Blackberry and Handheld Devices: Management Productivity Aid or Cyber-Crime Tools?

Nick Nykodym
Professor of Business & Innovation, The University of Toledo, Ohio USA
E-mail: nick.nykodym@utoledo.edu

Sonny Ariss
Professor of Business & Innovation
The University of Toledo, Ohio, USA

Michael P. Hoffman
Research Associate, College of Business & Innovation
The University of Toledo, Ohio USA

Kihyun Park
Research Associate, College of Business & Innovation
The University of Toledo, Ohio USA

Received: September 23, 2011 Accepted: November 24, 2011 Published: March 1, 2012
doi:10.5539/jpl.v5n1p139 URL: http://dx.doi.org/10.5539/jpl.v5n1p139

Abstract

Handheld devices such as mobile phones and PDAs have permeated organizational daily life along with the growth of information communication technologies. In this analysis, the researchers will explore the advantages and disadvantages of the use of these handheld devices, and possible sources of cyber-crime. Also, several solutions and strategies are suggested for dealing with cyber-crime. This research is a study to investigate the nature of handheld devices and cyber-crime, future research opportunities reside in the area of cyber-crime prevention strategies from a management standpoint and legislation from government agencies.

Keywords: Smartphones, The Virtual Organization, V. O., Electronic communication, Employee trust, Professional interaction, Professional expectations, Digital forensics, Blackberry, IPhone, Cyber-crime

1. Introduction

With increasing use, handheld devices such as mobile phones and PDAs (personal digital assistant) have permeated our daily life. These devices have been adopted and implemented in various for-profit business activities such as commerce, production, and logistics; as well as non-profit organizational activities such as education and healthcare organizations. Gartner and Alternative Resources Corporation (ARC) Group (2009) reported that smartphone use is expected to consist of 20% of the entire mobile phones shipping which amounts to 1 billion by 2009.

A smartphone can be defined as a cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as any combination of text messaging, e-mail, Web browsing, still camera, video camera, MP3 player, video player, television and organizer. In addition to their built-in functions, smartphones have become application delivery platforms, turning the once single-minded cellphone into a mobile computer (PC Magazine, 2010).

Siegmund, Floerkemeier, and Vogt (2005) indentified characteristics of handheld devices such as habitual presence, perception, mobility, computational resources and regularly refilled mobile energy reservoirs user interface and input capability, and personalization in smart environment. Unlike desktops and laptops, handheld devices can be easily carried around by their owners. This presence enables handheld devices to function as a mediator between users and

background infrastructure services. Cellular phones can be utilized as remote location sensors for understanding the environment. Regardless of their current location, handheld devices gain mobility. With keyboards, buttons, or a touchscreen they serve as a user interface and achieve input capability. Also, they can be personalized and customized to the extent which users implement functions exclusively for themselves since they often do not share the devices with others.

Chang, Chen, and Zhou (2009) identified nineteen features for the ideal smart phone: 1) Multi-tasking operating system; 2) Powerful SOC (System on Chip) application processor and DSP (Digital Signal Processing) communication processor; 3) Larger display with high screen resolution; 4) Internet access at 2.5 or 3 Gigabyte speed; 5) Real QWERTY keyboard; 6) E-mail, SMS, MMS (Multimedia Messaging), IM(Interactive Media) services; 7) Business productivity tool; 8) Host synchronization; 9) PIM (Personal Information Management); 10) WiFi for VoIP (Voice Over Internet Protocol) and Bluetooth for cable replacement; 11) Voice communication and voice-mail; 12) Camera; 13) Gaming; 14) File management and manipulation; 15) Video/audio streaming; 16) GPS; 17) Music player and mobile TV; 18) Open standard IO (Input/output) communication and storage expansion; and 19) RFID and biometric features like fingerprints. Chang et al (2009) suggest that the first eleven are must-have features and the last eight are desire-to-have. Chang et al (2009) also considered well-known mobile phone operating systems such as Blackberry OS, Nokia Symbian, Apple iPhone OSX, Google Android and others.

1.1 Advantages of Handheld Devices?

According to an analysis by Frost and Sullivan, a European mobile/wireless healthcare technology company, the market value of total mobile/wireless technologies in Europe during 2008 amounted to $1,479.2 million and is expected to reach $6,791.7 million by 2015 (Feick, 2009). Handheld devices have been regarded as emerging technologies in various areas such as education, healthcare, commerce, and others.

The advantages handheld devices entail can fall into three categories: 1) ubiquitousness, 2) convenience, and 3) cost (Locsin, 2004). Ubiquitousness allows users to not be confined by time and location. Handhelds allow users to have mobility and accessibility for obtaining necessary information anytime and anywhere they want (Is4profit, 2004). Handhelds offer the user convenience because they are usually easy to hold, learn and implement. Lastly, compared to desktops and other devices, user can achieve cost efficiency by using handhelds which are frequently less expensive than other computing devices.

Mahatanankoon, Wen, and Lim (2005) found five advantages from handheld mobile devices in developing mobile commerce or m-commerce using mobile devices: 1) always on, 2) location-centric, 3) convenience, 4) customization, and 5) identifiability. A mobile phone is portable and always on, so this allows users to access the Internet and provides the opportunity to purchase products. Identifying its users' location, an m-commerce service provider can meet their diverse and changing needs, allowing them to personalize their available services accordingly. Customized service and better service quality will therefore, enhance customer loyalty.

The adoption of technology in the health care industry has been shown to be of benefit for healthcare workers performing their job duties. Lapinsky, Weshler, Mehta, Varkul, Hallett, and Stewart (2001) argued that limited computer accessibility impeded clinicians from the full extent of computer use and handheld devices could be a solution to this situation. Physicians are using handheld computing technology for diverse functions such as patient data storage, scheduling, billing, and assessing drug reference information. According to Ebell and Rovner (2000), handheld devices are versatile, relatively inexpensive and able to combine electronic patient records and paper charts.

Several advantages of handheld devices can also found in the educational environment. Becta Company (2005) suggested that they can be used either inside or outside of the school. They are not confined by time and location providing wireless mobility at fast speed. They do not take up much space, so physical storage of devices such as lab and classroom and electrical connection are not necessary. Instant-on is another advantage when compared to desktop and portable computers because handheld devices are very quick to turn on and boot up.

1.1.1 Disadvantages of Handheld Devices

There are several disadvantages from handheld computer devices use. They are grouped into different categories such as 1) set up cost, 2) improper use, 3) battery life, 4) limited display 5) loss and theft and cybercrime.

Although mobile phones have become common and popular, some handheld devices such as PDA's (personal digital assistant), also known as a palmtop computer, are still costly to purchase starting at $100 for low end models. Because some parents cannot afford a $100 machine for use in an educational setting, some students must go without. Purchasing and setting up handheld devices for members at any laboratory or department (i.e. hospitals and companies) require management decisions and enough investment accordingly. Also, additional money must be spent in purchasing the related software such as operation systems and establishing network in enabling them to be

implemented.

Shields and Poftak (2002) mentioned three types of the improper use of handheld devices by students. The first one is that some schools report students engaging in other activities such as playing games and sending text messages. The second is an instance that a student programmed his devices on his own and changed the channels on his classroom television. Lastly, possible cheating on exams by students is a serious disadvantage of handheld devices.

Usually, the plug-in terminal and adapter have a finite lifecycle. Although, it is constantly improving, the life of a battery in a handheld device is still a big issue. Due to the small screen, it is inconvenient to type, edit, and read a lot of text. In order to see the whole text, users must scroll down very often. Farke, Sielaff, Franke, Geogler, and Fischer (2008) indentified 5 disadvantages of handheld computers for medical documentation: 1) insufficient memory (dependent on handheld type), 2) difficult to type (replay function of handheld inferior to laptops), 3) need for training, 4) network connection for handhelds more difficult than laptops, 5) handheld dictation function not user friendly, and 6) few software installations in basic configurations.

Mandryk, Inkpen, Bilezikjian, Klemmer, and Landay (2001) indentified two drawbacks of students' use of handhelds which are: "1) achieving the benefits of collaborative learning may be difficult given the personal nature of these devices, and 2) the small size of a PDA constrains the amount of information that can be meaningfully displayed." (p.225)

Finally, loss and theft can occur in using handheld devices. They are more likely to be lost, stolen, and damaged by users. In schools, students tend to forget their devices in the classroom when they leave. Even if teachers are fully ready to teach expecting their students to secure their devices, problems can happen.

1.1.2 The Possible Sources of Cyber-Crime from Handheld Devices Such as I-Phone and Blackberry:

Although the threat of cyber-crime on handheld devices is thought to be relatively minor (Fong, 2008) the danger is ever present. The possible cyber-crimes associated with handheld devices include counterfeiting, identity theft, drugs, software piracy online fraud, gambling, stalking, e-mail threat, prostitution, child abuse terrorism and so on. Shin, Lin, Chiang, and Shih (2008) identified cyber threats of mobile virus against mobile phone use. Mobile viruses can hamper the performance of devices, cause basic functions to become disabled, and take up memory space. Beken and Balcaen (2006) explicated crime opportunities in mobile phone sector: 1) The use of cloned mobile telephones/SIM cards to mask criminal activities; 2) Stealing and reprogramming/tumbling mobile telephones for resale; 3) Premium rate service fraud; 4) Using mobile phones as a tool for detonating bombs; 5) The use of pay-as-you-go mobile telephones to mask criminal activity; 6) Cloning mobile telephones/SIM cards as a means of gaining free telephone; 7) Stealing mobile telephones to export to countries; 8) Missing trader or carousel fraud (involving mobile phones). Also, Nykodym, Ariss, and Kurtz (2008) found four (4) types of cyber-crime; 1) Espionage, 2) Sabotage, 3) Thieves, and 4) Abuse of a company's network.

Dagon, Martin, and Starner (2006) categorized attacks against handheld devices based on securities attackers into several groups such as theft of data, Bluebugging, Bluejacking, BlueSnarfing, phone hijacking, denial-of-service attacks, and battery draining. Bluejacking is "the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth enabled device via the OBEX protocol." (Legg, 2005). BlueSnarfing is a snarf attack which is working against handheld devices by letting attacker's access owner information. Bluebugging is one of Bluetooth attack which allows the attacker to start a phone call, read contact information, send SMS, and access the Internet. In line with the taxonomy of Dagon et al. (2006) and Nykodym et al. (2008), the emphasize needs to be placed on information, service and theft issues.

1) Theft

Smith (1996) introduced six types of mobile telephone theft: 1) theft of telephones, 2) subscription fraud, 3) obtaining network access, 4) counterfeit telephones, 5) roaming fraud, and 6) lifetime phones. In order to gain static and transient information, hackers attack handheld devices. Static information includes phone numbers, stored programs, and contact information which the devices send over the network. The Bluebugging and BlueSnarfing are examples. Attacks on static information such as phone's power usage and its location can occur even when phones are off.

2) Theft-of-service attacks

Some malware can also attempt to steal phone recourses. 900-number calls, sending expensive text messages, and placing long-distance calls. Attacks approach mobile phone users with the form of messaging, advertising, and other unsolicited information. Examples are Bluejacking and Spam text messages (Shin et al., 2008)

3) Denial-of-service attacks

Denial-of-service (DOS) attacks are an attempt to drain battery power and flood the device with unnecessary information. Recently, a Bluetooth application is becoming vulnerable by incoming data such as corrupted packets, repeated pieces of information, and incorrect file formats (Dagon et al., 2006; Shin et al., 2008).

1.1.3 Options on Dealing with Cyber-Crime and Handheld Devices

In dealing with the several types of cyber-crime from handheld devices, diverse strategies can be adopted according to how handheld devices are implemented in different contexts. In this research, general recommendations are included to prevent and to assess threat and attacks. According to Dagon et al. (2006) and Nykodym et al. (2008), identified are 6 aspects of coping with threats to mobile devices: 1) education, 2) visualization, 3) conservative defaults, 4) profiling, 5) hard switching, and 6) heterogeneity.

The above recommendations, along with management and employee training, have been used to address similar attacks via phishing (falsely assuming the identity of an organization to conduct cyber-criminal activities) (Nykodym, Kahle- Piaseck, Ariss & Toussaint 2010).

Consumers along with government agencies and employees of service providers and mobile phone manufacturers should know what kinds of threats may possibly occur against mobile phones. Visualization is about providing logs of important statistics such as battery consumption rate, CPU activity, data transmission, and battery level and enables phone users to investigate the source of attack. One of the conservative defaults regarding network applications is to ship devices turned off and in a non-discoverable mode. Profiling is a typical method for service providers to identify and detect attacks (Nykodym, Taylor, and Vilela, 2005; Nykodym et al. 2008). If suspicious activity is found, they try to contact users to confirm that they are involved. Through the hard switch, users are able to disconnect the power to the phone, so they are sure that the phone is completely off. Diverse platforms and open standards are desirable to protect malware and viruses.

Chen, Chen, Song, and Korba (2004) listed prevention strategies concerning identity theft in the context of online gaming: 1) password set up, 2) biometric authentication such as fingerprint verification, voice recognition, and hand geometry, 3) dynamic password authentication known as one time Password Generator. Besides, they suggested other preventions such as 1) enhance identity authentication mechanism, 2) use insurance, 3) deploy built-in cheating detection mechanism, 4) back up and reserve the complete data, 5) install online scan mechanism to protect viruses and worms, and 6) assemble the related work such as legislation, standards investigation, skills for detection and tracing for use by enforcement authorities.

Guo, Wang, and Zhu (2004) addressed defense methods for smart-phone attack from four aspects which include smart-phone hardening, internet side protection, telecommunication side protection, and cooperation between the Internet and telecommunication networks. Smart-phone hardening is involving hardware hardening, Operating System (OS) hardening, and attack surface reduction. Subscriber Identity Module (SIM) card is one of the features which shows hardware hardening. By simply identifying caller's numbers and lightening up LCD display, OS can enforce security aspects. While calling or texting, other functions in mobile devices can be turned off. Internet side protection is associated with the malware defense mechanism. Increasingly, Internet service providers do not allow un-patched or unshielded devices to access their system. Regardless of the Internet service, telecommunication companies should provide their own functions to react and detect misbehaviors such as data packet drop rate, call blocking, call center load information, and abnormal end use behaviors. Effective coordination between the Internet and telecom networks is required by exchanging known vulnerability and attack information. Also, Ariss, Nykodym, and Cole-Laramore (2002) and Nykodym and Talyor (2004) argued that trusting relationship between manager and employee and effective electronic communication are vital tools to combat cyber-crime in the organizational level.

2. Overview and Conclusion

After Apple introduced the Apple Newton in the mid-1980's, handheld devices have been involved in the business to enable people to access databases, carry out calculation, create documents, and collect information (Jordan, 2004). Along with the growth of information technology and Internet, the use of handheld devices such as Blackberry's and iPhone's has highly increased. Judging from the growing body of researches in handheld devices and cyber-crime, this study offers an overview in dealing with many issues from mobile computers. In this analysis, the researchers will explore the nature of handheld devices, their advantages and disadvantages.

Advantages of handheld devices are ubiquitiousness, convenience, and cost reduction and disadvantages are high setup cost, improper use, short battery life, limited display, and loss compared to desktops. The use of handheld devices entails the sources of cyber-crime such as theft, theft of service attacks, and denial of service attacks. This research identifies prevention and mitigation strategies against possible cyber-crimes based on Chen et al. (2004), Guo et al. (2004), Nykodym et al. (2005), Dagon et al. (2006), Nykodym et al. (2008), and Nykodym et al (2010),: 1)

authentication and profiling to identify and detect threats, 2) contingency portfolios for diversification, and 3) cooperation among participants. The strategy to deal with types of cyber-crime requires involving employees in system provider, users, and government agency. Single entity is not able to handle and mitigate various types of cyber-crime. Effective collaboration and coordination among each entity reduce the threats such as service vulnerability and device loss, and malware viruses (Nykodym and Taylor, 2004).

3. Future Research

This research is conceptually developed concerning handheld devices generally and does not specify any context where handheld devices are adopted and implemented such as manufacturing, healthcare, education, personal use, and so on. To investigate the precise impact of handheld device implementation requires having in-depth interviews with users and service providers or device on manufacturing, healthcare, education, personal use, and other venues. To that end, it is possible for management to identify the characteristics of handheld devices and possible threats more accurately. Case studies can also illustrate how they are implemented and assess and quantify the degree of vulnerability. Another research opportunity resides in the legislation. Due to innovative technology and rapidly updated services, existing legislative framework is not sufficient to serve this change and new format of crimes (Nykodym and Taylor, 2004). Agile response and reflection of proper regulations by enforcement authorities worldwide are required.

References

Ariss, S., & Nykodym N., (2002). Trust and Technology in the Virtual Organization. Advanced Management Journal (03621863), 67(4), 22.

Becta Company (2005). Handheld computers. Technical paper, v2, 1-12.

Beken, T., & Balcaen, A. (2006). Crime Opportunities Provided by Legislation in Market Sectors: Mobile Phones, Waste Disposal, Banking, Pharmaceuticals. European Journal on Criminal Policy and Research, 12(3-4), 299 - 323. http://dx.doi.org/10.1007/s10610-006-9025-0

Chang, Y. F., Chen, C., & Zhou, H. (2009). Smart phone for mobile commerce. Computer Standards & Interfaces, 31(4), 740-747. http://dx.doi.org/10.1016/j.csi.2008.09.016

Chen, Y., Chen, P., Song, R. and Korba, L. (2004). Online Gaming Crime and Security Issue – Cases and Countermeasures from Taiwan, In Proceeding of the second annual conference on Privacy, Security, and Trust, Fredericton, 1-7.

Dagon, D., Martin, T. and Starner, T. (2006). Mobile phones as computing devices: the viruses are coming, IEEE Pervasive Computing, 3(4), 11-15. http://dx.doi.org/10.1109/MPRV.2004.21

Ebell, M., & Rovner, D. (2000). Information in the Palm of your hand. Journal of Family Practice, 49, 243-251.

Farke, S., Sielaff M., Franke C., Goegler H., & Fischer F. (2008). The handheld computer for surgeons helper or handicap. Surgery Journal, 3(2), 34-38.

Feick, K. (2009) Frost and Sullivan - Multiple advantages to boost deployment of wireless and handheld devices in healthcare.[Online] Available: http://www.frost.com/prod/servlet/press-release.pag?docid=171680656

Fong, C. (2008, May 8). Fighting the agents of organized cybercrime. [Online] Available: http://www.cnn.com/2008/TECH/05/08/digitalbiz.cybercrime/index.html

Gartner Says Mobile Phone Sales Will Exceed One Billion in 2009. [Online] Available: http://www.gartner.com/press_releases/asset_132473_11.html.

Guo, C., Wang, H. and Zhu, W. (2004). Smart-phone attacks and defenses, HotNets III, 1-6.

Is4profit. (2004, April). Smartphones: The benefits of smartphones. [Online] Available: http://www.is4profit.com/business-advice/it-telecoms/smartphones/the-benefits-of-smartphones.html

Jordan, T. (2004). Do handheld computers have a viable place in today's classrooms?, http://www.gartner.com/press_releases/asset_132473_11.html.

Lapinsky, S., Weshler, J., Mehta, S., Varkul, M., Hallett, D., & Stewart, T. (2001). Handheld computers in critical care. Critical Care, 5(4), 227-231. http://dx.doi.org/10.1186/cc1028 PMid:11511337 PMCid:37409

Legg, G. (2005). The bluejacking, bluesnarfing, bluebugging blues: bluetooth faces perception of vulnerability. EE Times. [Online] Available: http://www.eetimes.com/design/communications-design/4017819/The-Bluejacking-Bluesnarfing-Bluebugging-Blues-Bluetooth-Faces-Perception-of-Vulnerability

Locsin, A. (2009, July). Advantages and disadvantages of handheld computers. [Online] Available: http://www.ehow.com/facts_5159212_advantages-disadvantages-handheld-computers.html

Mahatanankoon, P., Wen, H. J., & Lim, B. (2005). Consumer-based m-commerce: exploring consumer perception of mobile applications. Computer Standards & Interfaces, 27(4), 347-357. http://dx.doi.org/10.1016/j.csi.2004.10.003

Mandryk, R., Inkpen, K., Bilezikjian, M., Klemmer, S., & Landay, J. (2001). Supporting children's collaboration across handheld computers. CHI, 225-226.

Nykodym, N. Kahle-Piaseck, L., Ariss, S.., Toussaint, T., (2010). Cybercrime and business: How to not get caught by the online Phisherman Journal of International Commercial Law & Technology , Vol. 5, Issue 4, 252-260.

Nykodym, N., & Taylor, R. (2007). Communication: A Vital Tool to Combat Cyber-crime. Journal of International Commercial Law and Technology, 2(3), 185-189

Nykodym, N., & Taylor, R. (2004). The world's current legislative efforts against cyber-crime. Computer Law and Security Report, 20(5), 390-395. http://dx.doi.org/10.1016/S0267-3649(04)00070-6

Nykodym, N., Ariss, S., & Kurtz, K. (2008). Computer addiction and cyber-crime. Journal of Leadership, Accountability and Ethics, 78-85

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber-crime. Computer Law & Security Report, 21(5), 408-414. http://dx.doi.org/10.1016/j.clsr.2005.07.001

PC Magazine (2010 Definition of Smartphone. [Online] Available: http://www.pcmag.cam/encyclopedia_term/0,2542,t=Smartphone&I-51537,00.asp

Shields, J. & Poftak, A. (2002). A report card on handheld computing. Technology & Learning, 22(7), 24- 36.

Shih, D., Lin, B., Chiang, H., & Shih, M. (2008). Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems, 108(4), 478-494. http://dx.doi.org/10.1108/02635570810868344

Siegemund, F., Floerkemeier, C., & Vogt, H. (2005). The value of handhelds in smart environments. Personal and Ubiquitous Computing, 9(2), 69 - 80. http://dx.doi.org/10.1007/s00779-004-0311-x

Smart phone sales to reach 126 m units by 2009, ARC Group, 15 November, 2004.

Smith R. (1996). Preventing mobile telephone crime. Communications Research Forum, Australian Institute of Criminology, 1-13.

University of North Carolina at Chapel Hill. (2003). Advantages and concerns of handheld technologies for school use. [Online] Available: http://www.learnnc.org/lp/pages/693.

Notes

This research comes from The University of Toledo, Ohio USA. This University is the third largest University in the State of Ohio USA, and only one of 17 USA Universities that grants the Doctoral degree in the fields of medicine, law, pharmacy, engineering, business, education, and all the major sciences all on the same campus. Doctoral degrees include the M. D., J. D. and PHD degrees.