Mobile Devices and Corporate Data Security

Blaž Markelj, Igor Bernik

***Abstract*—**Ensuring protection of corporate data has only recently become a main concern in the information and communication technology industry. In the past two years or so the use of mobile devices to access data has become a lot more frequent, therefore data security is now a new challenge for users and managers of information and computer systems alike – they all have to be aware of cyber threats, and the measures, which must necessarily be undertaken to maintain an adequate level of information security. Software for mobile devices, combined with the Internet, now provides easy and fast access to data and information; this relatively new technology facilitates rapid decision-making. Sophisticated software enables users to manage data and carry out various tasks on-line. The security of corporate data, in incidences when mobile devices are used to access information systems, can only be upheld, if users comply with certain safety measures.

***Keywords*—blended threats, corporate data, information security, mobile devices**

I. Introduction

The fast pace of modern life, accelerated business processes and decision-making, have all created the need for fast and reliable access to data and information. Due to the incredible development of technology and the changing methods of communication, it is unimaginable that one wouldn't have constant access to data and information. Mobile devices, which have recently become ubiquitous, offer easy connections to the world of information. Recent development (wireless technology) has also changed how we access the Internet and pushed corporations into centralizing their information systems. Thus users now have uninterrupted access to corporate databases and information, which speeds up the working process and decision-making. The knowledge, how to use mobile devices safely and efficiently, can be a competitive advantage in business and science. On the other hand there is the issue of information security. When corporations minimize the possibility of unauthorized and malicious access to their information system, theft and misuse of their data, they strengthen their business credibility. Therefore, maintaining information safety is a necessity [1].

Mobile devices, such as laptops, smartphones and PDAs, have become an essential part of our daily life. They are small and easy to carry but nevertheless powerful in computational and storage capabilities. Unfortunately, these merits also pose a certain risk. For example, because mobile devices are small, they are quite easily stolen, especially in public places like an airport terminal, library or café. Recently, as mobile devices got slimmer and more powerful, the number of mobile device thefts surged. According to the FBI's National Crime Information Center, the number of reported laptop thefts in 2008 rose with a 48 % increase over the previous two years, from 73.700 to almost 109.000 [2].

Almost all mobile devices facilitate a connection to the Internet and thus access to corporate information systems, and further, manipulation and transfer of data. Some corporations intentionally have open ports, so that their employees can work in virtual environments. This is an opportunity for anyone on the Internet, who wishes to access a corporation's information system unauthorized. From the safety viewpoint, besides many individual and/or blended threats, the following are the greatest risks: software for mobile devices, public networks, unprotected certificates, and the loss or theft of a mobile device.

Certain programs automatically cyclically transfer data from a corporate information system to a user's mobile telephone – this happens as soon as the user types in his username, password and server data. It is questionable, if software running automatically can be at all trusted. What is a program running in the background actually doing? What happens, if our telephone gets stolen? Our telephone contains much information, including data to access the domain and server system [3]. This means that anyone who "breaks into" the mobile devices, while it is connected to the Internet, can eavesdrop on all communication between the device and a corporate information system.

When we started using wireless mobile communication devices, we dismantled the "border" between internal information systems and the outer world. Today, an ICT web covers the world: everyone can communicate with anyone else, upload and transfer data. It has become fat too easy to get to crucial personal or business data. Developers and providers of security software are looking for ways to analyze and monitor contents flowing through communication channels. It is apparent that future technology will make it possible to analyze Internet traffic and information systems based on detected deviations from the routine. Regrettably, we still don't have simple, transparent solutions (from the user's point of view) to protect information systems from cyber criminals.

Users and mobile devices carry special-purpose wireless sensing devices, which work with the wireless network infrastructure to provide protection to the mobile device and the data stored in it. The system has the following features [2]:

- Context awareness: sensors carried by users and mobile devices collect context information (e.g., proximity between users and mobile devices) and the system adapts its behavior properly and promptly to the context change.
- Anti-theft protection for mobile device: the system will alert the user (directly or multi-hop via the wireless network infrastructure), when it detects a potential theft (e.g., via proximity sensor and motion sensor).
- Privacy protection for user data on mobile device: the system adapts the privacy protection level for user data on

mobile device. For example, when a user is away from his mobile device, user data on device shall be encrypted.

- Transparency: the system adapts its behavior autonomously, without requiring explicit user intervention.

II. MOBILE DEVICE USAGE

Even though mobile devices have introduced a new dimension into life and work, they aren't a very recent invention. In the past two decades several companies have tried to make a commercial break-through with palm and tablet computers, but sales and the number of users truly soared only after Apple introduced the iPhone and iPad. Today's smartphones with the iOS and Android OS represent useful working tools that enable people to be constantly connected to cyberspace and thus have remote access to business and other data.

Recent trends in enterprise mobility have made mobile device security an imperative. IDC reported in 2010 that for the first time smartphone sales outpaced PC sales. Faced by this onslaught of devices and recognizing the productivity and cost benefits, organizations are increasingly implementing bring-your-own device (BYOD) policies. Research firm J. Gold Associates reported that about 25 % - 35 % of corporations currently have a BYOD policy, and they expect the number of these to exceed 50 % over the next two years. This makes sense as mobility evolves from a nice-to-have capability to a business advantage [4].

It is crucial to know, what our mobile device is capable of performing, and there are two main reasons for this.

- We can exploit all possibilities of the device and its software to the maximum. This knowledge helps us simplifies many tasks and speed up working processes, and also transforms our perception of how we can conduct business.
- We gain awareness of, which functions of the device and its software represent a potential weak link in regard to cyber threats. Knowing, when data is most exposed and vulnerable, helps us adopt appropriate protective measures.

Users, who use their mobile device for business purposes (to access data in the central corporate information system), and also for personal needs (computer games, e-bank applications, GPS modules etc.), are at greater risk of having their data stolen or of suffering the consequences of other dangers posed by mobile devices.

Keeping data stored in a mobile device secure is not just a daunting challenge, but a critical requirement. Unfortunately, a majority of the mobile device users do not take necessary actions to protect the data stored in their mobile devices. Therefore, the loss of a mobile device could mean the loss and exposure of sensitive information stored in the lost device, which may be much more valuable than the device itself. According to CNN, a laptop theft case in 2006 related to the Veterans Affairs Department resulted in the exposure of millions of veterans' personally identifiable information, and it cost the department 20 million dollars to settle the lawsuit against it [2].

The competitive edge and other benefits of mobility can be wasted, if smartphones and tablet PCs are not adequately protected against mobile device security threats. While the market shows no sign of slowing, IT organizations identify security as one of their greatest concerns in regard to the extending mobility [4].

Many companies market software for mobile devices. This software has many useful functions. The authors Pocatilu, Doinea and Ciurea [5] have described in their article the advantages of software solutions for e-learning (current contents and accessibility). On one hand, users can choose those study materials, which they find most interesting, and on the other, educators can reach a wider audience. A central database of study materials, located on a central server, is easier to update and maintain. Software for e-learning is a good example, how technology influences not just the development of individuals but of society as a whole. The life span or cycle of such software should coincide with the current needs of society.

Furthermore, a mobile device loaded with specific software can help us monitor our home or vehicle security system. Details of security monitoring software were described in an article by authors Wu, Peng and Chen [6]. These authors have also presented test results for the mentioned software. Today, mobile devices also facilitate live distribution of video, which means that it is possible for the device to connect to a remote video surveillance system and monitor activities as they unfold.

It has been possible for some years now to use a mobile device with specific software for electronic banking, and, as noted by authors Tie-Jun and Lei-Na [7], to carry out on-line money transactions. These two authors described not only how money transactions are carried out but also certain software applications and safety precautions. Despite all security measures applied to e-banking the user must be aware of the many threats to mobile devices, and through them to information systems. When a mobile device is lost, the user is in danger that he will also lose crucial data and possibly even his money. Despite satellite tracking [8], it is highly unlikely that a lost or stolen mobile device will be retrieved.

Probably one of the most useful software solutions is email synchronization. Different software allows the user to synchronize different data, from email to calendars etc.

A. Blended Threats to Mobile Devices

Mobile devices are targeted by blended threats, with the goal to unlawfully acquire restricted information and profit from this. Threats act on various levels and can work simultaneously, thus the name blended threats. Blended threats are a significant danger to individuals and organizations alike [9]. When a connection with the Internet is established (and through this with a corporate network), the organization is immediately in severe risk. Threats can be direct or indirect and individual or combined. The most direct threat is the theft of a mobile device. If the owner has stored crucial information

and documents in his mobile device, but hasn't used even the most basic protection (e.g., PIN code), then he can blame himself for any unpleasant consequences. More sophisticated threats are interceptions of communication and implanted software, which automatically harvests information. Indirect threats are usually more severe, because they are unpredictable, and total protection from them is virtually impossible.

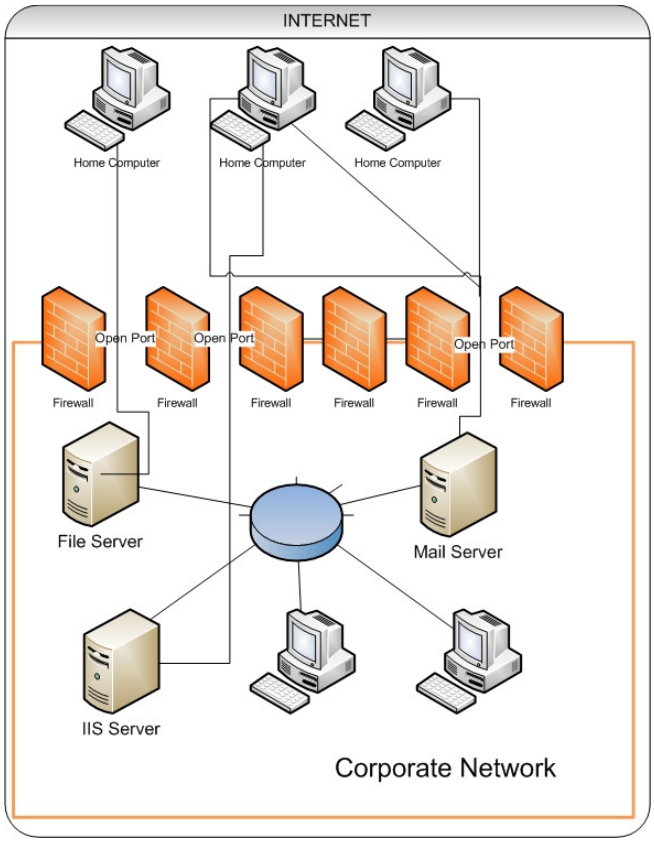

Figure 1: Communication between a corporate information system and the Internet via firewall, as in the past.

Contemporary communications, access to corporate networks and methods of connecting to them have recently changed significantly. Figure 1 shows the difference in communication between the central information system (Intranet) and the Internet.

It used to suffice that the information system was protected by a firewall, which monitored incoming communication. Until recently there were no external mobile devices that could connect to corporate networks and communicate with the world via WiFi, UMTS, etc. Users today use various mobile devices to establish connections and communication with different networks, regardless of firewalls. 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 that is 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. This happens because the firewall has already permitted communication between the device and system.

Since the mobile device communicates with several networks simultaneously, and the firewall has already allowed access to the corporate information system, the user is in a position, where his mobile device is open to blended threats (Figure 1 and 2). The mobile device is a gateway to the "treasury" of the corporation – the data and information stored in its information systems.

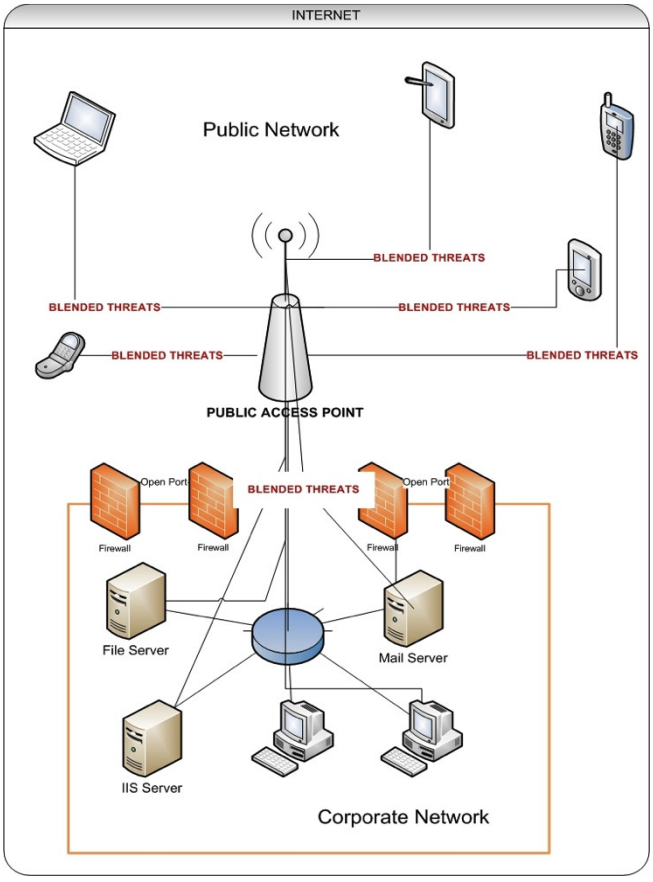

Figure 2: Communication between a corporate information system and mobile device, and communication between mobile device and the Internet, as currently possible.

Threats that usually lurked on the communication pathway (which, in the past, users have learned how to master) are now, due to their variety and combined effects, a serious risk to corporate networks. Solutions are currently under development, but because there are no general standards, new safety measures will probably not be optimally effective, at least not in the long term. Constant changes and adaptations will be needed.

It is up to individual users and organizations, how they ensure that they use safe connections to information systems and how they protect sensitive private or corporate data. In the past, the need for corporate information safety was, of course, stressed, but now it is becoming more and more evident that it is also vital to promote safe usage of mobile devices [10]. Any information system is as safe as its weakest link. Therefore it is important to focus on the least controllable elements, especially mobile devices. It is imperative to provide effective protection from blended threats [11].

A step towards better security is being aware of the various

threats to information systems and their consequences [12] One way for an organization to protect itself is to put in place a solid policy for maintaining the safety of their information system [13]. A good safety policy encompasses standardized rules for the safest usage of mobile devices. This is the basis for determining, which hardware and software are the most appropriate for an organization [14]. Furthermore, it is necessary to monitor network traffic, set up firewalls, encrypt data, and enable remote erasure of data from a stolen mobile device. Also, authorization of access to the system must be in compliance with standards and recommendations for ensuring the highest level of information security [3].

III. Safe Usage of Mobile Devices and Software

The rapid development and expansion of big information systems is followed, specifically, by advancements in the technology of mobile devices and software for them [15]. Recently the number of people using mobile telephones and tablet personal computers has risen significantly [16], [17]. 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 [18]. Mobile devices with sophisticated software are quite functional 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.

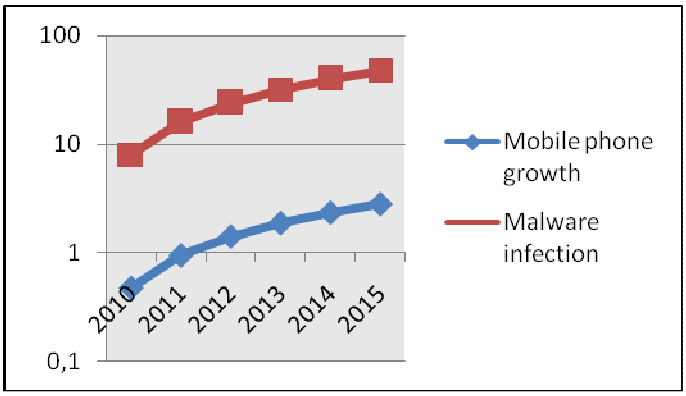

Figure 3: A comparison of the growth in mobile phone sales and the number of malware infections (logarithm ordinate axis).

Figure 3 shows the rising trend in the number of malware attacks in relation to the number of mobile telephones sold – based on research carried out by [18] and [19]. On the basis of this data, it is possible to get an ideal of how fast the numbers of both smartphones and malware are growing. The diagram of the 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 Internet in general.

When a mobile telephone is used to access data in an organization's information system software on the device can function only as a user application, which displays data. 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, also be aware of information security issues and act accordingly. Often this is not the case, therefore certain software on mobile devices runs unnoticed. 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. Many banks have already implemented their own software solutions for mobile devices, so that their clients can manage their bank accounts with the help of their mobile device. Corporations use such software for mobile devices to improve their market shares (B2C) and in direct sales (B2B) [20]. Specific software for mobile devices can also be used in education, since they facilitate e-learning.

Such software may contain potentially harmful code, so consequently our data or money can be stolen [21]. 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 [21]. Results of research carried out by Lookout show that the volume of 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. 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 [19] also states that 85 % of users have inefficient software protection on their telephones.

Providers of software for mobile devices usually install "back doors", programs that 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 [22]. Flores [23] noted that the results of recently carried out research 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 [24] 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 an information system or cloud and greatly increase the risk that data will be stolen and/or misused. This endangers the integrity and business of the whole organization [1].

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, etc. Employees must be informed about the consequences of harmful activities or the incorrect usage of a mobile device [25], [26].

IV. SECURITY SOLUTIONS TODAY

Mobile security threats come in many forms, and they are rapidly evolving. Many corporations now have mobility at the center of their IT strategy, and it will serve you well to put new emphasis on your mobile device security strategy [27]. Milligan [28] noted in his article that corporations and other organization can't monitor something that can't be identified. What the author had in mind, were threats endangering corporations, which come with the usage of the rapidly evolving mobile devices and information technology in general. Therefore, corporations should constantly upgrade their information security policies and assess the risk of having their system breached. Corporations minimize risk by implementing hardware, which checks for potential dangers at the level of Internet traffic [26], and special equipment, which prevents invasions into information systems [29]. Some companies that are developing security software are already providing advanced software solutions for mobile devices [30], and firewalls, which monitor Internet traffic on the mobile device and the information system [31]. Certain software enables corporations to define their own safety guidelines for the use of mobile devices [32]. Employees usually have passwords to wireless networks [33]. Some corporations implemented their own rules for maintaining information security in the process of acquiring the ISO 27001 certificate [34], [35].

Corporations can protect their data by using encryption software, but this method of protection is only as strong as the encryption key itself. It is possible to encrypt only certain segments of data stored on a mobile device, or data transferred through the Internet, or an information system as a whole. The encryption should in no way hinder the functions of a mobile device. Gilaberte [36] wrote about various methods and algorithms, which can be used to encrypt certain data in certain ways. Corporations strive to achieve better information security, especially in regard to log-on procedures, and/or the transfer of crucial data and information. This can be accomplished by implementing safer »http« data transfer protocols, and by authentication with certificates, as well as by encrypting and decrypting data (SSL), and also by the use of virtual private networks (VPN). Good examples of how the above-mentioned technology is used are bank portals and portals used for managing email. Certificates are used to authenticate the identity of a user when he or she tries to access these portals. Corporations try to protect their data by using strong passwords and authentication by a smart-card. Smart-cards can function only, if supported by sophisticated »background« technology.

Most corporations and other organizations set up virtual private networks to enable direct communication between mobile devices and their corporate information system or systems. This technology functions on the principle of establishing a »channel« between the virtual private network software of the mobile device and the virtual private network server located within a corporation's information system. Verification between a mobile device and an information system is done by using certificates – entrance to the system is granted once the identity of the user is verified (username, password). Zheng Yan and Peng Zhang [37] noted in their article that we should be aware of two crucial security weaknesses in the virtual private network technology. These are: (1) software for mobile devices and virtual private network clients are so diverse that it is impossible to guarantee that the technology will work flawlessly; (2) it is questionable, whether the software on a mobile device (including specific software used to establish a connection to a virtual private network) can be fully trusted.

As noted by Milligan [28] some security measures in use today (table 1) are inadequate protection for mobile devices against blended threats (shown in table 2). He also discloses which measures could significantly enhance information security in regard to the use of mobile devices. Some of the proposed measures are shown in table 3. The list of protective measures, as proposed by Milligan, is compiled on the basis of research, carried out by CIO Magazine and PricewaterhouseCoopers, of 250 organizations in Great Britain and other European countries, the USA, Canada and India.

Different Solutions For Maintaining Information Security Today		
NETWORK	**MOBILE DEVICES**	**USERS**
VPN		
Encryption		Education
Authentication		Awareness
Firewall		Restriction
IPS, IDS systems		

Table 1: These are the solutions, which are currently used to maintain information security.

Why These Solutions For Maintaining Information Security are Insufficient Today		
NETWORK	**MOBILE DEVICES**	**USERS**
VPN (insufficient)		
Encryption (endpoint not encrypted)		Education (not specially for mobile device security)
Authentication (not always possible)		Awareness (lacking)
WAN integration (problems with insufficient integration within corporate WAN security)		
Firewall (insufficient)		Restriction (not always present)
IPS, IDS systems (insufficient)		

Table 2: A short explanation, why currently used solutions for maintaining information security are no longer sufficient.

Suggested Solutions For Maintaining Information Security		
NETWORK	**MOBILE DEVICES**	**USERS**
Peer to peer not allowed	Authentication (password, access key, biometric access)	Awareness (report possible threats)
Searching for unauthorized usage network	Anti-malware and anti-virus software	Education
Accessing data just on servers in DMZ		
Remote wipe device		
Controls for traffic and applications using corporate network		
Policy for controlling and surveying		

Table 3: This is a quick overview of suggested measures for achieving better information security.

V. 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) [27]:

- 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.

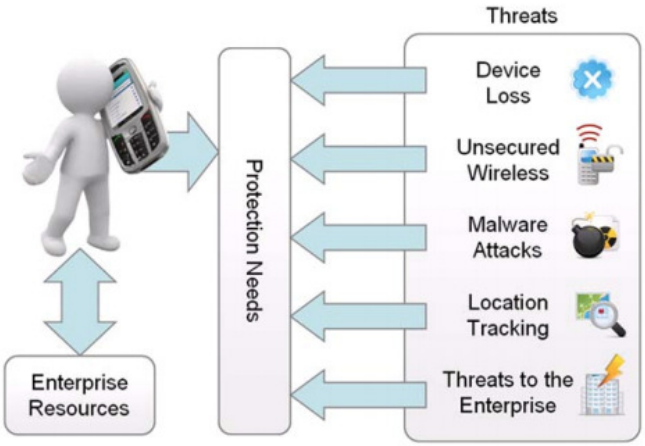

Figure 4: This is an overview of the basis threats to corporate information security [38].

Protection from blended threats can only be achieved, if the corporation or other organization has an internal safety policy that regulates information security. Table 4 shows how to use certain security techniques as a leverage to mitigate the risk of threats to mobile devices [38].

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.

Table 4: Security techniques used to mitigate information security risks.

VI. Conclusion

Technological innovations have put an end to traditional working processes. The advantages of using mobile devices in business now play an integral part in the workplace, but new technologies also pose some serious threats to information security. With this in mind, it is necessary to plan activities at all levels within a corporation or organization, which are somehow connected to mobile device usage and advanced information technologies. It is also important to standardize working processes; to determine, which procedures are in compliance with information security standards; and to set safety policies for the usage of mobile devices and wireless networks. A crucial part of information security, is the privacy issue – the standards for this issue should also be defined within an organization.

Technological development in information security is focused on analyzing Internet traffic and the behavior of information systems. Development is based on discovering discrepancies in standard behavior of Internet traffic or the system. The human factor is still mainly overlooked. After all, people are the ones using and managing information technology, and thus always represent the weakest link in information security. It is crucial for corporations to become aware that development of increasingly sophisticated mobile devices cannot be stopped. It is important for corporations to provide constant training and education for their employees, and so alleviate the risks to information security. It is necessary that corporations have internal regulations for the safest usage of mobile devices and, based on their existing technology, determine, which mobile devices and software are most suitable for them.

The usage of mobile devices can't be restricted just because they represent an information security risk, but we should use this technology wisely. The following advice is useful:

- Don’t ignore, but investigate the complete range of mobile devices, which are used to enhance workflows and business processes within the corporation.
- Set a strategy. Realize that mobile and wireless technologies will inevitably create new privacy and security challenges that will require new policies and technical controls. Be sure to include device ownership, support and maintenance.
- Choose the integration approach and employ standards-based technologies where possible.
- Monitor and manage.

New mobile devices, and software for them, are developed extremely fast; the process is unpredictable. It is crucial to maintain a flexible and safe information system. Current safety measures tend to only partially cover mobile devices and their software. There is yet no system, which could enable corporations to monitor the performance of their information system in regard to accessing and transferring data via mobile devices.

REFERENCES

[1] Saksida, M. (2008). *Preprečite uhajanje podatkov iz omrežja*. Acquired 17. 1. 2011. at http://dne.enaa.com/Racunalniska-oprema/Racunalniska-oprema/Preprecite-uhajanje-podatkov-iz-podjetij.html

[2] Yang, K., Subramanian, N., Qiao, D. and Zhang, W. (2009). *A Pervasive Mobile Device Protection System.* Acquired 20. 10. 2011 at http://www.ieee-infocom.org/2009/demos/4%20-%20A%20pervasive%20mobile%20device%20protection%20system.pdf.

[3] Chickowski, E. (2009). *10 Mobile Security Best Practices*. Acquired 10. 1. 2011 at http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Mobile-Security-Best-Practices.

[4] Learning guide: Mobile device protection (2011). Acquired 20. 10. 2011 at http://searchmobilecomputing.techtarget.com/guides/Mobile-device-protection-and-security-threat-measures.

[5] Pocatilu, P. , Doinea, M. and Cirurea, C. (2010). Development of distributed mobile learning systems. *9th WSEAS Int. Conf. on Circuits, systems, electronics, control & signal processing: Conference Proceedings (pp 196-201)*. Stevens Point, Wisconsin: WSEAS.

[6] Wu, B.-F. , Peng, H.-Y. and Chen, C.-J. (2006). A Practical Home Security System via Mobile Phones. *5th WSEAS Int. Conf. on Telecommunications and Informatics: Conference Proceedings (pp. 299-304)*. Stevens Point, Wisconsin: WSEAS.

[7] Tie-Jun, P. and Lei-Na, Z. (2006). Security key: a new mobile payment solution. *5th WSEAS Int. Conf. on Information Security and Privacy: Conference Proceedings (pp 152-155*). Stevens Point, Wisconsin: WSEAS.

[8] Kämppi, P. , Rajamäki, J. and Guinness, R. (2009). Information security in satellite tracking systems. *3rd Int. Conf. on Communications and information technology: Conference Proceedings (pp 153-157)*. Stevens Point, Wisconsin: WSEAS.

[9] Markelj, B. and Bernik, I. (2011). *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.

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

[11] International Data Group Company. *Security for Mobile Devices on the Corporate Network*. Acquired 15. 1. 2011 at http://www.networkworld.com/newsletters/2010/032210wan1.html.

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

[13] Bernik, I. and Prislan, K. (2010). *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. Acquired on 1. 3. 2011 at http://www.fvv.uni-mb.si/DV2010/zbornik.html.

[14] Simt (2009). *Upravljanje, nadzor in varnost informacijskih sistemov.* Acquired 11. 10. 2011 on http://www.simt.si/informacijski_sistemi.html.

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

[16] Chicone, R. G. (2009). *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.

[17] Riedy, M. K., Beros, S. and Wen H. J. (2011). *Management Business Smart Phone Data*. Journal of Internet Law, 3-14.

[18] IDC. (2011). *IDC - Press Release.* Acquired on 10 .9. 2011 at http://www.idc.com/getdoc.jsp?containerId=prUS22871611.

[19] Juniper Networks. (2011). *Malicious Mobile Threats Report 2010/2011*. Acquired on 10. 9. 2011 at http://www.juniper.net/us/en/dm/interop/go.

[20] Hawick, K. A. and James, H. A. (2002). Middleware Issues for Mobile Business and Commerce. *WSEAS Int. Conf. on E-Activities: Conference Proceedings.* Stevens Point, Wisconsin: WSEAS.

[21] Leavitt, N (2011). *Mobile Security: Finally a Serious Problem?* Largo: University of Maryland. Acquired on 7. 9. 2011 at http://www.computer.org/portal/web/computingnow.

[22] Lookout. (2010). *Zlonamerna koda nad zasebnost uporabnikov mobilnikov Android*. Racunalniske-novice.com. Acquired on 7. 9. 2011 at http://www.racunalniske-novice.com/novice/mobilna-telefonija/google/zlonamerna-koda-nad-zasebnost-uporabnikov-mobilnikov-android.html.

[23] Flores, M. (2011). *What Your Cell Phone Data Reveals About You and Your Life*. Acquired on 7. 9. 2011 at http://www.intomobile.com/2011/04/25/your-cell-phone-data-reveals-you-and-your-life.

[24] Kučić, L. J. (12. 7. 2011). *Uporabniki hočejo imeti pravico do elektronske svobode*. Delo.si. Acquired on 12. 9. 2011 at http://www.delo.si/druzba/infoteh/uporabniki-hocejo-imeti-pravico-do-elektronske-pozabe.html

[25] Allen, M. (2006). Mobile Security. *The Journal of International Security,* 16(6), 25-27.

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

[27] Mathias, C. (2011). *Mobile Security Threats.* Acquired 20. 10. 2011 at http://searchmobilecomputing.techtarget.com/tip/Mobile-security-threats.

[28] Mayer Milligan, P. (2007). Business Risk and Security Assessement for Mobile Device. *8th WSEAS Int. Conf on Mathematics and Computers in Business and Economics: Conference Proceedings (pp 189-193)*. Stevens Point, Wisconsin: WSEAS.

[29] Scarfone, K. in Mell, P. (2007). *Guide To Intrusion Detection and Prevention System*. Acquired 4. 3. 2011 at http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

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

[31] Endait, S. (2010). *Mobile Security – The Time is Now*. Acquired 5. 3. 2011 at http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security.

[32] Mottishaw, P. (2010). *Policy Management Will Be Critical to Mobile Operators as Data Traffic Grows*. Acquired 6. 3. 2011 at 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.

[33] Arbaugh, W. (2003). *Wireless Security Is Different*. Acquired 5. 3. 2011 at svn.assembla.com/svn/odinIDS/Egio/artigos/.../Firewall/01220591_IMP.pdf.

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

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

[36] Lacuesta Gilaberte, R. (2004). Encryption tools for devices with limited resources. *4th WSEAS Int. Conf. on Applied Informatics and Communications: Conference Proceedings (pp. 299-304)*. Stevens Point, Wisconsin: WSEAS.

[37] Yan, Z. and Zhang, P. (2006). Enhancing Trust in Mobile Enterprise Networking. *5th WSEAS Int. Conf. On Applied Computer Science: Conference Proceedings (pp. 1057-1064).* Stevens Point, Wisconsin: WSEAS.

[38] Booz Allen Hamilton (2009). *Mobile Device Security*. Acquired 20. 10. 2011 at http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf