.)
6	U of New Mexico Health Science Center	Not dated	Parts of policy refer to devices owned by the university (mobile devices must be locked in safe places, not loaned, marked as 'owned by university', anti-virus required). Some parts seem to apply to any mobile device, e.g., cell phones must be turned off at least one/week to receive security updates from provider, disable wireless when not in use, do not store ID on mobile device, etc. Not as thorough as other policies as much of it is directed only at university-owned PDAs and other mobile devices.
7	Azusa Pacific U	Mar 10, 2010	Not clear if this policy relates only to mobile devices purchased by the university or to individually owned devices as well. It seems to combine elements of both usage and security, and not in very specific terms. It is included here as a 'security' rather than 'usage' policy because it appears the intent of the policy is to cover mobile device security, e.g., it states "personal or confidential data must not be stored on mobile computing devices. In addition, all data stored on mobile computing devices should be backed up regularly" and "Given that Mobile Computing Devices may be storing and transferring critical APU data while connected to the internet, all APU Policies (Acceptable Use, Email, Data Security, etc.) are applicable and will be enforced. Mobile users must password protect access to stored information and take precautions to ensure the device is not lost or stolen." This is about all this policy says about security.
8	Rockhurst U	Mar 10, 2010	Policy that requires users to use a password or they will not be able to connect to the system, whether university or personally owned. Password length minimum,must be changed everyone 120 days, lockout procedure, who to contact if lost.
9	U of Detroit, Mercy	Not Dated	Policy is more of a disclaimer. "Please be advised, the ITS department strongly suggests users access their e-mail through the web-based interface at http://tc.udmercy.edu. Should you use a third-party client for advanced e-mail management, you do this at your own risk and assume your own support." No mention is made of the risk the university is assuming when users connect.
10	U of Tennessee	Mar 27, 2009	Detailed and thorough rules, applies to all lap-tops, PDA, smart phones whether owned by the university or individuals. Cover the type of information that may/may not be stored on device, what device can/cannot connect to, password, lockout, remote wipe if lost, physical security of device, etc.