Mobile Policy in Enterprise Information System

Zuzana Šedivá
Katedra informačních technologií
Vysoká škola ekonomická Praha
sediva@vse.cz

Abstract: The article focused on views associated with the deployment of mobile enterprise policy in terms of ensuring security policy. The objective way to evaluate the management of mobile devices and applications and ensure their adequate security, including the positive and negative aspects associated with the deployment of mobile policy in the business. The paper is to evaluate the results of the survey to evaluate a current state of implementation of mobile policy in enterprises in the Czech Republic.

Key words: mobile technology, smart phone, tablet, enterprise information system, IT security, mobile application, mobile policy.

1. Introduction

The aim of any enterprise is to work effectively and provide their products or services on the market. Information technology can greatly contribute to the company goals and to support efficient processing of corporate agendas. With the rise of mobile technologies has opened the possibility of greater use of mobility in the treated activities. The possibility of sending messages from a remote location directly into the information system of the mobile phone via SMS or WAP were the first options to speed up communication and at the same time strengthening the availability and extend the functionality of the system. With the involvement of smart phones and tablets have further strengthened the possibility of using these mobile devices in applications of enterprise information systems. With the deployment of new mobile technologies and applications in the enterprise need to be addressed method of management in ERP systems. The text of this article deals with the problems of mobile technology in business practice and identifies factors affecting their successful deployment in the enterprise.

At the beginning of this article, it should be noted basic definitions that will be applied here. The following text will be considered among mobile devices for mobile phones with the operating system (smart phones) and tablets. They will therefore considered PDA devices, special mobile terminals (RFID) and other mobile computers such as laptops or netbooks.
Similarly, it is necessary to specify the concept of mobile applications. Mobile applications are meant to applications that enterprises use for communication in trade or cooperation between business partners or between employees. Mobile phones and tablets are thus used for the mediation of mobile data transfer to/from the ERP system.

2. The Use of Mobile Applications in the Enterprise Information System

According to Michl [2012] mobile applications can be divided into native applications, hybrid applications, web applications and mobile web. **Native applications** are created for a specific mobile platform and hardware. The main advantages of native applications include speed, reliability and the ability to use the hardware capabilities of the handset. For native applications also benefit from its distribution, which is often carried out using various supermarkets mobile platforms including the App Store and Google Play. The rate of development of these applications, respectively adoption of a new set of tools, or hire a programmer may be time, organizationally and financially challenging.

A **hybrid application** is a compromise between Web application and native application. As a rule, they can take advantage of the hardware capabilities of the handset and are usable on multiple mobile platforms. These applications must be for the correct functioning of the increasingly connected online. This may be a disadvantage in terms of their operation. Promotion and distribution of hybrid applications is not as simple as native applications on its promotion often have to take care of the developer himself.

**Dedicated web application** is a mobile website that is adapted to the mobile OS or hardware configuration. For example, a Web application created specifically for touch phones or tablet.

**Mobile web** is a universal platform that can be used on all mobile platforms. It is a customization website browsers for small smartphones and tablets. Page content is tailored to the specific display resolution and its specifications. User friendliness is influenced by several parameters such as: connection speed, location, service, type of data plan, etc.

The use of mobile devices in the enterprise is usually the added value for the business. Using these technologies can be easily and quickly achieve business objectives, edit individual processes, or set of indicators to monitor results. According to Polák [2012] there is usually work to optimize the company's human resources, which set correctly mobile policy allows shortening time to prepare data for business, time for immediate updating of data from the merchant to the client, improving productivity at the expense of error, the possibility of control of the activities of individual employees, streamline operations for field workers and lower costs (eg. by reducing paper consumption), etc.

High performance mobile phones or tablets, larger display area allowing a larger display data content and decreasing prices of mobile phones and tablets and hence their greater availability to the end consumer - that are trendy, responded to suppliers of business information and applications come to market in the form of mobile
applications that the traditional form of complementary solutions functionalities of information systems.

Mobile applications are therefore used mainly in areas that support activities such as sales representatives in the negotiations in the field at the customer. They are now indispensable in applications supporting logistics and dispatching processes. A very noticeable trend in recent years is evident emphasis on the development of mobile analytical applications for decision-making activities of managers who need to monitor the current status of important data and indicators and outside the enterprise, such as during business trips.

Yet corporate activities that can be effectively and meaningfully in the process of mobile applications, is still very limited levels of mobile devices. Due to the use of mobile phones in enterprise applications, especially for data services is one of the major limiting factors of smaller display area. Diagonal screen is now moving around with equipment 4.7 " on a mobile phone and about twice the tablets. It is therefore a significantly smaller area than a conventional size of a standard 19 " screen of a personal computer or laptop. This implies the fact that the use of mobile applications is particularly suitable only where it can be efficiently and transparently organize data of a small area display screen. The more data or text is displayed in the application or process, the more the state of the application and the screen confusing and challenging for users, and thus less useful.

In terms of business objectives and requirements for data processing can be stated that the use of mobile business applications are mainly used:

- Where are not the large input text or tables of data that would be on the small screen cluttered and difficult to read,
- Due to the fact that mobile applications provide enterprise IS primarily transactional nature of tasks, the mobile application to perform without compromise to functionality by at least the same level of quality transaction processing master data in applications such as information system
- In places where it is necessary to ensure the functionality of location-independent (space) processing,
- In places where it is very adequate and reliable data connection. Mobile applications must also ensure the preservation of the transaction if the mobile device was temporarily off-line mode. The transaction is then sent to the back-end system at the moment is to re-establish a connection.

The use of mobile phones or tablets in ERP systems need to be addressed and the appropriate type of equipment. Claims on customers' mobile devices for personal use are different from the constraints of the device that is to be considered for use in business practice. In addition to the above-mentioned screen size, which should be sufficient for displaying text and graphics (eg, statistical graphs, data tables, time series, ...) are mainly security features of the mobile operating system with which the device operates.
Among the safety features required by mobile OS mobile phones or tablets in business practice should not miss features like:

- Data encryption on the device,
- Remote data encryption,
- Remote lock,
- Selective deletion of enterprise applications and data,
- Enforcement of rules for creating passwords,
- Complex passwords,
- Support for VPN,
- Promotion and management rules,
- Limit / block access to app stores.

Above mentioned functions are often used in personal use of mobile devices, but they play an important role in setting up and solving enterprise mobile policy.

3. Ways of Solving Mobile Policies on the Enterprise

Enterprise policy for the management of mobile devices can be oriented in two directions. Either the company will focus on mobile device management enterprise owned or used by private institutions that own the company employees themselves. Administration of mobile devices only in business ownership requiring costly investment in building mobile infrastructure, application development and management, but its great advantage is the visibility, management, updating and installing applications on managed devices, OS and applications, which are usually kept always in the same versions for all mobile devices. This corresponds to the simpler and ensuring the security policy. Control and monitoring of safety in this regard is clear. [Sluněčko, 2012] It is also important for the company to determine whether, to implement mobile policies across the board for the entire enterprise or just for certain employees, such as for landscaping or business employees. Not always is for all internal staff mobility policy justification.

Nowadays, however, make extensive use of policy BOYD (Bring Your Own Device) and BYOA (Bring Your Own Apps). Thus, the use of private facilities employees within the company, which also brings a great many risks. This eliminates the initial cost of mobile devices, but this approach entails many problems. IT department loses control over the administration, maintenance, installation, maintenance and control applications on individual devices and over who accesses the corporate network and what mobile device. When you use private phones is usually a problem to keep all versions of OS and application of employees that are generally in all other or in other versions and not all OS or versions support all types of applications needed. [Sluněčko, 2012] Strong may also be disruption and security policy firm that has an overview of all the devices entering the corporate network. Therefore, the costs of mismanaged governance BOYD policy in this solution may be higher than in providing mobile policies on their own.
Figure 1 represents the most frequently mentioned disadvantages and risks of BYOD policies resulting from a survey conducted by Symantec in 2012. When using these types of policies is often a decrease in employee productivity, which usually has limited access to a mobile phone, and so often not fully work activities. Others already mentioned facts are direct financial costs and the third most important consequence is the frequent loss of corporate data.

Management and access to mobile enterprise applications within the company can be solved gradually by the application level (Figure 2).
According to SAPSA [2012] mobile application management can be divided by 5 levels. The first three levels of mobile applications are common to all businesses and generally to all employees in the company. When introducing mobile policy is in the first category first to synchronize communications with mobile phone, including email, calendar, contacts, etc. On the second level there is a synchronization and access settings for internal and external data. In the third level applications can be set to different employees access to corporate applications (functions), the date, etc. according to their user rights. Category 4 and 5 may be in companies vary greatly and can set specifically tailored to the requirements and business management. The fourth level of application management is concerned with setting verification of applications that every business has different. In Category 5 is given a set application access for transferring data between a mobile phone and the information system of the company. It is important to mention that all employees may not use the application at all 5 levels. Access to different levels is provided by staff role in the company and its rights and obligations. Managers often access to all levels of application, while employees working only operational level can be attributed to only the first two levels, etc.

4. Rules for Secure Mobile Device Management in the Enterprise

Mobile phones and tablets have become in many enterprise systems an integral part of it. Mobiles should be taken as one of the other types of terminal equipment in the internal and external corporate communications and become the next target of security attacks. This fact should respond primarily security policy rules. According Pužmanová [2005] and Computerworld [2012] should be set strict rules for the use of mobile devices in the enterprise. Employees often underestimate the threats and dangers that may arise, and do not comply with security rules and do not pay them enough attention. Therefore, the rules must be checked continuously. A related
staff training in this area. Again the fact that more and more employees are educated, the more aware of the potential hazards and thus accountable is their approach to mobile security policy.

Regardless of how mobile solutions policy should make an inventory of all mobile equipment, whether owned business or personal property of employees. To address the operation of mobile applications in the enterprise need to create a detailed list of equipment is technically and in terms of operating system platforms. [Northcutt, 2005]. On this overview can establish a list of applications for business operations on these mobile devices operate.

Mobile policy must clearly define what mobile applications and from what sources these applications can be downloaded. It is also necessary to define the rules under which they are buying the new version. You should only use reliable, proven source. To ensure safety, it is advisable to run their own app store, so to minimize the risks arising from the installation and use of unverified sources. Each application is yet to be checked prior to installation to reduce the risk of malware.

Large quantities and types of mobile devices that operate on different platforms, operating systems, brings many management problems. This complex situation helps to solve the registration device management server mobile devices. Enables configuration profiles defined IT department, as it is common in the operation of PCs and laptops in the enterprise information system. The configuration profile can then monitor and control the mobile communication device including management of user rights application level encryption of data, etc.

The mobile policy should set active protection on mobile devices. One form of solution is a security encryption that can protect your mobile device in case of loss or theft of equipment. In case of mobile devices in the enterprise IS, may result in the loss of sensitive data stored on the SIM card or mobile phone to get through to the corporate email or data accessible mobile applications. Therefore, users should encrypt your data and protect with a strong password. In the case of mobile OS can use their special features that allow you to control mobile device remotely (eg via SMS), mobile device remotely lock or remotely delete data or applications.

A study by Cisco IBSG of 2012 [Fuk, 2012] used every other employee in the Czech Republic his private mobile devices that uses access to the company's corporate network. 82 % of employees use remote connection primarily to access the e-mail client, 48 % of employees use a mobile connection to the calendar and 45 % for use for access to corporate applications. These numbers survey carried out in the Czech Republic confirmed by the results of the aforementioned survey conducted by Symantec in 2012. Almost a third of people (31 %), according to survey does not have secure access to the corporate network. Only two thirds of companies (58 %) of companies have set rules limiting the use of private facilities in an enterprise environment. An interesting and at the same time alarming is the fact that 12% of workers surveyed are unaware that some rules for mobile management in business there. The study also shows that private mobile devices will be in companies grow and BOYD policy becomes a common form of mobile device management in the enterprise. Businesses will have to respond to this fact and adjust their mobile device management and security policy of the company.
5. The Solution Mobile Policy In Enterprises In The Czech Republic

In the following text some interesting results of the survey carried out at the Department of Information Technology University in Prague, which took place in the first half of 2013. It was attended by 79 companies operating in the Czech Republic. According to company size in the survey involved 34 small firms (under 50 employees), 12 medium-sized companies (50-250 employees), 7 large companies (over 250 employees) and 26 corporations (over 1000 employees). The survey focused on the use of mobile technologies in the Czech enterprises and the use of mobile applications and solutions to mobile policy in enterprises. Full survey results are given in [Filipčík, 2013], in this text we present only the results associated with resolving security mobile policy.

The survey shows that mobile-established policy, respectively. rules on the use of mobile technology in enterprises in the Czech Republic is not supported too. Only 32% of the surveyed companies said they have mobile policy put in place and only 1% of its introduction into the business thinking. Mobile policy has established more than 48% of the surveyed enterprises. 18% of respondents did not know whether their company mobile policy in place.

The surveyed companies that had not yet mobile policy, the high proportion of small firms (79%), and 11% are medium-sized companies, large companies 5% and 8% of the corporation. The problem may be the size of the company, where a very small number of employees is unnecessary to introduce mobile policy, or some small businesses do not have sufficient financial costs, so that they can manage mobile and politics allow.

As further from the survey analyzed the main reason for companies to introduce mobile policy (48%), the mobile redundancy policy to the subject of business company (55%). Another important reason is the lack of experience with the introduction of mobile policy (26%). The financial cost of implementing mobile policy and fro mobile devices such firms as key not to deploy mobile policy of only 8%.

The companies, which in turn establish enterprise policy (32%) are the most represented corporate companies that are in the area represented by a majority of 52%, are also represented 20% of medium-sized companies, 16% of small company and 12% of large companies. The reason for the high representation of corporations may be a good market segmentation view of competition and consumer market, high turnover and profits that allow to implement policy and manage mobile and various mobile technologies and devices. [Filipčík, 2013]

In terms of carrier selection 66.67% of the firms prefer to select the same operator for all employees in the company and the remaining 33.33% of companies stated that solve mobile device management company employees by type of operator. The most frequently used operator in the surveyed companies, Telefonica O2 (44.83%). 37.93% of employees in companies using the services of T-Mobile and the rest of the workers surveyed companies use the services of Vodafone. The operator U-fon was not represented in any of the companies surveyed.

In terms of mobile device management outweighs the companies surveyed support only company phones and tablets (47%). Another 47% of firms allows the use of a combination of private and corporate mobile devices. Only 6% of companies with
established mobile policy that only use private mobile devices. The above figures confirm the fact that these companies will prefer a clear and unified management of mobile devices and applications in the enterprise system. IT departments can manage mobile devices with a single operating system with more secure access to resources and mobile applications, and to manage their versions.

An important aspect is also the possibility of remote access and the ability to synchronize data. In the survey 61% of companies that allow their employees remote access to corporate information system and remote data synchronization. [Filipčík, 2013] The remaining 39% of the companies does not remote access to the information system or data synchronization, see Figure 3.

![Remote Data Synchronization](image)

**Figure 3 Way remote synchronization of data in company. Zdroj: [Filipčík, 2013]**

From Figure 3 it is clear that the synchronization of data is usually performed by standard Internet connection by the mobile operator tariff (39%). It is also an important factor for selecting a mobile operator whose services must meet the requirements of business both operationally and financially. The second most frequently selected method in the surveyed enterprises synchronization is based on the wifi connection (37%). Currently also more growing use of cloud computing in this area, which is used in 12% of firms. Only 10% of companies solve sync via data cable.

In terms of the type of policy they prefer mobile multiplatform company policy (62.07%) than single-platform mobile policy represented in 37.93% of companies surveyed. In mobile OS platforms supported by most businesses, as this survey shows, the Android operating system (28%), followed close behind BlackBerry (24%) and iPhone (22%).

6. Conclusion

This article outlines the issues to deal with aspects of the management of mobile devices in the enterprise. They were the basic terms and context of the subject matter.
It was mentioned the positives and negatives of mobile solutions policy. In the final part of the article were the results of the survey on the level of policy in mobile solutions companies in the Czech republic.

Acknowledgement: This paper is prepared as one of the outputs of the research project No. P403/11/1899 Sustainability support of SMEs based on ICT innovations funded by the Grant Agency of Czech Republic.

References
Lippert, T. Deset pravidel pro ochranu mobilních zařízení. IT SYSTEMS. Brno. 12/2012. str. 34-35. ISSN 1802-002X
Macryllos, G. 2012. Tipy pro bezpečnou správu mobilů. IDG Czech Republic.. Computerworld 20/2012, str. 31. ISSN 1210-9924

JEL Classification: M11, M15