INFORMATION AND COMMUNICATIONS TECHNOLOGIES

MOBILE DEVICE MANAGEMENT AS A COMPONENT OF CORPORATE IT INFRASTRUCTURE

Assist. Prof. Iskren Liubomilov Tairov, PhD

Abstract: Digital economy and the rapidly growing use of the Internet have rendered it impossible for a corporate IT infrastructure to perform successfully unless adopting the necessary techniques, technology and procedures for controlling access to resources. Mobile devices have become tremendously popular and they are an indispensable part of people's everyday life, as well as a preferred option for accessing corporate IT infrastructure resources. Therefore, organisations need to design and implement efficient management solutions, based on in-depth analyses and in line with the specific properties of mobile devices.

This research paper describes in detail corporate IT infrastructure and mobile devices as components of that infrastructure, reviews their use in business environment and presents appropriate tools for exercising control.

Key words: corporate IT infrastructure; mobile devices; management.

JEL: L63, L86, M21.

There have been dramatic developments in corporate IT infrastructure over the last years. Wireless connectivity, a greater number of laptops and personal mobile devices that are connected to corporate networks are increasingly used.

The computing power of modern mobile devices is amazing; they are manufactured in large quantities and their popularity is growing rapidly among all categories of users, thus rendering them increasingly important. Although mobile devices are mainly used for entertainment, their use has also become a key factor for accomplishing the business objectives of enterprises, for improving the standard of living and for doing routine everyday activities. According to data provided by the National Statistical Institute (NSI, 2018), in 2018 in Bulgaria, more than 55% of people aged 16-76 used a mobile phone or a smartphone to access the Internet outside their home or at their work place. In comparison, 67% of global population (that is, 4.68 billion people) are predicted to own and use a mobile phone or a smartphone by the end of 2019 (Statista, 2019).

A lot of analysists and specialists (CIO, 2011) share the opinion that the mass use of mobile devices in a business context poses new challenges to the management of corporate IT infrastructure.

The main **objective** of this paper is to describe the structure of corporate IT infrastructure and to emphasise the need of control over mobile devices as an essential component of that infrastructure.

To accomplish this, the following **tasks** need to be fulfilled:

- Identify the components of corporate IT infrastructure;
- Focus on mobile devices;
- Study the use of mobile devices;
- Review efficient control techniques.

1. Structure and Properties of Corporate IT Infrastructure

The term corporate IT infrastructure (CII) is used to refer to the set of all physical devices and system software, which comprise the computer network of an enterprise and ensure the provision of general system (network) services. It is also considered to be the enabling technical foundation of the overall system for managing internal corporate information. CII is a set of devices and equipment that support the operation of corporate management. It is therefore closely related to management performance and efficiency.

There are numerous scientific research papers that deal with IT infrastructure and the structure and components of corporate IT infrastructure in particular, most of them based on the **model** designed by McKay and Brockway (McKay, 1989), which is presented in Figure 1.

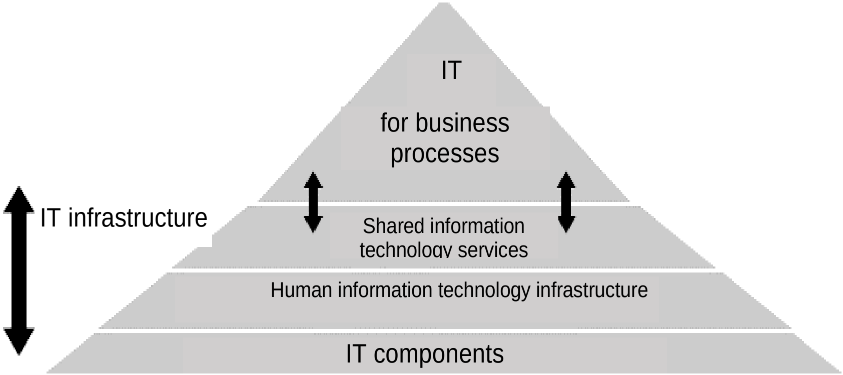

IT
for business processes
IT infrastructure
Shared information technology services
Human information technology infrastructure
IT components

Figure 1 Elements of IT infrastructure

The model defines Corporate IT Infrastructure (CII) as an essential element of any organisation since it is the enabling foundation for sharing information technology. The elements of Corporate IT Infrastructure are presented in a three-layer model:

- The bottom layer (layer 1) consists of 'IT components'; those include computers, printers, routers, database software and operating systems;
- The middle layer (layer 2) includes the knowledge, skills, standards and experience required for binding the IT components to the IT services referred to in layer 3;
- The top layer (layer 3) is called 'Shared IT services'; it includes services which are stable over time, for example, management of shared customer databases.

Over the years, other authors have added new elements to the model in their pursuit to determine and describe IT infrastructure. Our suggestion for updating the model of corporate IT infrastructure is in terms of adding the following components: cloud infrastructure, mobile devices and new concepts for working with them, such as the BYOx (Bring Your Own Anything) one (Trent, 2013).

Corporate IT infrastructure has evolved through a series of stages in result of research and is still evolving. Different authors share similar approaches to the contents and components of CII and tend to add new elements to CII contents to account for new technological advancements over the years.

In synthesis, the structure and components of CII may be presented as:

- Computers and IT equipment;
- Communication networks and technology;
- Computer networks;
- Software;
  - Operating systems;
  - General purpose software;
  - Business software;
- IT specialists;
- Web technologies;
- Virtual and cloud solutions and technologies.

The focus of this research will be on the control exercised over mobile devices and applications.

2. Some Research on the Use of Mobile Devices

Mobile devices, the up-to-date approach to using IT services and the Bring Your Own Device (BYOD) concept (IBM, 2017) about using personal devices at work are only some of the factors which have a dramatic impact on corporate control systems. The risk of losing enterprise data or having it compromised poses numerous challenges to IT managemers and specialists. Hence, we could summarise the following characteristics of mobile device use:

- **Personal devices are becoming increasingly popular**

The BYOD concept was based on the assumption that smartphones and laptops are the two types of personal devices that employees use to work. Analysts report a major change in this respect, since a significant number of the laptops, which are used for work, are owned by business associates. According to experts from Forrester (Growder, 2019), IT departments have become more flexible and more tolerant towards the BYOD culture, and in result, an increasing number of employee-owned laptops are used at work. Personal devices are becoming a standard practice and enterprises need to respond to that trend adequately. Analysts predict that the increasingly growing demand for mobiles access to companies will result in a number of serious changes, such as:

- Investment in broadening remote access to contents and data that are usually stored behind corporate firewalls;
- Reviewing the architecture of enterprise apps and activating as much 'Software as a Service' (SaaS) and platform-independent solutions as possible;
- Cutting costs on fixed communication services and expending exempted funds on wireless equipment and services.

In our opinion, this will make the issue of exercising control over those devices even more relevant, since threats to corporate data security may grow dramatically.

- **Mobile on-demand virtualisation is becoming a major trend in mobile device management** (Jaramillo, 2014)

In order to comply with corporate policies on personal devices, a number of enterprises embracing the BYOD concept employ mobile device management technologies that are often perceived as a harsh and cumbersome approach to ensuring data security. Therefore, alternative methods for separating personal from enterprise data on employee-owned devices are developed, such as mobile Virtualized Desktop Infrastructure (VDI), containers, app wrappers and device virtualization tools. The employment of those methods, however, tends to have a negative impact on user experience and poses a number of threats to corporate IT infrastructure and enterprise data in particular. The positive effect of mobile virtualization is expected to be felt in near future, though. We believe that new technologies will be developed to enrich workflow apps management policies, thus reducing to a minimum the risks for enterprises.

In our opinion, those technologies will guarantee the quality of user experience and will contribute to mobilizing corporate resources. In the best-case scenario, new technologies will help resolve any issues related to the BYOD practice.

- **The popularity of enterprise HTML5 applications is growing** (Schrock, 2014)

According to many specialists, the rate at which HTML5 apps are entering the corporate sector is faster than that of apps developed in a special programming language, such as Objective C for iOS or Java for Android. This observation is confirmed by the ambition of the US Federal Communications Commission (FCC) to broaden the wireless spectrum of frequencies in order to reduce connectivity costs and ensure higher reliability. This contributes to the popularity of HTML5 apps, which have a number of advantages, two of them being that they are easier and cheaper to develop and support. This could result in enterprises choosing to use cloud infrastructure for their apps, which will increase the costs they incur on cloud apps and infrastructures. A browser will thus become the main tool for managing devices and it will be possible to develop technologies that make safe the use of a browser via a mobile device.

- **Personalised mobile services require increased awareness about data security**

The use of mobile devices has led to the establishment of new, potentially efficient, business models that are based on current user preferences and former user activities. Mobile devices are designed so as to allow the integration of data about a specific person and their online presence, which could result in major data security issues. A lot of users and enterprises have stated their worries due to the lack of clearly formulated mechanisms for managing mobile user data. The accumulation of large volumes of mobile data is therefore expected to face serious resistance. Many experts predict that the adoption of stricter regulations about the interaction of user data in the mobile ecosystem is not very likely. Within this context, we expect users to become increasingly careful about the security of mobile data.

3. Mobile Device Management Solutions and Approaches

In order to efficiently manage and control mobile devices, it is advisable that they be included in the scope of approved standards of access management. In addition, organizations need to focus on their mobile device management awareness programs and on issues related to the BYOx (Bring Your Own Anything) concept.

An efficient solution to mobile device control is Enterprise Mobility Management (EMM) (Lirex). This is a set of technologies, processes and policies that ensure centralized control over the use of mobile devices, which are owned by an enterprise and its employees. Enterprise mobility management technologies configure devices and applications for enterprise deployment, use and upgrades. They also ensure mechanisms for replacing or removing the access of devices to an enterprise. EMM solutions are designed based on the Bring-your-own-device trend (BYOD), according to which, instead of restricting mobile devices to the workplace, many organisations choose to implement EMM solutions, thus allowing users flexibility, while at the same time retaining full IT control.

EMM technologies help track and keep inventory of devices, their settings and usage, test their compliance with corporate policies and manage access devices.

EMM solutions work by:

- Adding control to encrypt data;
- Data access rights;
- Shared devices;
- Packaging applications and containers;
- ‘Locking’ devices.

Those options enable IT departments to identify and track problems related to mobile devices that access the network through inventory, analysis and remote management tools. EMM solutions have been designed for VM ware, Symantec, Checkpoint, Microsoft and Sophos.

Practice has proved the deployment of EMM of solutions to be more efficient when combined with mobile application management.

Mobile application management (MAM) refers to the software and the services that provide and control access for both employee- and enterprise-owned smartphones and tablets to mobile applications in a business context. Those applications can be commercially available to the public or internally developed within the company. Mobile application management is different from mobile content management (MCM)

(Contentful) and mobile device management (MDM) (Itforce, 2013), since its focus is on the applications used by devices, rather than on the management of devices themselves or of their content. MAM gives systems administrators less control over devices, but more control over their applications, whereas MDM may incorporate both types of management. The MAM system enables enterprises to control the mobile applications their employees use when those applications are updated or removed from end-user devices. In general, MAM will incorporate an enterprise app store similar to a typical app store on a mobile device for the purposes of supplying updates and adding or removing applications. It also allows companies to track how an application performs and how it is used. In addition, the system administrator can remotely remove or wipe any data from these mobile applications.

Major features of MAM systems include delivery, updating, wrapping, version and configuration management, performance monitoring, tracking and reporting, event management, usage analytics, user authentication, push services and crash log reports. Since mobile devices are increasingly used in business, the ability to employ these features across a range of devices and operating systems is becoming a much more pressing issue, which could be resolved by MAM.

Forrester Research experts published a report listing 10 points that require special attention in terms of mobile device management systems (CIO, 2011):

- Different employees require different kinds of mobile support from IT;
- IT should query users to understand staff needs and preferences;
- Create a clear common policy for enterprise- and employee-owned mobile devices;
- Know the limitations of mobile platforms and prioritise support for those that need it most;
- There are no one-size-fits-all platforms MDM solutions;
- Encourage IT suppliers to offer app stores that suit the enterprise;
- Employ virtualization for access to Window-apps on non-Window devices;

- Support employee-owned devices but set strict usage guidelines;
- Make it clear to users which mobile services are approved;
- Consider reimbursement for the service costs of employee-owned device as an incentive.

Some of the mechanisms for preventing the materialization of mobile devices risks require the observation of certain rules, such as:

- To download apps from official sources only;
- Not to click on any suspicious links;
- To avoid using public Wi-Fi and always connect to a VPN server;
- To avoid using major apps, for example, mobile banking apps, if not connecting to a secured home or office network;
- Not to enable the ‘Unknown sources’ and ‘Developer mode’ options in the settings of the mobile device;
- To specify the types of devices that can be used in the organisation (i.e. devices provided by the enterprise or personal devices which employees have special permission to use, for example, BlackBerry or iPhone);
- To specify the type of services accessible via mobile devices by accounting for existing IT architecture;
- To determine the mode in which employees will use mobile devices by accounting for the established corporate culture and human factors;
- To integrate all enterprise devices into a single application for managing data assets;
- To describe the type of authentication and encrypting that are inherent to the mobile devices;
- To identify the tasks which employees can use mobile devices for and the types of apps they are allowed to use;
- Clarify requirements on data storage and transmission.

In summary, mobile devices have posed some major challenges to efficient control and management over the last years. Enterprises have been searching for solutions to different issues related to the use of mobile computer devices, which are employer- or employee-owned.

Resolving those problems requires the establishment of certain rules and patterns of behavior, which must be observed within organisations. The accomplishment of this objective will take time and effort not only in terms of technology, but also in terms of adequate social development. It is essential to design and implement a prevention policy that accounts for potential problems, while society needs to be constantly informed about the occurrence of any new issues since they are bound to accompany further advancements in technology. The ability of organisations to effectively deal with problems related to mobile devices will ensure that they have major competitive advantages, as well as a high level of employee comfort, satisfaction and security.

* * *

Mobile device management has evolved tremendously, enabling even strictly regulated industries to allow their employees to use devices which have been approved by the company for communication and business activities, for accessing social media and networks, playing games, etc. The benefits from the deployment and management of mobile devices and apps, alongside the fast rate of ‘employee mobilisation’ and the impact it is expected to produce on the ability of organisations to provide corporate data on a growing variety of employee-owned mobile devices naturally provokes management’s interest in developing further the BYOD concept and implementing mobile application management (MAM), enterprise mobility management (EMM) and internal control rules.

References

CIO. (15.12.2011). Upravlenie na mobilnite ustroystva – 10 uroka ot Forrester. Retrieved on 20.03.2019 from CIO.bg: http://cio.bg/4299_upravlenie_na_mobilnite_ustrojstva__10_uroka_ot_forrester/

Contentful. (n.d.). Mobile CMS: a comprehensive overview. Retrieved on 21.02.2019 from https://www.contentful.com/r/knowledgebase/mobile-cms/

Growder, J. H. (18.01.2019). The Future Of Enterprise Computing. Retrieved on 18.03.2019 from https://www.forrester.com/report/The+Future+Of+Enterprise+Computing/-/E-RES142617

IBM. (2017). Bring your own device. Retrieved on 19.03.2019 from https://www.ibm.com/security/mobile/maas360/bring-your-own-device

Itforce. (04.09.2013). MOBILE DEVICE MANAGEMENT - AN OVERVIEW. Retrieved on 16.03.2019 from https://www.itforce.ie/blog/mobile-device-management-an-overview

Jaramillo, D. F. (2014). *Virtualization Techniques for Mobile Systems.* Springer.

Lirex. (n.d.). EMM. Retrieved on 06.03.2019 from https://lirex.bg/en/home-2/our-portfolio/cybersecurity-2/information-systems-protection/mobile-device-management-mdm/

McKay, D. B. (1989). *Building IT infrastructure if the 1990s Stage by stage.* Nolan Norton & Company.

Mobile Application Management. (n.d.). Retrieved on 16.02.2019 from https://www.kony.com/resources/glossary/mobile-application-management/

NSI. (17.12.2018). *Izpolzvane na mobilni ustroystva ot litsata za dostap do internet* [in English: Individuals using mobile devices to access the

Internet]. Retrieved on 21.06.2019 from Natsionalen Statisticheski Institut: http://www.nsi.bg/en/content/6107/individuals-using-mobile-devices-access-internet

Schrock, A. (28.08.2014). HTML5 and openness in mobile platforms. *Continium, 28*, pp. 820-834.

Statista. (2019). *Number of mobile phone users worldwide from 2015 to 2020 (in billions)*. Retrieved on 21.06.2019 from statusta.com: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

Trent, R. (11.06.2013). BYOx: Bring Your Own Anything Announced at TechEd 2013. Retrieved on 15.03.2019 from https://www.itprotoday.com/compute-engines/byox-bring-your-own-anything-announced-teched-2013

BUSINESS management

D. A. Tsenov Academy
of Economics, Svishtov

Year XXIX * Book 3, 2019

CONTENTS

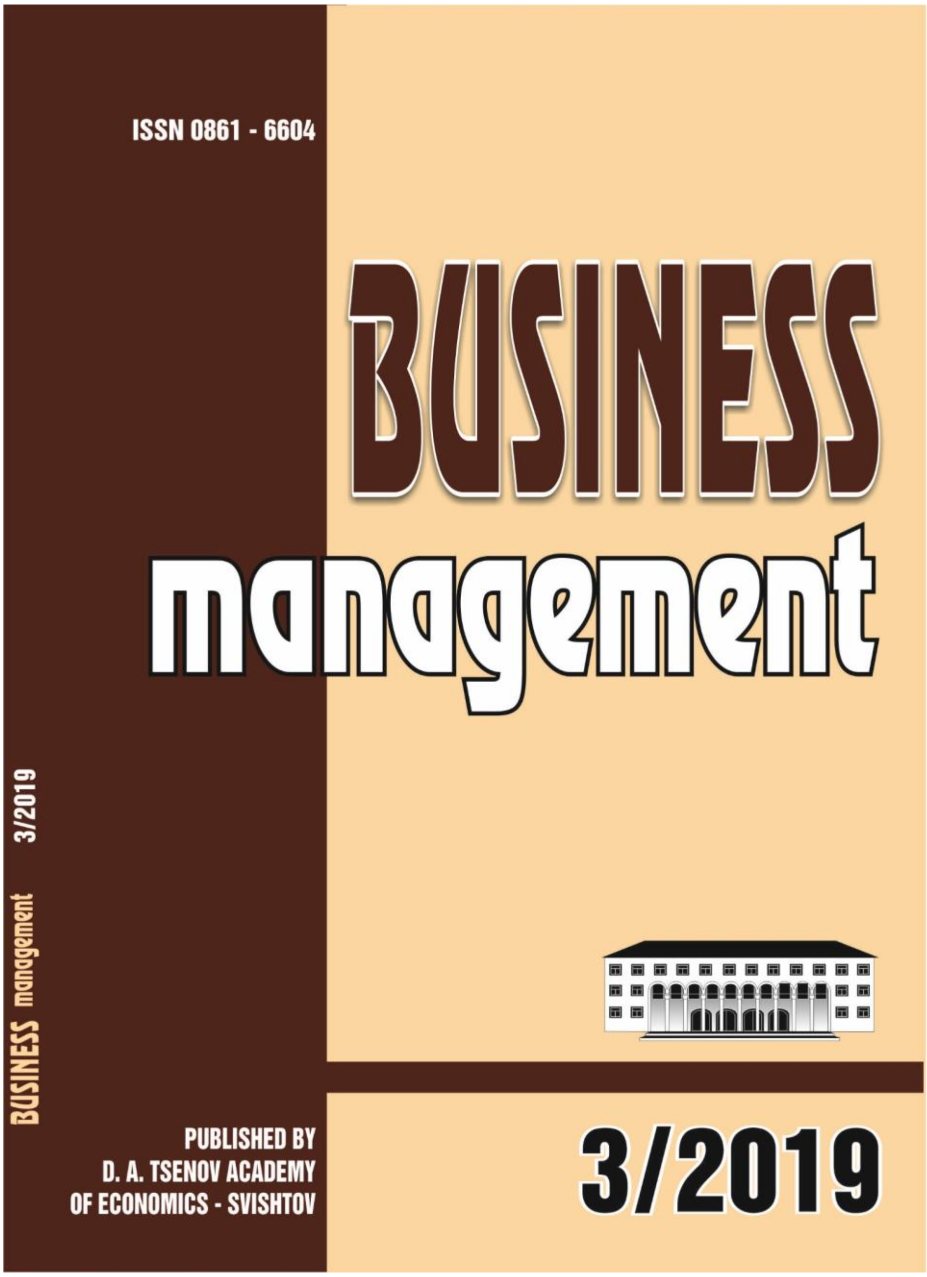
MANAGEMENT practice

INFORMATION AND COMMUNICATIONS technologies

Proofreader – Anka Taneva
English translation – senior lecturer Zvetana Shenkova, senior lecturer Daniela Stoilova, senior lecturer Ivanka Borisova
Russian translation - senior lecturer Irina Ivanova
Technical secretary – Assist. Prof. Zhivka Tananeeva

In 2019, the printing of the journal will be funded with a grand from the Scientific Research Fund, Contract KP-06-NP/36 by the competition Bulgarian Scientific Periodicals - 2018.

Submitted for publishinq on 09.09.2019, published on 16.09.2019,
format 70x100/16, total print 100



ISSN 0861 - 6604

BUSINESS management

BUSINESS management 3/2019

PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

3/2019

TO THE READERS AND AUTHORS OF "BUSINESS MANAGEMENT"

The journal of "Business Management" publishes research articles, methodological articles and studies, review articles, book reviews, commentaries and good practices reports.

1. Volume:

- Articles: between 12 – 20 pages;
- Other publications (review articles; book reviews, etc.): between 5 – 10 pages.

2. Submission of materials:

- On paper and electronically at one of the following e-mail addresses: bm@uni-svishtov.bg or zh.tananeeva@uni-svishtov.bg

3. Technical requirements (the article template is can be downloaded from the webpage of the journal):

- Format – Word for Windows 2003 (at least);
- Font – Times New Roman, size 14 pt, line spacing 1,5 lines;
- Page size – A4, 29–31 lines and 60–65 characters per line;
- Line spacing 1,5 lines (at least 22 pt);
- Margins – Top – 2.54 cm; Bottom – 2.54 cm; Left – 3.17 cm; Right – 3.17 cm;
- Page numbers – bottom right;
- Footnotes – size 10 pt;

4. Layout:

- Title of article title; name, scientific degree and scientific title of author – font: Times New Roman, 14 pt, capital letters, Bold – centered;
- Employer and address of place of employment; contact telephone(s) and e-mail – Times new Roman, 14 pt, capital letters, Bold – centered.
- Abstract – up to 30 lines; Key words – from three to five;
- **JEL** classification code for papers in Economics (http://ideas.repec.org/j/index.html);
- Introduction – it should be from half a page to a page long. It should state the main ideas and/or objectives of the study and justify the relevance of the discussed issue.
- The main body of the paper – it should contain discussion questions, an outline of the study and research findings/main conclusions; bibliographical citation and additional notes, explanations and comments written in the footnotes.
- Conclusion – it should provide a summary of the main research points supported by sufficient arguments.
- References – authors should list first references written in Cyrillic alphabet, then references written in Latin alphabet.
- Graphs and figures – Word 2003 or Power Point; the tables, graphs and figures must be embedded in the text (to facilitate language correction and English translation); Font for numbers and inside text – Times New Roman, 12 pt;
- Formulae must be created with Equation Editor;

5. Citation guidelines:

When citing sources, authors should observe the requirements of **APA Style**. More information can be found at: https://www.uni-svishtov.bg/default.asp?page=page&id=71#jan2017, or: http://owl.english.purdue.edu/owl/resource/560/01/

6. Contacts:

Editor in chief: tel.: (++359) 631-66-397
Co-editor in chief: tel.: (++359) 631-66-299
Proofreader: tel.: (++359) 631-66-335
E-mail: bm@uni-svishtov.bg; zh.tananeeva@uni-svishtov.bg;
Web: bm.uni-svishtov.bg
Address: "D. A. Tsenov" Academy of Economics, 2, Em. Chakarov Str., Svishtov, Bulgaria