2012

Business Practices and Procedures Regarding Smartphone Security

S. Ann Wilson
Nelson Rusche College of Business, Stephen F. Austin State University, wilsonsa@sfasu.edu

Michael York
Nelson Rusche College of Business, Stephen F Austin State University

Courtney Short
Nelson Rusche College of Business, Stephen F Austin State University

BUSINESS PRACTICES AND PROCEDURES REGARDING SMARTPHONE SECURITY

Ann Wilson, Stephen F. Austin State University
Michael York, Stephen F. Austin State University
Courtney Short, Stephen F. Austin State University

INTRODUCTION

Smartphones are having a transformational effect on the way that users access, use, and store information. Smartphones have essentially blurred the line of what is considered a phone, becoming the pinnacle multi-tasking devices of today's world. Current smartphones have their own dedicated operating system, Bluetooth capabilities, GPS, WiFi, constant network connection, PC connectivity, and are internet enabled, leading them to have similar security risks as that of a computer. Businesses are now worrying about the information employees are storing on these devices and want to find new ways to protect it (Schiller, 2011). Smartphone capabilities used for business application will be investigated for their potential vulnerabilities due to lack of employees' precautions and smartphone usage.

REVIEW OF LITERATURE

The first precaution employees and employers can take when using a smartphone for business use is to educate themselves in the areas that a virus can infect the phone. These areas include multimedia messaging system (MMS), Bluetooth, internet, syncing/docking, and peripherals. MMS messages are sent over the provider's cellular network, typically virus free, to exchange media files. However, Töyssys and Helenius (2006) note that, "malicious software can spread via MMS messages by attaching a copy of itself and sending it to some device capable of receiving MMS" (p. 111). Cheng, Wong, Yang, and Lu (2007) reaffirm this by pointing out that "the most well-known virus of such a kind is CommWarrior" (p. 259). Cabir, the first smartphone virus, was spread via Bluetooth (Töyssys, 2006, p. 111). However, a weakness of spreading the virus by the means of Bluetooth is that it must be in discoverable mode, which often times out, and the user must accept and install the incoming file. Similar to computers, smartphone users have the risk of downloading a virus from the internet that is masquerading as a game or some other application the user may find enticing. Since current smartphones are nearly always connected to the internet, it only amplifies the seriousness of the issue because it allows the virus to be in constant communication with the host. The Crossover virus was spread through syncing, when, "smartphones are connected to a computer in order to synchronize calendar events and new contacts," notes Cheng et al. (2007, p. 260). However, for this type of attack to succeed, the user's computer first must be infected. The final way a smartphone can be infected is through peripherals or removable media.

The more likely threat regarding smartphones is data confidentiality, with "Pointsec Mobile Technologies [estimating] that 60 percent of security breaches occur from device theft or loss, 25 percent due to network intrusions and viruses, and 15 percent from social engineering tricks" (Carson, 2006, p. 12). Data can be

compromised in a variety of ways such as "theft, inadvertent publishing, fraud, and uncontrolled employee behavior" (Collins and Vile, 2007). Unfortunately, this is where the biggest problem is for employers – the onus is on the employees for the greater part of data security.

To help prevent a breach in data, Allyson Garrone (2011) recommends the following: "define use-case requirements, create a mobile device security policy, enforce strong passwords, perform remote wipe, encrypt memory, enforce use of a virtual private network (VPN), perform regular backups, perform 'over the air' upgrades, remove residual application data, evaluate third-party products, and perform user education" (p. 3). The variety of smartphone OS's in use, such as Android OS, iOS, Windows Mobile OS, and Blackberry OS, make it challenging for IT departments to implement a single system due to the lack of compatibility with all devices. To aid with this dilemma, employers can issue employees a BlackBerry or a Windows Mobile device, as "most analysts agree that [these devices] provide the best inherent level of security" (Nelson and Simek, 2011). However, even if employers choose to take this route, they must be aware that employees may use their personal devices for business purposes, which are not likely to be as secure; furthermore, it begins to raise legal issues on how much control employer's can have access to these personal devices, even for security reasons.

This research indicates that with several possible infection methods, an anti-virus program for an employee's smartphone seems like a wise choice. However, the program has the challenge of working within the capabilities of the smartphone, while not hogging too many resources or draining battery life. It is perhaps due to these current limitations and drawbacks, that more users don't have an anti-virus program installed on their smartphone. In addition to an anti-virus program, the requirement of using a PIN to access the cell phone seems like a necessary precaution. Unfortunately, the annoyance of inputting a PIN before using the smartphone for anything typically deters most users from utilizing this long existing feature. To help discourage undesired use of smartphones, companies should utilize policies regarding business and personal smartphone usage regarding business information.

PURPOSE

The purpose of this paper is to examine real or perceived vulnerabilities and the lack of precautions that lead to security breaches resulting from increased availability and use of smartphones for business applications.

DESIGN OF THE STUDY

Alumni of a mid-size Texas public university will be asked to complete an anonymous online questionnaire asking the following questions:

1. Provide demographic information (gender, age, industry).
2. Do you have a smartphone?
3. What is your smartphone primarily used for?
4. Which type of smartphone operating system (OS) do you use?
5. How many years have you had a smartphone?
6. Does your company have a usage policy regarding a business-issued smartphone?
7. Does your company have a usage policy regarding a personal smartphone for business?

8. Have you ever, to your knowledge, had private information stolen while using your smartphone?
9. How concerned are you about having private information stolen from your smartphone?
10. Are you aware of any smartphone viruses?
11. Have you ever had a virus on your smartphone?
12. Do you use an anti-virus program on your smartphone?
13. What features on your smartphone(s) do you use the most?
14. Do you download apps on your smartphone?
15. Have you downloaded any apps to increase functionality on your smartphone(s) to aid in business tasks?
16. How often do you read the User Agreement license for the apps you download?
17. How concerned are you about getting a virus on your smartphone?
18. How concerned is your employer about getting a virus on your smartphone?

FINDINGS

The total number of respondents that screened into the survey was 29. In some isolated cases, answers were left blank. The results of the administered survey questionnaire are summarized as follows:

Gender:

Male	24 (70.6%)
Female	10 (29.4%)

Age:

18-25	4 (11.4%)
25-35	9 (25.7%)
36-45	8 (22.9%)
46-59	6 (17.1%)
60 or older	8 (22.9%)

Industry:

Education
Electronics/Computer/Software
Financial Services/Insurance
Healthcare/Pharmaceuticals
Management Consulting
Real Estate/Construction
Sales/Sales Promotion
Sports
Telecommunications
Television
Legal
Energy
Wholesale Distribution
Accounting
Oil and Gas
Manufacturing
Retired

Do you have a smartphone?

Yes	29 (82.9%)
No	6 (17.1)

What is your smartphone primarily used for?

Personal use	4 (13.8%)
Business use	0 (0.0%)
Both	25 (86.2%)

OS on smartphone?

Blackberry	6 (21.4%)
iPhone	22 (78.6%)
Android	3 (10.7%)
Other	0 (0.0%)

Years owning smartphone:

<1 Year	2 (6.9%)
1-2 Years	7 (24.1%)
2-5 Years	16 (55.2%)
>5 Years	4 (13.8%)

Company policy for business-issued smartphone?

Yes	8 (30.8%)
No	18 (69.2%)

Company policy for personal smartphones for business usage?

Yes	11 (40.7%)
No	16 (59.3%)

Private information stolen from smartphone?

Yes	0 (0.0%)
No	28 (100.0%)

Concern of private information stolen from smartphone

Not at all	3 (10.7%)
Not very	8 (28.6%)
Neutral	1 (3.6%)
Somewhat	11 (39.3%)
Very	5 (17.9%)

Aware of any smartphone viruses?

Yes	5 (17.9%)
No	23 (82.1%)

Had a virus on smartphone?

Yes	0 (0.0%)
No	28 (100.0%)

Use an anti-virus program on smartphone?

Yes	1 (3.6%)
No	27 (96.4%)

Most used features on smartphone (top 5)

E-mail	27 (96.4%)
Texting	26 (92.9%)
Camera	22 (78.6%)
Internet	22 (78.6%)
Calendar	21 (75.0%)

Download apps on your smartphone?

Yes	26 (92.9%)
No	2 (7.1%)

Downloaded apps to increase smartphone functionality for business tasks?

Yes	14 (53.8%)
No	12 (46.2%)

How often do you read the User Agreement license for apps?

Never	11 (42.3%)
Rarely	10 (38.5%)
Sometimes	3 (11.5%)
Often	1 (3.8%)
Always	1 (3.8%)

Concern of getting virus on smartphone:

Not at all	6 (21.4%)
Not very	8 (28.6%)
Neutral	2 (7.1%)
Somewhat	7 (25.0%)
Very	5 (17.9%)

Employer concern of smartphone virus:

Not at all	5 (18.5%)
Not very	7 (25.9%)
Neutral	7 (25.9%)
Somewhat	3 (11.1%)
Very	5 (18.5%)

The following significant findings were found:

Operating system regarding concern of private information stolen:
100% of Android OS users claimed to be at least somewhat concerned. 83% of Blackberry OS users claimed to be at least somewhat concerned. iOS users are split between being concerned and not concerned.

Operating system regarding concern of getting a virus:
100% of Android OS users are at least somewhat concerned. 67% of Blackberry OS users are at least somewhat concerned. 54% of iOS users are at most not very concerned, with 32% being at least somewhat concerned.

Length of owning smartphone and concern of private information stolen:
67% users that had the phone at least 5 years are not very/at all concerned. 100% users that had a smartphone less than a year are somewhat concerned. 71% of users that have owned a smartphone between 1-2 years are at least somewhat concerned. Users that owned a smartphone between 2-5 years are split.

Length of owning smartphone and concern of getting a virus:
67% of users that owned a smartphone at least 5 years are not at all concerned. All other users are split nearly 50/50 regarding concern.

Gender regarding private information stolen from smartphone:
72% of males are at least somewhat concerned, while only 33% of females are.

Gender regarding concern of getting a virus:
78% of women are not very or at all concerned of getting a virus. Men are nearly split regarding their concern.

Age regarding concern of getting a virus:
80% of respondents that are 60 or older are at least somewhat concerned. 67% of 26-35 and 36-45 users are not very or at all concerned. Users in the 18-25 demographic are split 50/50.

Age regarding concern of private information stolen:
Users of the 18-25 and 36-45 demographic are split 50/50. 80% of users over the age of 60 are at least somewhat concerned. 67% of users aged 26-35 are at least somewhat concerned.

SUMMARY OF RESULTS

Employees are becoming reliant on smartphones for business usage. The increased number of business smartphone users increases the likelihood of companies' data and information being exposed. Despite the increased risks, businesses at large have yet to implement policies for smartphone usage. While the lack of policies may seem counterintuitive, no respondents reported information stolen or viruses on their smartphone. One could assume that companies do not want to invest resources into areas that are of no immediate concern. While employers themselves do not seem concerned about private information being stolen, over half of respondents are at least somewhat concerned over the respective issues. Respondents are minimally aware of smartphone viruses, and employers could use the opportunity to utilize smartphone usage and security awareness programs. These programs could inform employees of proper smartphone usage and risks and security measures to protect data on smartphones.

REFERENCES

Carson, P. (2006, July 31). Device security demands precious processing power. In *News Bank Access World News*. Retrieved October 5, 2011, p.12

Cheng, J., Wong, S., Yang, H., Lu, S. (2007, June). SmartSiren: Virus detection and alert for smartphone. The 5th International Conference on Mobile Systems, Applications, and Services, San Juan, Puerto Rico. doi:10.1145/1247660.1247690

Collins, J., & Vile, D. (2007, June). Mobile security: A primer on the security of mobile devices, and the implications for enterprise IT. In *The Register*. Retrieved October 4, 2011, from http://whitepapers.theregister.co.uk/paper/download/delayed/210/001-mobile-security-2.0.pdf

Garrone, A. (2011, March). Best practices for mobile devices and smartphone security in the workplace. In *Compliance Maven*. Retrieved October 5, 2011

Nelson, S., & Simek, J. (2011, March). How smartphones threaten business security: Coming to grips with the facts [Electronic version]. *Law Practice: The Business of Practicing Law*, *37*(2), 24-26.

Schiller, K. (2011, March). Moving target: Security risks and the mobile work force. *Information Today*, *28*(3), 1, 35-36.

Töyssy, S., & Helenius, M. (2006). About malicious software in smartphones. *Journal in Computer Virology*, *2*(2), 109-119. doi:10.1007/s11416-006-0022-0