To Use or Not to Use Mobile Devices

Blaž Markelj, Igor Bernik
University of Maribor, Slovenia

Abstract

Each day more people use mobile devices and public networks to connect to the Internet and access data in corporate information systems. Cloud computing has simplified many business operations and also helped decrease operational costs, because this new technology has created virtual working spaces and eliminated the need for on-site information systems. Software for mobile devices has advanced greatly, but so has malicious code. Statistical data shows that both the number of mobile phone users and incidences of malware infections are on the rise. Users are often unaware of the threats in cyberspace and carelessly download free software, and so they become the weakest links in information security. Many software developers haven't yet standardized and certify all their products, therefore, users must deal with information security issues on their own. New protective measures are constantly under development, but new changes and adaptations will always be needed. Corporations and other organizations will have to implement efficient safety policies and continuously educate employees how to avoid the potential risks of cyberspace.

1. Introduction

Nowadays we are compelled to make decisions and to act hastily therefore easy and uninterrupted access to data and information is a necessity. This can easily be achieved with the aide of modern mobile devices (mobile telephones, notebooks, etc.), wireless connections, centralized corporate information environments, and cloud computing. Blended threats are most harmful when connections, established through public networks, are used for communication between mobile devices and the cloud, and to access data in the cloud. Making use of cloud computing and the Internet decreases the cost of building and maintaining one's own information infrastructure, and also doesn't require special computer knowledge. Cloud technology mostly runs automatically, so corporations and other organizations don't need to employ computer scientists. These are reasons, why the number of subjects opting for cloud computing is on the rise. Company TechNavio published a report on their home page in regard to the current number of cloud users, and predicted that their number will rise by 42 % in the coming years [1]. When organizations transfer data to the cloud, they don't need to employ as many computer scientists as previously. This impacts the transfer of knowledge from computer specialists to other employees, and significantly lowers awareness of information security issues. Advanced technology, public access to the Internet, and faster connections enable us to use mobile devices to browse current news, email, transfer money and utilize other possibilities. Knowing how to efficiently and securely use all that modern technology has to offer, can be an advantage in the race for success in business and science. Information technology can be a useful tool only if we know how to use it correctly, and, if we succeed in protecting our data. If the potential for information breaches and theft of corporate or private data is minimal or completely eliminated, then it is possible to maintain credibility in the eyes of customers and business partners.

Almost any modern mobile telephone can be used to browse the Internet, manage email and work in a virtual environment. Many employers leave open their "virtual doors", so that work is more flexible and expedient, but this exposes the corporation's information system to a blend of threats, if it hasn't been appropriately protected. The corporation risks losing data or having data stolen and misused; there is also the danger of picking up computer viruses or spyware. Certain software automatically transfers data from a corporate information system or cloud to a mobile telephone as soon as a user types in his username and password. Another question is: Is it truly possible to access data in the cloud at any time? What about the issues of data security and privacy policies? Can we trust software set by default which runs automatically, without the user's knowledge? What is a program running in the background actually doing? What becomes of credentials and the access to data, if the telephone is stolen? The telephone, after all, is storage for a variety of important data, including data to access the domain and server system [2].

When we started using wireless mobile communication devices, we disposed of the "border" between internal systems and the outer world. Today the world is thoroughly covered by a communications web: anyone can communicate with whomever or read, collect, upload, and transfer data. Easy access to data simplifies life and work, but is a big risk in terms of information security. Developers

of security software are seeking optimal methods for analyzing and monitoring contents flowing through communication channels. It can be expected that in the future technology will be able to analyze Internet traffic and complete information systems, based on detection of deviations in routine processes. As for the moment, there are no simple, transparent solutions (at least not from the user's point of view) for protecting information systems from cyber criminals. Risk can be minimized by applying software to monitor Internet traffic [3], and by installing hardware which regularly checks for potential dangers [4]. Some companies that are developing security software are already providing advanced software for mobile devices [5] including firewalls which monitor Internet traffic on mobile devices and in corporate information systems [6]. Certain software enables corporations to define their own internal safety guidelines for the use of mobile devices [7]. Employees usually protect their access to wireless networks with passwords [8]. Some corporations have defined their own rules for maintaining information security in the process of acquiring the ISO 27001 certificate [9], [10].

2. Safe Usage of Mobile Devices and Software

The rapid development and expansion of big information systems, specifically cloud computing, is followed by advancements in the technology of mobile devices, and software for them [11]. Recently the number of people using mobile telephones and tablet personal computers has risen significantly [12], [13]. According to the 2010 report published by IDC global sales of mobile telephones have gone up by 17 % in the last quarter of 2010 (compared to sales in the last quarter of 2009). In 2011 sales have gone up by 55 % in comparison to the previous year. Based on the IDC report, it is safe to expect that sales of mobile telephones will increase by 200 % by 2015 [14]. Mobile devices with sophisticated software are quite functional – they can be used to access the cloud – and have begun to replace personal computers. Anyone with a mobile device can connect to the Internet whenever needed and read email, search the Internet or work with business data, etc.

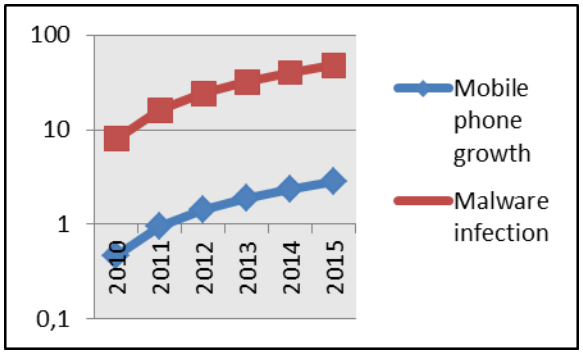

Figure 1. A comparison of the growth in mobile phone sales and the number of malware infections (logarithm ordinate axis).

Figure 1 shows the rising trend in the number of malware attacks in relation to the number of mobile telephone sold – based on research carried out by IDC [14] and Juniper [15]. On the basis of this data, it is possible to get an ideal of how fast the numbers of both smart phones and malware are growing. The figure of two trends shows that the increase in both instances is comparable. This is the result of two factors, (1) the protection of operating systems for mobile devices is continually getting better, and (2) the "quality" of malware is also continually improving. To sum up: more sophisticated protective measures lead to more sophisticated and subtle attempts to penetrate this protection.

While the evolution of information technology has been rapid and efficient, not much has been gained in regard to information security. As long as the user stays within the protected environment of a corporate system, information security is attainable. The security of a corporate information system is maintained on the basis of standardized guidelines for procedures, which have been defined in the past fifty years. The danger is greatest, when someone utilizing public networks and simple (insecure) protocols or software is accessing the virtual environment of an organization. Users should be aware that whenever such a connection is established, a "door" in the protective "wall" of an information system is opened. This "opening" puts the information system to great risk. From the user's standpoint, there is no difference between connecting to a corporate information system or the cloud. It should be noted only, that connections to public or hybrid clouds are riskier.

When a mobile telephone is used to access data in the cloud, software on the device can function only as a user application, which displays data – data analysis is carried out by cloud software. Computer scientists have noted that while software is being developed at a fast pace, little is done to standardize and certify it. Evidently the problems lies with software providers, but users should, after all, be aware of information security issues and act

accordingly. Often this is not the case therefore certain software on mobile devices runs unnoticed. Corporations and other organizations choose to transfer their data bases to a cloud to minimize the cost of maintaining an information system. A lease to a cloud provides space, services, software, redundancy and unlimited access to data, all at a much lower cost. The downside is the information security issue. The Gartner company has published several analytical reports informing the public about both the advantages and disadvantages of cloud computing. One of seven pitfalls described is the question, how the right to access data in the cloud is regulated. As soon as an organization transfers its data to the cloud, it is uncertain who else can access and possible manipulate their data. Cloud providers promise data security and privacy, but a leaseholder to a cloud (or part of one) can't know for sure, where the data is and who else can get hold of it. It is quite possible that data in the cloud can be accessed by unauthorized persons, i.e. competitors or secret service agents. When data is stored in the cloud, much depends on the reliability and capability of the proprietors Internet connection. A good connection is an inevitable requirement for anyone intending to utilize a public or hybrid cloud. The next question to consider is the quality of data redundancy in the cloud. Also: Does the cloud truly function without interruption? Interruptions affect accessibility. We should also consider legal and proprietary issues in regard to the contents of the cloud. Redundancy should be guaranteed so that, should a corporation change owners, nothing happens to its data [16]. When a mobile device is integrated into a network, it usually isn't known what else happens. A good example of the risk involved is free software on the Internet, which facilitates on-line payments or data transfers. Such software may contain potentially harmful code so consequently our data or money can be stolen [17]. A mobile device can also be targeted by software fragments which breach the device by way of malware, spyware, botnets, or when a bluetooth connection is established, or through participation in social networks [17]. Results of research carried out by Lookout [18] show that the volume threatening malware applications has increased significantly in the past six months – by 14 % in comparison to threats from spyware. There is a possibility that 1 to 4 % of mobile devices are "infected" because users download free software [18]. The Juniper company reported that there has been a 400 % increase in the number of mobile devices (running on the Android platform) infected by malware. This report [15] also states that 85 % of users have inefficient protection on their telephones. Providers of software for mobile devices usually install "back doors", programs which manage settings and other software on the device without the knowledge of the owner. Such programs automatically send GPS data to locate the user and/or device, and can even take control of the device [19]. Flores [20] noted that the results of research recently carried out in different parts of the globe clearly show that anyone collecting and analyzing data automatically acquired from mobile devices can make assumptions about a user's lifestyle (health, political preferences, consumer habits, etc.). Known are incidences, when data was secretly collected with the help of the GPS module in mobile devices and stored in larger information databases. Such software can also monitor the frequency and methods of communication, which again uncovers a user's habits. Kučič [21] commented on the matter of deleting personal data – when a user stops using certain software, an Internet browser or his mobile device, he assumes that he will be able to delete all personal data and that later no one else will be able to retain it. By using unauthorized, non-standard software we can inadvertently open the "door" to the information system or cloud and greatly increase the risk that data will be stolen or misused. This endangers the integrity and business of the whole organization [22].

The contents, which is being transferred between server and client applications, is not protected well enough and is relatively accessible to anyone determined to get to it. Perpetrators nowadays don't necessarily have to be computer scientists to achieve their goal. The user of a mobile device is the weak link in information security so employers should make sure that their employees receive enough information about safety standards. Good internal regulations must contain details about correct procedures, lists of permitted software, Internet protocols. Employees must be informed about the consequences of harmful activities or incorrect usage of a mobile device [23], [3].

3. The Dangers of Mobile Devices Integrated into Central Information Systems

Cyber criminals target mobile devices with a combination of threats, all with the goal to unlawfully acquire restricted information and profit from this. Dangerous software combines with threats which arise when data is transferred from a corporate information system or cloud. Blended threats are a combination of separate threats which most often act simultaneously, but at different levels [24]. Users are exposed to blended threats as soon as they establish the connection: mobile device – Internet – information system. Threats can be direct or indirect. The most direct threat is, if a mobile device is lost or stolen. If crucial information and documents are saved on the device, and its owner hasn't applied even the most basic protection (PIN code), then the

owner alone is responsible for any consequences. More sophisticated and indirect threats are interceptions of communication and secretly implanted software which automatically harvests information. Indirect threats are usually more severe, because they are unpredictable, and total protection from them is impossible.

4. Data Exchanges between Mobile Devices and Central Information Systems

It used to suffice that the central information system was protected by a firewall which monitored incoming communication. Figure 2 shows how communication used to be exchanged between Intranets and the Internet.

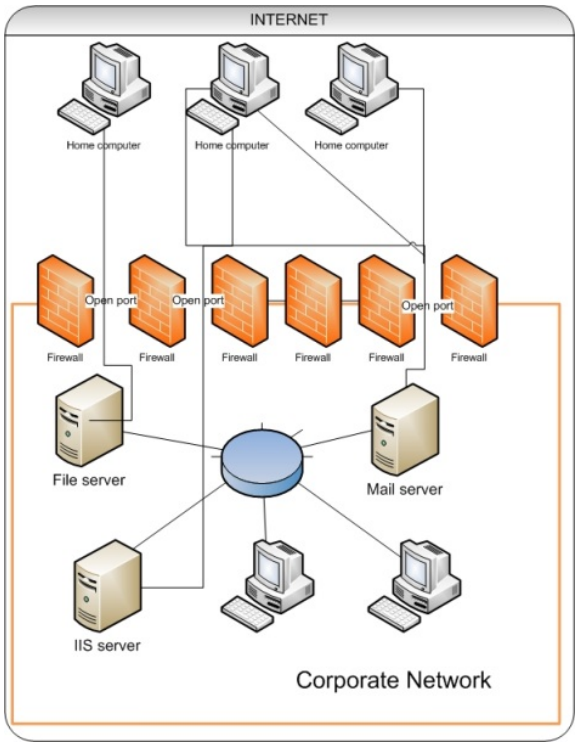

Figure 2. Communication between a corporate information system and the Internet via firewall, as in the past.

Until recently there were no wireless mobile devices that could establish connections to the Internet and other systems, such as WiFi, UMTS, etc.A firewall regulates communication between a mobile device and the information system it is protecting, but the weak link in the whole system is a mobile device connected to a public network. When a mobile device is breached, while it is connected to the Internet, an unprotected path to the central information system is opened – the firewall has already allowed access to the information system (Figure 3).

The cloud is usually integrated into the information system and controlled by the corporation. Figure 4 shows a corporate central information system comprising a cloud. The cloud can be owned by the corporation or leased from an outside provider, who is responsible for maintenance and trouble-shooting. Employees access data through their mobile devices and the Internet. Because public networks can't be monitored and controlled by the corporation, their devices and information systems are exposed to various threats. These can be indirect (theft of device, listening in, interception of communication, etc.) or direct; the latter are unpredictable, so total protection is almost impossible.

Public cloud is leased by a corporation or other organization, as shown in figure 5. In this case the cloud itself presents a danger. As in the case shown in figure 2, here also, the possibility of a breach is relatively big. Threats present themselves independently or simultaneously. The risk of a breach and loss of data is greater when two systems are under attack. Because a private cloud is at a remote location, it is a weak spot in the information system.

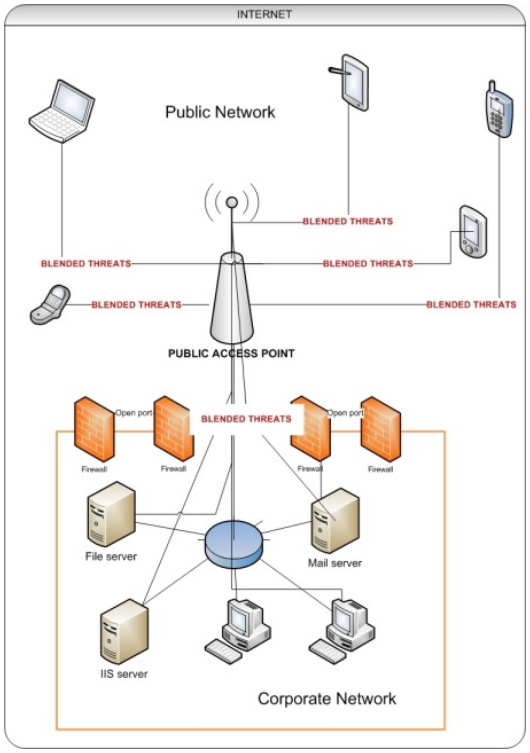

Figure 3. Communication between a corporate information system and a mobile device, and communication between a mobile device and the Internet, as currently possible.

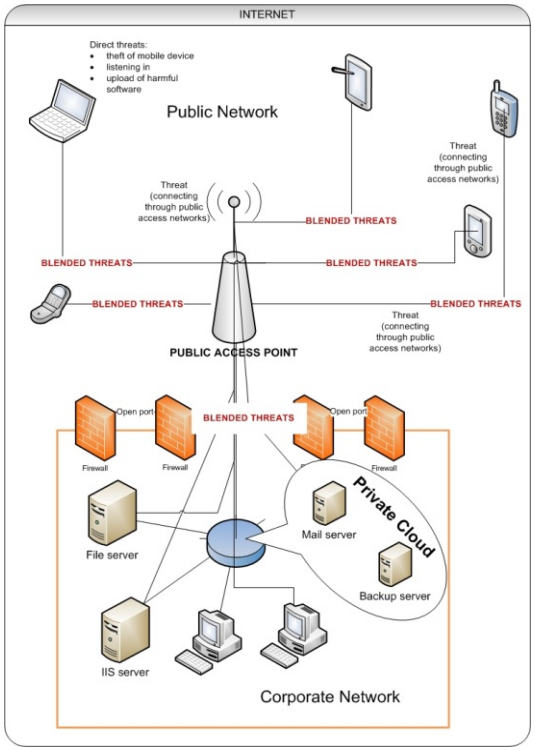

Figure 4. Communication between the central information system and a mobile device, communication between a mobile device and the Internet, and the utilization of the private cloud.

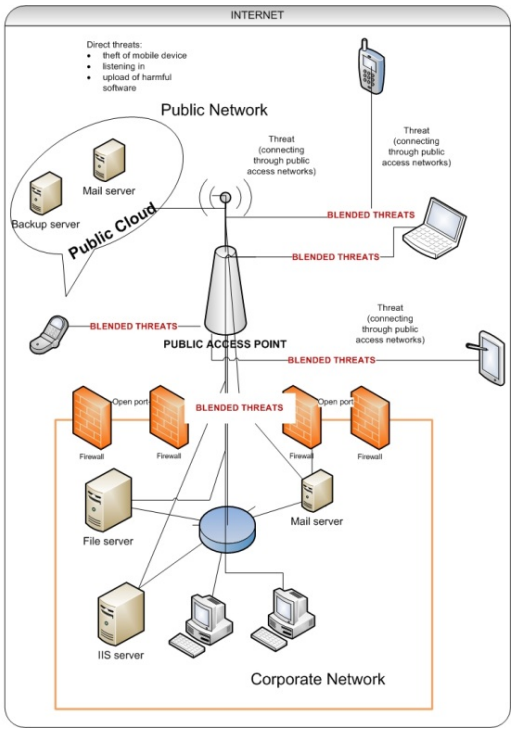

Figure 5. Communication between the central information system and a mobile device, communication between a mobile device and the Internet, and the utilization of a public cloud.

Since a mobile device can simultaneously communicate with various networks, and the corporate security system allows access to the information system, the mobile device under attack of blended threats can seriously endanger the corporation's assets (i.e. data and information). Technical solutions are currently under development, but because there are yet no general standards, new safety measures probably won't be optimally effective, at least not in the long term. Changes and adaptations will always be necessary.

5. Safety Standards and Regulations for Safer Use of Mobile Devices

Awareness of safety issues in regard to mobile devices can be a competitive advantage in business and/or science. Information security is the key to the integrity of any organization, its employees, business processes and compiled data. The lack of knowledge about the safety risks of mobile devices and internal safety standards can get an organization into serious trouble. An ignorant user is the first weak point in any information system; the second weak point is the absence of standards for the use of hardware and software. Because of the rapid development of information technology, which is now used by the majority of employees, it is necessary to constantly inform and educate users of the pitfalls of modern technology. The goal of any organization should be to ensure that all information technology is used safely.

A. Safety Regulations

Mobile devices are safe, if they are used in compliance with safety regulations – these should be based on the following:

- Better information security can be achieved, if an organization defines its own safety standards and regulations.
- Safety regulations are a control factor, functioning as preventive measures in cases of irresponsible usage of mobile devices in the corporate environment.
- Safety regulations define how and why mobile devices and software can be used.
- Safety regulations also define legal responsibilities of the user and/or the organization, if damages arise from irresponsible usage of mobile devices.

If an organization succeeds in getting their employees to comply with safety standards for the usage of mobile devices, then it has also successfully limited the risks of blended threats.

B. Mobile Device Protection Toolkit

To ensure that mobile devices are secure, we need to follow at least the most basic protective measures.

Threats currently plaguing the highly mobile world are, not surprisingly, pretty much the same as we find in computing in general. The implication is clear: we need strategies and tools that are remarkably similar to those we've been using on desktop and notebook PCs for some time. These are the key requirements for building our mobile device security toolkit (examine the solutions available) [25]:

- Viruses and malware: Antivirus software for the mobile device operating system is available from a few vendors today, but this can't always be recommended. It's still best to educate users in the basics – don't visit arbitrary websites, don't download anything that's not authorized by IT, and use mobile device management capabilities from your carrier or implemented within the corporation to verify and control the configuration of your mobile devices.
- Encryption: Carrier networks have good encryption of the airlink in every case, but the rest of the chain between client and corporate server remains open, unless explicitly managed. Always use a VPN connection when dealing with sensitive data. SSL is the preferred solution, but there are many good mobile VPN strategies available. Sensitive data should be available only to authorized users, so file and volume encryption should really be used.
- Authentication and authorization: These requirements fit in nicely with the RADIUS or similar solution that you're already using for remote access. We might also look into obtaining, or enabling (if the mobile device OS is already equipped), firewall functionality, just as we already do on our laptops and notebooks.
- Physical security: Mobile devices will get lost; that's why authentication and encryption are so important. Mobile device management can handle the "phone home" or "remote wipe," depending upon our preference. But plan for device loss; it will happen much more often than you think it will.

C. Ensuring a High Level of Information Security for Mobile Devices

The figure below shows, which security incidences are a threat to mobile device users, and how they can protect themselves. Specific threats are:

- Unauthorized access to sensitive data stored in the device,
- Unauthorized access to data stored on corporate networks,
- Attacks from malicious software,
- The ability to impersonate the authorized user.

Protection from blended threats can only be achieved, if the corporation or other organization has an internal safety policy that regulates information security. Table 1 shows how to use certain security techniques as a leverage to mitigate the risk of threats to mobile devices [26].

Table 1. Security techniques used to mitigate information security risks.

Mobile device access	Power-on authentication – Require a power-on password or PIN, so the device cannot even be powered by an unauthorized user. Implement a standard process for creating unique usernames and PINs.
	Auto-lock – Configure device to automatically lock up after a certain period of time.
	Two-factor authentication – Implement two-factor authentication for access to systems that contain PHI. Consider the use of tokens, call-back, and biometrics.
Data storage	Data encryption – Establish data encryption for mobile devices. Identify the types of hardware and electronic media that must be tracked (hard drives, digital memory cards) and develop inventory control systems.
	Auto-run applications – Prevent memory cards from automatically running specific programs.
Data transmission	Encryption – Implement and mandate appropriately strong encryption solutions for transmission of PHI. For example access can be implemented over SSL, IPSec or a similar VPN technology.
	Signed applications – Allow only signed applications to be loaded onto the devices (S/MIME, token-based).
Data access	Role-based – Employ role-based access as part of a user-provisioning solution. Different users may require different levels of access based on job function. Develop and employ proper clearance procedures and verify training of workforce members prior to granting access.
	Logging and auditing – Implement logging and auditing on device and parent network. Ensure that the issue of unauthorized access of PHI is appropriately addressed in the required sanction policy.

6. Discussion

Trends in the development of information security technology show that, in the future, analyzing Internet traffic as well as deviations in routine system functions will come to the foreground. The human factor is most often ignored or overlooked. Any user unaware of the dangers is inevitably the weakest link. Every employer should realize the importance of educating employees, because this is the only way to gain control over various threats to mobile devices and consequently to the corporate information system.

In the past the need to secure business information was stressed, but it is now evident how important it is to ensure safe usage of mobile devices, especially since these are handled by increasing numbers of users [27]. An information system is as weak (or strong) as its weakest link. It is therefore important to focus on the least predictable

and most uncontrollable elements (namely mobile devices) of the system, but also to uphold security of all other parts of the system, i.e. the central corporate system, different clouds, etc. [28]. A step towards better security is any attempt to spread the knowledge of the dangers of various threats to information systems, and also of the consequences of security breaches [29]. One way for owners and information system managers to ensure protection is to put in place a solid safety policy [30]. A good security policy encompasses standardized rules and regulations for the safest use of mobile devices [31]. These should be based on the following guidelines:

- Better information security can be achieved, if an organization defines its own safety standards and regulations.
- Rules and regulations are control factors, functioning as preventive measures to deter irresponsible usage of mobile devices in the corporate environment.
- Standards should define which mobile devices and software can be used, and how they should be used.
- Regulations also define the legal responsibilities of users and/or corporation in case of damages due to irresponsible use of mobile devices.

In addition, corporations should monitor communication channels and Internet traffic, install firewalls, encrypt data, and be able to remotely erase data in case a mobile device gets lost or stolen. Certain software solutions exist which enable the user to locate and lock a lost or stolen mobile device. This software enables remote erasure of data or return to the manufacturer's default settings [32]. User authorization should also be in compliance with information security standards [2]. It's also important to choose the appropriate cloud services and configuration of the central information system. Furthermore, it's necessary to have standards and rules to define the most appropriate devices and software allowed. Software for mobile devices changes rapidly, therefore information system protection should be as flexible and efficient as possible. Current security guidelines in regard to hardware and software only partially cover issues concerning mobile devices. So far we are still without a system that could effectively monitor (or restrict) communication and flow of data between mobile devices and information systems.

7. References

[1] Infiniti Research Limited, "Global Cloud System Management Software Market 2010-2014", http://www.marketresearch.com/Infiniti-Research-Limited-v2680/Global-Cloud-Systems-Management-Software-6458283/view-stat (Access Date: 7. 9. 2011)

[2] Ericka Chickowski, "10 Mobile Security Best Practices", http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Mobile-Security-Best-Practices (Access Date: 10. 1. 2011)

[3] M. E. Whitman, and H. J. Mattord, Management of Information and Security, 2nd edition. Boston: Course Technology Cengage Learning, 2008.

[4] Karen Scarfone, Peter Mell, "Guide To Intrusion Detection and Prevention System", http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (Access Date: 4. 3. 2011)

[5] Dave Schechtman, "IPad Security from En Pointe and McAfee's Mobile Security Practice", http://www.enpointe.com/blog/ipad-security-en-pointe-and-mcafees-mobile-security-practice (Access Date 5. 3. 2011)

[6] Sneha Endait, "Mobile Security – The Time is Now", http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security (Access Date 5. 3. 2011)

[7] Peter Mottishaw, "Policy Management Will Be Critical to Mobile Operators as Data Traffic Grows", http://www.analysysmason.com/About-Us/News/Newsletter/Policy-management-has-become-an-urgent-issue-for-mobile-operators-as-a-result-of-the-rapid-growth-in-mobile-data-traffic-increasing-availability-of-flat-rate-data-plans-and-new-regulations-in-Europe (Access Date: 6. 3. 2011)

[8] William Arbaugh, "Wireless Security Is Different", svn.assembla.com/svn/odinIDS/Egio/artigos/.../Firewall/01220591_IMP.pdf (Access Date: 5. 3. 2011)

[9] A. Calder, Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide. Hogeweg: Van Haren Publishing B. V., 2006.

[10] I. Bernik, and K. Prislan, "Information Security in Risk Management Systems: Slovenian Perspective". B. Dobovšek and A. Sotlar (edit.), Varstvoslovje, vol. 13(2), pp. 208-222, 2011.

[11] A. Weber, and A. Darbellay, "Legal Issues in Mobile Banking" in Journal of Banking Regulation, vol. 11(2), pp. 129-145, 2010.

[12] R. G. Chicone, An Exploration of Security Implementations for Mobile Wireless Software Applications within Organizations. Minneapolis: Graduate Faculty of the School of Business and Technology Management, Northcentral University, 2010.

[13] M. K. Riedy, S. Beros, and H. J. Wen, "Management Business Smart Phone Data" in Journal of Internet Law, pp. 3-14, 2011.

[14] IDC, "IDC - Press Release", http://www.idc.com/getdoc.jsp?containerId=prUS22871611 (Access Date: 10 .9. 2011)

[15] Juniper Networks, "Malicious Mobile Threats Report 2010/2011", http://www.juniper.net/us/en/dm/interop/go (Access Date: 10. 9. 2011)

[16] Jon Brodkin, "Gartner: Seven Cloud Computing Security Risks", www.infoworld.com (Access Date: 27. 4. 2011)

[17] Neal Leavitt, "Mobile Security: Finally a Serious Problem?", Largo: University of Maryland, http://www.computer.org/portal/web/computingnow (Access Date: 7. 9. 2011)

[18] Lookout, "Lookout Mobile Threat Report", https://www.mylookout.com/mobile-threat-report (Access Date: 10. 9. 2011)

[19] Lookout, "Zlonamerna koda nad zasebnost uporabnikov mobilnikov Android", http://www.racunalniske-novice.com/novice/mobilna-telefonija/google/zlonamerna-koda-nad-zasebnost-uporabnikov-mobilnikov-android.html (Access Date: 7. 9. 2011)

[20] Marc Flores, "What Your Cell Phone Data Reveals About You and Your Life", http://www.intomobile.com/2011/04/25/your-cell-phone-data-reveals-you-and-your-life Acquired (Access Date: 7. 9. 2011)

[21] Lenart J Kučić, "Uporabniki hočejo imeti pravico do elektronske svobode",

http://www.delo.si/druzba/infoteh/uporabniki-hocejo-imeti-pravico-do-elektronske-pozabe.html (Access Date: 12. 9. 2011)

[22] Matej Saksida, "Preprečite uhajanje podatkov iz omrežja", http://dne.enaa.com/Racunalniska-oprema/Racunalniska-oprema/Preprecite-uhajanje-podatkov-iz-podjetij.html (Access Date: 17. 1. 2011)

[23] M. Allen, "Mobile Security" in The Journal of International Security, vol 16(6), pp. 25-27, 2006.

[24] B. Markelj, and I. Bernik, "Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav". Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb [Digital source]: zbornik konference / 18. konferenca Dnevi slovenske informatike, Portorož, Slovenija, 18.-20. april 2011.

[25] Mathias, C. ,Mobile Security Threats. http://searchmobilecomputing.techtarget.com/tip/Mobile-security-threats (Access Date: 20. 10.2011).

[26] Booz Allen Hamilton ,. Mobile Device Security. http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf. (Access Date: 20.10. 2011)

[27] N. Boudriga, *Security Of Mobile Communications.* New York: Auerbach Publications, 2010.

[28] Jim Metzler, Steve Taylor, "Security for Mobile Devices on the Corporate Network", http://www.networkworld.com/newsletters/2010/032210wan1.html (Access Date: 15, 2011)

[29] European Network and Information Security Agency (ENISA), The New User`s Guide: How to Rise Informations Security Awareness. Luxembourg: Publications Office of the European Union, 2010.

[30] I. Bernik, and K. Prislan, "Proces upravljanja s tveganji v informacijski varnosti", P. Umek and T. Pavšič Mravlje (edit.), Smernice sodobnega varstvoslovja [Digital source]: zbornik prispevkov. 11. slovenski dnevi varstvoslovja, Ljubljana, 3.-4. junij 2010. Ljubljana: Fakulteta za varnostne vede, http://www.fvv.uni-mb.si/DV2010/zbornik.html (Access Date: 1. 3. 2011)

[31] Simt, "Upravljanje, nadzor in varnost informacijskih sistemov", http://www.simt.si/informacijski_sistemi.html (Access Date: 11. 10. 2011)

[32] Lisa Phifer, "Find remote mobile device wipe solutions on a budget", http://searchmidmarketsecurity.techtarget.com/tip/Find-remote-mobile-device-wipe-solutions-on-a-budget (Access Date: 7. 9. 2011)

