Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?

Mark Harris
Integrated Information Technology, University of South Carolina, Columbia, SC, United States., marharris1@augusta.edu

Karen Patten
Integrated Information Technology, University of South Carolina, Columbia, SC, United States., pattenk@sc.edu

Elizabeth Regan
Integrated Information Technology, University of South Carolina, Columbia, SC, United States., earegan@mailbox.sc.edu

Jerry Fjermestad
School of Management, New Jersey Institute of Technology, Neward, NJ, United States., jerry.l.fjermestad@njit.edu

Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?

Mark Harris, Ph.D.
University of South Carolina
maharris@hrsm.sc.edu

Karen Patten, Ph. D.
University of South Carolina
pattenk@hrsm.sc.edu

Elizabeth Regan, Ph.D.
Integrated Information Technology
University of South Carolina
earegan@mailbox.sc.edu

Jerry Fjermestad, Ph.D.
School of Management
New Jersey Institute of Technology
jermestad@adm.njit.edu

ABSTRACT

Business mobility is rapidly becoming an everyday way of doing business. Mobile technologies, such as smartphones and connected devices, are enabling this business evolution. However, they are also creating new security concerns for the enterprise and its employees. Security experts are studying these increased security concerns to develop more secure practices and policies for the next generation mobile technologies. This paper describes these new mobile security concerns and discusses preliminary expert recommendations to reduce an increasing business risk. Although large enterprises have the resources to implement emerging security recommendations, small and medium enterprises (SMEs) may not be able to adopt the new recommendations because they lack IT resources and capabilities. This paper describes the SME dilemma: Embrace the mobility business strategy and adopt and invest in the necessary security technology, or give up their mobility business strategy to protect enterprise and customer data and information. Finally, the paper identifies future research questions concerning SME security awareness and capability to minimize security threats to develop more viable security practices.

Keywords

Small business, medium business, SME, mobile business, connected devices, smartphones, security considerations, 4G wireless

INTRODUCTION

In today's changing business world, mobile capabilities are being integrated into an enterprise's everyday business environment. In a 2006 White Paper, Nokia defined 'business mobility' as giving employees the "*freedom to collaborate and transact business outside traditional workplaces and times. It is communications on the go, with access to the right information at the right time,"* (Nokia, 2006, p. 2). Employees spend less time at their desks and more time interacting with customers and vendors. Customers also expect immediate responses to any requests, which require improved customer support services. As enterprises integrate business mobility into their business strategy to leverage flexibility and productivity advantages, they soon realize that the business requires new policies for addressing people, processes, and technology implications from the mobile way of doing business. If not addressed, enterprises may find themselves overwhelmed with a mish-mash of various employee-owned mobile devices (referred to as bring your own devices, BYOD) and services. In this case, the enterprise employees also probably lack systematic access to enterprise information, which impedes their ability to collaborate with each other because of incompatible services and technologies.

The technology on which mobile phones and connected devices are based is changing rapidly as well. Mobile phones include smartphones and featured phones, where smartphones typically have faster processors, higher resolution touch screens, and better compatibility with third party software applications. Connected devices include tablets, personal digital devices (PDAs), gaming consoles, and e-readers. Since desktop computers and mobile laptops have been used in businesses for quite some time, information systems security specialists are more familiar with these technologies such as the most-widely used Microsoft Windows operating systems. However, with the new popularity of smartphones and tablets, security experts and users have new concerns. These devices do not use the common Windows operating systems. Instead they use operating systems like Apple's iOS and Google's Android OS, which are much newer and less familiar. They also use different software applications than found on typical computers. This software is most often purchased through online stores

controlled by the operating system's parent (i.e., Apple and Google). These new security concerns raise issues about the security and safety of enterprise data and information as well as an employee's own personal information. By providing employees with better mobile technology tools to increase productivity and improve competitiveness, SME managers often allow any mobile technology that helps their employees get the job done. This practice comes with a price – the threat of increased security problems.

This paper first defines the SME and its importance to the economy. It explores the growth and the need to provide increased security for new mobile phones and connected devices as an integral part of a business mobility strategy. The paper describes the new security risks and preliminary recommendations, which a sophisticated large enterprise IT organization should implement. However, these preliminary recommendations may not be doable by the SME, that has little or no enterprise IT organization or expertise. This paper describes the SME dilemma: whether to implement the new security recommendations for smartphones and continue the SME mobility advantages or to risk serious security threats to the business from the new technologies. Finally, the paper identifies future research questions concerning SME security awareness, the capability to minimize security threats, and the potential of more viable security solutions for SMEs.

SMALL AND MEDIUM ENTERPRISES (SME)

Small and medium enterprises (SMEs) are very important to the economies of most countries. The United States Small Business Administration, Office of Advocacy, defines a small business as an independent business having fewer than 500 employees. According to the latest United States labor statistics based on enterprise size, 99.6 percent of all enterprises had fewer than 500 employees making up 55.8 percent of the total employment (USDL, 2005). Fifty-four point four percent of all enterprises had one to four employees, accounting for only 5.2 percent of total employment. On the other hand, only 0.2 percent of enterprises had 1000 or more employees, but made-up 37.4 percent of total employment (United States Department of Labor, 2005). The SME definition differs for Europe. The 2003 European Commission for enterprise and industry defined a medium business as having less than 250 employees, a small business as having less than fifty employees, and a micro business as having less than ten employees (Commission of European Communities, 2003). In Europe, SMEs comprise 99.8 percent of all enterprises.

With mobility changing the ways people work, enterprises are becoming more aware that they require some type of mobility security strategy, but many have not developed one for a number of reasons (Waltz, 2011). New generations of smart phones and connected devices are being introduced rapidly, leading to increasing diversity of mobile devices in the work place. Unlike the case with many other technologies, employees are driving the mobility strategy, not the enterprise IT organization. For example, employees often bring their own devices (BYOD) for both work and personal uses. Finally, the easy access to numerous mobile applications (apps) complicates the ability to develop security management policies.

THE GROWTH OF BUSINESS MOBILITY PHONES AND DEVICES

The Nielsen Company (2011) reported that, as of mid-2011, sixty percent of all cellular phones in the United States were smartphones. Thirty-nine percent of those smartphones utilized Google's Android operating system (OS), 28 percent used the Apple iPhone OS, 19 percent used the RIM Blackberry OS, and nine percent used the Windows Mobile or WP7 OS. The top tablet operating system on the market continues to be Apple iOS, as found on the iPad, which accounts for 58 percent of the tablet market as of the fourth quarter of 2011 (Strategy Analytics, 2011). However, that is a decrease of ten percent from a year earlier. Strategy Analytics reports the Android OS from Google gained that ten percent by moving to 39 percent from 29 percent a year earlier. As a category, global tablet shipments hit 66.9 million units in 2011, surging 260 percent from 18.6 million in 2010 (Strategy Analytics, 2011).

THE SECURITY CONCERNS

Information systems security specialists are more familiar with personal computers and laptop technology using Microsoft Windows operating systems. Statcounter Global Stats (2012) reports that as of January 2012, Microsoft Windows 7, Windows XP, and Windows Vista represent the operating systems used by 89.3 percent of the computers connected to over three million Web sites monitored by the company. The Mac operating system and Apple's iOS account for 9.04 percent (Statcounter, 2012). Besides security experts being more familiar with Microsoft's operating systems, so are end users. Many end users are familiar with the need to perform windows updates and install antivirus and firewall software. The popularity of smartphones and tablets and the use of the newer and less familiar Apple's iOS and Google's Android OS are leading to new security concerns. As a result, smartphones and tablets, with their new operating systems, pose new threats to

information technology specialists and end users. The next few sections discuss these new security concerns with Android and Apple iOS mobile and connected devices with a focus on various implications for small, medium, and large enterprises.

WiFi

Connectivity to corporate networks and the Internet typically occur either through a mobile broadband network (3G/4G) or a WiFi network. As of mid-2011, 37.2 percent of U.S. digital mobile traffic and nearly ninety percent of tablet traffic occurred via a WiFi connection (Comscore, 2011). This implies that, as with laptop connectivity to corporate networks and the Internet, smartphone and tablet users also need to be aware of Wi-Fi security protocols and risks associated with using WiFi.

WiFi encryption passwords or passphrases, such as Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA and WPA2) have been used for years to protect communication between the device and the access point. WEP was developed first, but contained many flaws and became easily cracked as long ago as 2004. Cracking WEP now takes only seconds (Gold, 2011a). WPA was developed to fix the vulnerabilities of WEP and is also now easily cracked (Bradbury, 2011). WPA was then improved upon with the release of WPA2, the current WiFi encryption standard.

Since the release of WPA2, most security experts were comfortable with its protection and many believed it was uncrackable (Gold, 2011a). However, that all changed in September 2010, when Elcomsoft's Wireless Security Auditor (WSA) was released, which could crack WPA2 passphrases. The company's WSA software has the ability to brute force crack as many as 103,000 WPA2 passwords per second. The WSA software can also crack WPA.

Since the WPA2 Wi-Fi encryption technology is not as safe or uncrackable as once believed, experts recommend companies do not use Wi-Fi if they have a hard-wired alternative (Gold, 2011a). For those companies that must use Wi-Fi, Peter Wood, a member of the Information Systems Audit and Control Association (ISACA) security advisory group, advises the use of 20+ character WPA2 passphrases with upper and lower case characters along with a Radius-based virtual private network (VPN) system (Gold, 2011a). This first part of this solution, the use of 20+ character WPA2 passphrases, is practical for all enterprises and end users. WPA2 passphrases can easily contain 20+ characters and be more easily remembered if a phrase is used, such as this 40 character "*ComeToOurDentalPracticeForTheBestService*" passphrase. A passphrase of this length is much harder to crack with brute force cracking software and very difficult to guess. The second part of the proposed solution may be more practical for a large enterprise than it is for smaller companies with limited or no enterprise information technology staff. Installing and administering a Radius VPN system is not something most small to medium enterprises can accomplish without an information technology professional.

Another major problem with WiFi is the vulnerability to rogue access points, known as evil twins. Evil twins are access points with the same ESSID (Extended Service Set ID) as a legitimate access point. Wrong doers can easily obtain the software needed to turn a simple laptop into an evil twin that tricks unsuspecting user's devices. Most Wi-Fi devices automatically connect to known networks already configured in the device. The evil twin access point can copy the MAC (Media Access Control), ESSID, and other identifying information to spoof the legitimate access point's packets and essentially become a clone. Wi-Fi encryption, such as WPA2, does not help because WPA2 encrypts data after the association is established and cannot protect against management packet spoofing, MAC address spoofing, ESSID spoofing, and others (Phifer, 2011). Plus, WPA2 can now be cracked with brute forces attacks, greatly diminishing its effectiveness (Gold, 2011a).

The solution to the evil twin problem that most large enterprise organizations take is to utilize a Radius server with VPN, which authenticates users against a database instead of using a pre-shared key. With typical Radius server authentication, an encrypted tunnel is created to send the username and password, which protects the credentials from wrong doers. Again, using a Radius server is something large organizations can do more easily than small to medium organizations. However, even Radius server authentication is vulnerable to evil twin attacks if the end user fails to properly identify the proper radius server (Nussel, 2010).

To further protect mobile devices, tablets, and laptops, personal virtual private network (VPN) software can be purchased and installed in individual devices. A personal VPN creates an encrypted tunnel over unsecure networks, thus protecting the data within the tunnel. Larger organizations often host their own VPN servers that employees connect to from anywhere there is an Internet connection. But for smaller organizations without VPN Servers, personal VPN software vendors host the VPN servers. Therefore, employees can better protect their Wi-Fi connections from WPA2 cracking and evil twin access points, both in the office and out while traveling. There are many vendors of personal VPNs and the software is available for all of the popular operating systems, including smartphones and tablets. Personal VPNs also have different security levels, where an iPSec VPN is considered the most secure and is also the most expensive.

Another reason to use VPNs, whether corporate or personal, is that cellular networks are not completely safe either. In 2010, Vodafone's cellular network in Europe was hacked through a device known as a femtocell (Gold, 2011b). A femtocell is a miniature cellular base designed for localized use by homes and small businesses. The hacking used a method similar to the evil twin concept on Wi-Fi to access victim's cell phones voice and data transmissions. Other companies, such as AT&T, Sprint, and Verizon, have since launched their own femtocells. While Vodafone claims their vulnerability has been patched, the incident further strengthens the argument to use VPNs over cellular and Wi-Fi networks.

Android OS

The Android operating system is quickly becoming the most popular operating system on mobile devices in the United States, running in stride with Apple's iOS as the two major players. However, when it comes to security, Android falls far behind. McAfee (2011) reported that the Android OS is by far the biggest target of mobile malware writers. In the fourth quarter of 2011 alone, over 400 malware programs were detected, up from just over 100 in the third quarter (McAfee, 2011). One of the reasons Android is susceptible to malware is that it does not close applications when the user is done with them (Gold, 2011c). Instead, it allows processes to run until resources are needed and then closes processes with the least priority. Malware writers take advantage of this by writing malware that runs in the background, where it is undetected by users. Then the malware writers give the malware the highest priority. This helps ensure the malware will remain undetected and will not be the first to be closed by the OS due to priority (Gold, 2011c). According to Nigel Stanley at Bloor Research, the Android has other security flaws by not protecting memory cards, allowing data to flow over communications channels in clear text, allowing text message bombs to run the background undetected, and not allowing users or software to verify senders of email (Gold, 2011c). Overall, Stanley considers Android to be a complete failure on the security front (Gold, 2011c).

Apple iOS

Apple's iOS security model is much safer than Androids' model. Apple runs each third party application in its own isolated environment and only allows access to the application's own data and permitted system resources (Lookout, 2011). With the exception of only a few applications, all third party applications are granted the same data access and capabilities (Lookout, 2011). This makes iOS a much safer operating system than Android's OS.

Mobile and Tablet Software

Apple attempts to limit users downloading from only official channels, where Android makes no such attempt. For example, Android allows users to download from various sources, including the Android Market, Amazon's Appstore for Android, carrier markets like Verizon V-CAST, and alternative app markets (Lookout, 2011). From a stronger security point of view, download sites like Amazon's Appstore for Android and Verizon's V-CAST use a curated model, similar to Apple's model (Lookout, 2011). The curated model consists of a manual review process before software is available to download, but this approach takes longer to bring software to market. The alternative to a curated model is the Google Android Market's community enforced model, where some security checks are performed, but the Android community is expected to participate in determining malicious or undesirable applications (Lookout, 2011).

Unlike Google's Android OS, Apple's devices require users to download software from the Apple Store. Applications there follow the curated model, where there is a manual review process with restrictions based on data collection, API (Application Programming Interface) usage, content appropriateness, and user interface guideline compliance (Lookout, 2011). This curated model is safer than Android's model because of the review process and limited options for obtaining the software. However, jailbroken devices are capable of obtaining software from other sources. Jailbreaking alters the operating system to allow full access to the OS and bypass Apple's software restrictions.

Just because an application came from the vendor's store, even a store with a curated model, does not mean the application is completely safe. While there have been more instances of malware applications on Android markets than on the Apple market, both are susceptible to malware.

When vulnerabilities are discovered with the Android OS, Google quickly produces a patch and uploads it to the Android Open Source Project (AOSP), where device manufactures then download the patch, modify it to work with specific phone models, and, specifically, customize it for the various carriers of those models (Lookout, 2011). Because there are many models and multiple carriers involved, it takes longer to get Android patches to the end user. With Apple iOS, Apple creates the patch and an operator tests it. The patch is then uploaded to iTunes where end users can sync their devices to receive the update. This process has fewer parties involved and is quicker, however, many users do not regularly sync their devices, thus they do not receive critical updates in a timely manner (Lookout, 2011).

THE UNIQUE SME SECURITY CONCERNS

Security concerns create a new dilemma for innovative SMEs that over the last five to eight years have become early adopters of mobile technologies. It has commonly been assumed that small and medium enterprises are slow to adopt new technologies for a number of reasons. The NFIB Research Foundation reported in a 2005 National Small Business Poll that a very small number of small businesses were bleeding or leading edge adopters of emerging technologies (Dennis, 2005). However, the introduction of mobile technologies began an evolution where innovative small businesses had the opportunity to adopt these emerging technologies to create a more equal competitive stage with the largest enterprises. Advantages for innovative SMEs revolve around four aspects (Patten and Passerini, 2007):

- Structure – SMEs are not constrained by inflexible and legacy IT infrastructures technology, which makes it easier to adopt newer technologies.
- Size – Organizational size and flexibility have less implementation issues with few employees with specific roles.
- Processes – Although often informal, SME processes are usually fluid and easily adaptable to new situations.
- Workplace – Dynamic workplaces and workforces require the latest mobility capabilities and tools to give their employees the capability to work from anywhere, anytime.

The rapid introduction of smartphones and tablets are again changing the way small businesses compete. For example, these new services help SME employees increase their individual productivity, lower cost of services make them affordable for the small business, and wireless services providers are beginning to provide more IT support to even the smallest businesses.

However, SME's just like larger enterprises need to effectively manage business relationships and part of this is to provide security (Romano and Fjermestad, 2007). Security breaches and threats can cost the enterprises millions of dollars each year (Gordon, et al., 2004) and more importantly can result in lost customers and decreased customer trust (Ponenon, 2005). SME's cannot afford to either lose customers or decrease customer trust. The SME's need to protect customer information such as customer names, SSN, credit card numbers and then to a lesser extent telephone/cell numbers, mailing addresses and email addresses just as the large enterprises do (Romano and Fjermestad, 2007).

But, smartphones and tablets, with their new operating systems, pose new threats to the security and safety of enterprise information as well as customer information, especially for SMEs who lack the finances and security infrastructure that larger enterprises may have. A smaller company, such as a doctor's office, may use smartphones, tablets, and laptop devices, but often these offices lack information technology specialists to properly secure the devices.

As discussed in the previous sections, some of best solutions for the new security concerns require new SME enterprise policies such as the use of 20+ character WPA2 passphrases with upper and lower case characters, which is doable. However, most of the solutions involve technology or practices. These solutions are difficult or expensive for small and medium enterprises. The best security solution for small organizations without an information technology security staff is to not allow any WiFi access and require that all mobility devices physically connect to the network and on all wireless capability devices have WiFi disabled.

One way to protect devices from malware is to install security software, such as antivirus and firewall software. For those with Android devices, security software from various vendors is readily available. For those with Apple iOS devices, security software is very limited. This is because software can only be obtained from the Apple Market and Apple prides itself with how applications are isolated from the operating system. Because applications run in their own isolated environment and cannot communicate with other applications, security threats are minimized (ePlanet, 2011).

From a corporate and end user point of view, applications designed for the Apple iOS are safer than Android applications. Even though the Android OS is targeted more frequently by malware writers, both are vulnerable to malware. When vulnerabilities are detected, Apple is faster at getting patches to the end user devices. This assumes that end users regularly sync their devices with iTunes. On the other hand, Android devices are slower at getting updates, but updates are pushed to devices via the network without having to manually sync.

Security Recommendations for SMEs

The following recommendations apply for all enterprises, but are considered doable for SMEs:

- Use 20+ character passphrases with WPA2, if WiFi connections are necessary. Now that WPA2 is vulnerable, it is a good idea to limit WiFi use.

- Install antivirus software on all mobile and connected devices. The Android OS has more options, but is also more vulnerable.
- Password-protect all mobile and connected devices. Requiring a password will make it harder for wrong doers to access the device.
- Have the capability to erase data on lost or stolen devices. Many of the antivirus software programs also contain features to remotely erase data and accounts on lost or stolen devices. Some even contain GPS tracking software to help find the device.
- Purchase iOS products over Android devices. Because of the way iOS handles software applications, the operating system is safer than the Android OS. Apple has also added a few high security features to entice business users.
- Sync Apple products with iTunes on a regular basis. When an iOS vulnerability is discovered and patched, the update does not get to the device without a sync with iTunes. Failing to sync often may delay security updates (Lookout, 2011).
- Turn-off discoverable Bluetooth (Loo, 2009). When Bluetooth is set to discoverable, it leaves a door for hackers to exploit. Bluetooth versions older than 2.1 are easily hacked, allowing access to the phones data.
- Update the devices operating system and software frequently. Updating the devices can fix known vulnerabilities, such as Bluetooth 2.1 fixed the vulnerability of version 2.0.
- Avoid storing usernames and passwords on the device or in the browser. If a device is compromised and accessible, stored usernames and passwords will make it easy for wrong doers to access data and accounts.
- Educate employees. All employees should be educated about the vulnerabilities of these devices and the best practices for protection. Education is essential for maximum security.

The above list of recommendations is important for SMEs. Other recommendations are more practical for larger enterprise with IT staff. Enterprises should install Radius servers with iPSec VPNs, which maximize security. All smartphones, tablets, and laptops should be connected to corporate iPSec VPN servers. These enterprises should also utilize deep packet sniffing on all packets on the VPN (EcommerceTimes, 2010). While stateful packet inspection might be enough for most connections, remote VPN connections should utilize deep packet inspection. Another important security aspect is data control. If users do not log into the network within a certain amount of time, the devices will delete its own data or block access to corporate email (SYBASE, 2011). Finally, large enterprises should use two-factor authentication for laptop and tablet remote access (Kemshall, 2011). The process sends a passcode via mobile short message service (SMS) to the users' cellular phone. The required combination of passcode and regular log on credentials to access corporate networks remotely will increase security. Passcodes are one time codes that expire, while regular log-on credentials are reusable and only changed periodically.

To summarize, SMEs with no IT staff should not allow WiFi access and they should require that all mobile devices be physically connected to the network and that WiFi access be disabled.

THE SME MOBILITY STRATEGY DILEMMA

The biggest security difference between large enterprise security and SME security is that the smaller firms with limited IT staff may not be able to implement VPNs with Radius servers, perform deep packet sniffing, and control the data. The partial solution, though not optimal, is for SMEs to utilize personal VPNs. The security of personal VPNs will not be as strong, but using them with the other recommended security solutions for all enterprise will increase security somewhat. But, this is not a complete solution that protects the SME's critical enterprise data as well as the risk to the health of the SME business if customer data is compromised. This leads to the SME dilemma: Embrace the mobility business strategy and adopt and invest in the necessary security technology, or give up their mobility business strategy to protect enterprise and customer data and information.

FUTURE RESEARCH

The SME mobility strategy crossroad described above is serious. We do not know the potential implications. However, these new technologies and the new security concerns create an opportunity for future research in several areas. How aware are SMEs to the new threats? What are the costs and implications for SMEs to adapt to and invest in the new security technologies? What other security solutions might be more effective at less cost? What IT capabilities must SMEs acquire to stay in the mobility business? Plus, many more questions.

REFERENCES

1. Bradbury, D. (2011) Hacking WiFi the easy way, *Network Security*, February.
2. Comscore (2011). Accessed 2/15/2012 from http://www.comscore.com/Press_Events/Press_Releases/2011/10/Smartphones_and_Tablets_Drive_Nearly_7_Percent_of_Total_U.S._Digital_Traffic .
3. Commission of European Communities (2003) Commission recommendation concerning the definition of micro, small and medium-sized enterprise adopted by the commission, *Official Journal of the European Union*, 2003/361/EC.
4. Dennis, W. J. Jr. (2005) The state of technology, *NFIB National Small Business Poll*, 5, 5. ISSN: 1534-8326.
5. ePlanet (2011) Top 10 fun facts about iPad security. Accessed 02/22/2012 from http://www.esecurityplanet.com/trends/article.php/3936411/Top-10-Fun-Facts-About-iPad-Security.htm .
6. Gold, S. (2011a) Cracking wireless networks, *Network Security*, November.
7. Gold, S. (2011b) Cracking cellular networks via femtocells, *Network Security,* September.
8. Gold, S. (2011c) Android insecurity, *Network Security*, October.
9. Gordon, L.A., Loeh M.P., Lucyshyn W., and Richardson, R. (2004) Ninth annual CSI/FBI computer crime and security survey, *Computer Security Institute*. Retrieved from http://www.theiia.org/iia/download.
10. Kemshall, A. (2011) Security should not cost the world, *ChannelWeb.Co.UK*, December 22. Retrieved 02/22/12 from http://www.channelweb.co.uk/crn-uk/opinion/2134340/security-cost-earth .
11. Loo, A. (2009) Security threats of smart phones and Bluetooth, *Communications of the ACM*, 52, 3, 150-152.
12. Lookout (2011) Lookout mobile security, *Lookout Mobile Treat Report*. Accessed 02/22/2012 from https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf .
13. McAfee (2011) McAfee threats report: fourth quarter 2011. Accessed 02/22/2012 from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2011.pdf .
14. Nokia White Paper (2006) A holistic approach to business mobility, *Wiley Publishing*. Accessed 03/01/2012 from http://dailywireless.tradepub.com/free-offer/a-holistic-approach-to-business-mobility/w_aaaa993?sr=ct&_t=ct:Tele .
15. Nielsen (2011) Mobile and smartphone trends. Accessed 02/15/2012 from http://www.nielsen.com/us/en/insights/top10s/mobile.html .
16. Nussel, L. (2010) The evil twin problem with WPA2-enterprise. Accessed 02/15/2012 from http://www.suse.de/~lnussel/The_Evil_Twin_problem_with_WPA2-Enterprise_v1.1.pdf .
17. Passerini, K., and Patten, K. (2006) Small and medium enterprises in the wireless revolution: Directions and areas for future research, *Proceedings of the United States Association of Small Business and Entrepreneurs (USASBE) Conference*, Tucson AZ, January 11-14.
18. Patten, K., and Passerini, K. (2007) Next generation small and medium enterprises mobility strategy roadmap, *Proceedings of ISOneWorldConference*, Las Vegas NV, April 11-13.
19. Phifer, L. (2011) Anatomy of a wireless "evil twin" attack (Part 1). *WatchGuard Technologies.* Accessed 02/21/2012 from http://www.watchguard.com/infocenter/editorial/27061.asp .
20. Ponemon, L. (2005) Lost customer information: What does a data breach cost companies? Ponemon Institute, Tucson AZ, from http://www.securitymanagement.com/library/Ponemon_DataStudy0106.pdf .
21. Romano, N.C. and Fjermestad, J. (2007) Privacy and security in the age of electronic customer relationship management, *International Journal of Information Security and Privacy*, 1, 1, 85-106.
22. Statcounter (2012) *Statcounter Global Stats*. Accessed 02/19/2012 from http://gs.statcounter.com .
23. Strategy Analytics (2011) Accessed 02/19/2012 from http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5167 .
24. United States Department of Labor (2005) New quarterly data from BLS on business employment dynamic by size of firm, *United States Department of Labor, Bureau of Labor Statistics*, USDL 05-2277, December 8.
25. Waltz, M. (2011) Mobility threats, *Mobile Enterprise*, March 7.