TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Fakhri Ramazan 195958IVSB

IMPROVEMENT RECOMMENDATIONS FOR THE MOBILE DEVICE MANAGEMENT POLICY OF PUBLIC SECTOR ORGANIZATION EMPLOYEES IN AZERBAIJAN

Bachelor's thesis

Supervisor: Kaido Kikkas

Associate Professor,
IT College, School of
Information
Technologies, Tallinn
University of
Technology

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Fakhri Ramazan 195958IVSB

MOBIILSEADMETE HALDUSEESKIRJADE TÄIUSTUSSOOVITUSED ASERBAIDŽAANI AVALIKU SEKTORI ORGANISATSIOONIDE TÖÖTAJATELE

Bakalaureusetöö

Juhendaja: Kaido Kikkas

Associate Professor, IT College, School of Information Technologies, Tallinn University of Technology

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Fakhri Ramazan

24.04.2022

Abstract

Every day, governmental structures are implementing more modern and various types of cybersecurity solutions to achieve protection of main aspects: availability, confidentiality, and integrity to control massive amount of data of every person in the country. However, it also important to control the internal workflow of data of the employees. This thesis will mostly concentrate on the standard that will come most suitable for public sector usage and analyse the current situation in the organization, outline the benefits of using Mobile Device Management services and threats that may endanger facility without them. At the end theoretical solution, or concept of the Mobile Device Management solution that will include best suitable features from existing solutions and how it will impact the cybersecurity aspects in the organization.

This thesis is written in English and is 42 pages long, including 6 chapters, 5 figures and 1 table.

Annotatsioon

Valitsusstruktuurid rakendavad iga päev kaasaegsemaid ja erinevat tüüpi küberturvalisuse lahendusi, et saavutada põhiaspektide kaitse: kättesaadavus, konfidentsiaalsus ja terviklikkus, et kontrollida tohutul hulgal andmeid iga inimese kohta riigis. Siiski on oluline kontrollida ka töötajate sisemist andmete töövoogu. Antud lõputöö keskendub valdavalt avaliku sektori kasutusse sobivaima standardile ning analüüsib hetkeolukorda organisatsioonis, toob välja mobiilseadmete haldusteenuste kasutamise eelised ja ohud, mis võivad ilma nendeta organisatsiooni ohustada. Töö lõpuosas on esitatud teoreetiline lahendus ehk MDM-lahenduse kontseptsioon, mis sisaldab olemasolevatest lahendustest parimaid sobivaid omadusi ja kirjeldab mõju küberturvalisuse aspektidele organisatsioonis.

See lõputöö on kirjutatud inglise keeles ja on 42 lehekülge pikk, sisaldab 6 peatükki, 5 joonist ja 1 tabel.

List of abbreviations and terms

BYOD	Bring Your Own Device
COBO	Corporate Owned, Business Only
COD	Corporate Owned Device
CYOD	Choose Your Own Device
EMM	Enterprise mobility Management
GPS	Global Positioning System
IT	Information Technologies
Jailbreaking	Modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator.
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MITM	Man-in-the-middle
MSP	Managed Service Provider
OS	Operational System
OTA	Over-the-air
Rooting	Acquiring administrative rights privileges on a device
PC	Personal Computer
SaaS	Software-as-a-Service
SME	Subject Matter Expert
SMS	Short Message Service
SIEM	Security Information and Event Management
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
UWYT	Use What You are Told
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
Wipe	Render all data on drive unreadable

Contents

List of figures

List of tables

1 Introduction

Since the moment mobile devices entered our life, it is hard to imagine a simple day without them. Communicating with relatives, surfing on the Internet, listening to the music and so much more activities that may be done by using them. The comfortability of these devices is also an aspect that made them so popular in everyday usage, as well as in the work environment as well. However, where are the new technologies develop and grow, the more threats come from cybercriminals and it may pose great danger to the companies, where mostly every employee possesses a mobile device. Situation that is going to be described in this thesis is a direct example of an organization, with lots of devices with no proper cybersecurity and management supervision.

They may possibly use their mobile devices (laptops or smartphones) for work purposes and these devices may have leftovers or direct access to sensitive data, for example access to the governmental personal e-office of a notary or company internal mail, thus endangering both employee, company and citizens' data he may be working with.

This problem was encountered during the internship period in the governmental facility in Baku, Azerbaijan. Like many organisations, this facility also has Active Directory system based on Windows Server, or simply as it may call for simplicity in our case, a Domain system which is, in basic, a private area of all the PCs inside the organization network which gives an opportunity to manage and control them as well. While static PCs are managed by Active Directory Domain system, mobile devices such as mobile phones and laptops (which are in active use for both corporate and personal usage at least by the notary by my own observations) are left without the necessary care, because such devices could not be operated by Active Directory system. This leaves an absolute requirement in the usage of MDM service, which is currently not used by the public sector and there are no visible actions of promoting such technologies now in our country. [1,2,3]

2 Methodology

This section will describe the methodology used by the author to conduct the research, how the data is collected, analysed, and used to create the final recommendations and solutions. Even though, the scope of this research is limited to certain organization, this thesis will include the qualitive and their review for both existing MDM utilities, cybersecurity threats and comparisons between the data. Moreover, additional information from this concrete organization will be collected from an interview of the employee staff and use collected information and their opinion on it, as a reference in certain points of the analysis.

In this research, author proposes the usage of MDM solution, to increase the cybersecurity management in the scope of mobile devices, whether smartphones or laptops and display how much it is important in terms of which threats may be evaded and how it can improve the ease of the control regarding corporate data which may be contained in employees' devices and in the same way, even make it more comfortable for employees to keep the needed corporate data without high risk.

Contribution in this thesis is based upon bringing the data from various sources: blogs, research papers and personal

The main goals of research are:

I. To analyse existence threats, which may endanger company or its employees due to lack device management. Analyse 4 main concepts of device management and if they are currently used in public sectors

II. Discover the consequences of certain threats, impact to the flow of work and endanger important documents or other data, analyse possible existing solutions

III. Based on the previous points, create an evidence-based proposition in the usage of one of the MDM standards and outline the functions that the MDM software should have for concrete MDM policy, that will help secure the mobile devices in governmental environment

3 Background information

This section will describe concepts, technologies, software and research problem in more details, describing the definitions of MDM concepts, abilities of MDM software and limitations that may be applied to the scope of this research.

3.1 Research problem

In this situation, where poor usage of MDM services seems to be an only problem itself, there are also many other issues that should be considered in the research as well. What are the reasons of such a poor MDM solutions promotion? What are the existing solutions, and will they fit in the need of the governmental organization in the scope of this research? What is the best MDM standard to fit in this concrete case? However, all these questions are more or less general, but in the context of governmental organization where possible solution will be implemented, it is needed to specify the facility to which proposal is being made, in order to understand for which purpose certain decisions are made. This thesis is written for the branch of Ministry of Justice of Azerbaijan, where citizens' sensitive data like notarized documents, litigations and many other personal confidential documents are being transferred between another governmental facilities. With this being said, it is becoming more obvious that MDM technologies should be used more widely to prevent possible data leak due to possible cybersecurity incidents.

3.2 Definition of MDM

At first, it is needed to understand and give the definition to the MDM standard itself. MDM abbreviation stands for Mobile Device Management. In fact, it is a software that gives an opportunity to manage the security and policies for mobile devices such as smartphones, laptops or tablets. Though being closely related to Enterprise Mobility Management (EMM) or in fact its core component as well as being a part of Unified endpoint Management (UEM). [7]

Even though the EMM and UEM is not the main scope of the research, it is needed to give a describe some details as well, in order to make comparisons and differentiate them from MDM. EMM is the set of technologies or services which purpose is to secure corporate data on employee mobile devices while UEM is an also set of technologies which is used to secure broad range of employee devices and operating systems from a single console. In the end, we have an UEM tool, which unite several EMM technologies which are Mobile Device Management (MDM) and Mobile Application Management (MAM). In short, by using MDM software we are implementing an UEM solution and EMM together. Mobile Application Management falls out of the scope in our case, because the thesis gives a solution that is mostly related to proposing MDM solution concretely. [10,11,12]

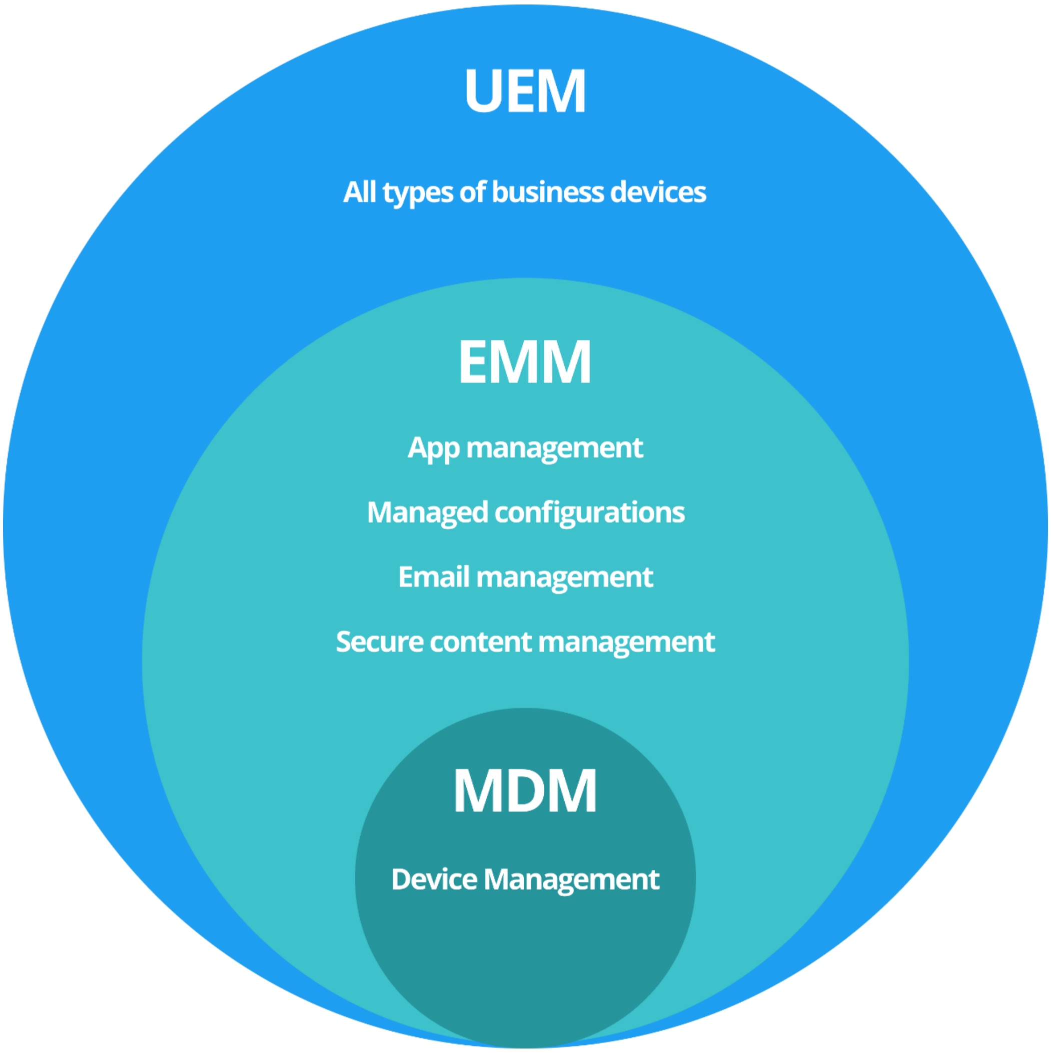


Figure 1. Visual representation of UEM, EMM and MDM. [19].

The software is relied on a server located in the data centre, whether physical or in the cloud. By using the MDM server's console, IT administrator is able to configure the policies or deploy the desired applications and push them to the MDM agent that is already installed on the device, where these policies or application changes are applied. [7,8]

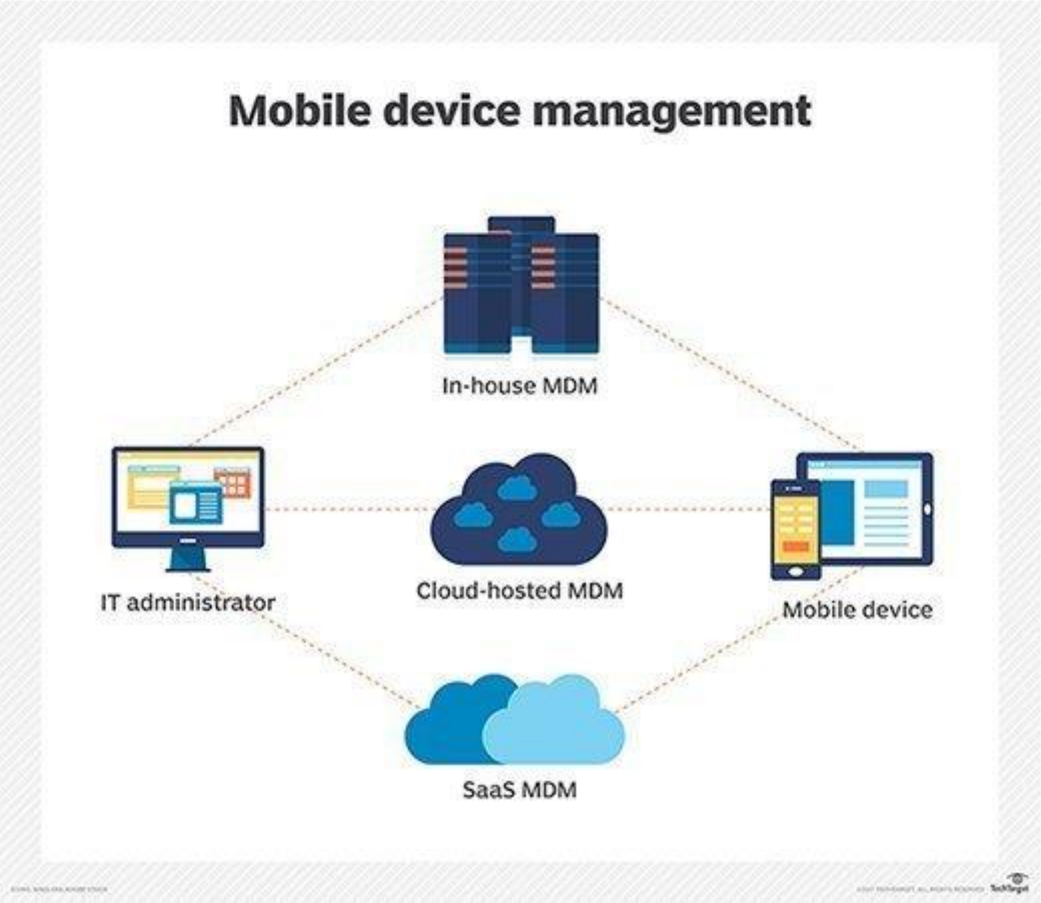


Figure 2. Representation of MDM software work principle. [7]

3.3 MDM software conceptions

Before making decisions of how and which software is going to be implemented, it is critical to understand which conception, or simply method of organization is suitable for the organizational needs. There are 4 types of MDM software usage scenario: Bring Your Own Device (BYOD), Choose Your Own Device (CYOD), Corporate Owned, Personally Enabled (COPE), and Company Owned/ Business only). CYOD and COBO types may be united in one group of standards known as UWYT (Use What You are Told)

To begin with the describing the models, it is important to start off from the BYOD (Bring your Own Device) policy, which is probably the most famous model in the business scope. Employees that follow a BYOD policy bring their own devices to work and utilize them for work-related tasks. The organization must then install an agent or program that allows them to control the device's security from a central management system after the device has been approved by the enterprise (such as an enterprise mobility management solution). Employees are solely responsible for keeping the device safe by preventing it from being lost or stolen while using a BYOD model. This includes staying away from public Wi-Fi networks and not installing harmful programs and apps on the smartphone. Because the device's security is ultimately in the hands of the user, it might be challenging for businesses to enforce security regulations.

As for the CYOD (Choose Your Own Device) policy, we have already prepared and pre-approved set of devices from which employee can choose the one they want. In this case, devices are configured beforehand with all the necessary security protocols and business applications used by the enterprise. In this scenario, employee may own the device with the funding help of enterprise or in some cases pay for it themselves. CYOD is frequently viewed as a compromise between BYOD and other policies, as it still allows employees to choose their own device. The organization can maintain device compatibility and apply security features before employees start using them because they pick which types of devices will be distributed. This can assist them in ensuring the security of the devices and the data they contain. Unfortunately, employees may be dissatisfied with the device options available. Employees may not be able to grow totally familiar with the gear they're provided, even if you authorize a wide range of devices.

The last, but not the least MDM solution policy is COPE (Corporate-Owned, Personally Enabled). The organization provides COPE devices to an individual. They are usually utilized for organizational goals, but an individual may also use them for personal reasons. It's worth noting that with COPE devices, privacy can be jeopardized because the organization can see everything that happens on the device. However, with the right containerization techniques that isolate work-related data from personal data, privacy concerns can be alleviated. A role that necessitates the usage of a smartphone is one illustration of this. Employees can carry a single phone instead of two during work hours using a COPE phone. As in the previous solutions, the phone will have pre-installed with work-related applications and other functions with the ability to perform calls, send text message, check personal inbox or even download applications for personal usage. Such devices might be a good settlement between strict COD (Corporate Owned Device) and more friendly BYOD (Bring Your own Device) policies. [14,15]

When mobile devices first became popular, businesses treated them like any other piece of gear. Companies with a COBO policy provide employees with a device to use, with the hardware being restricted to business use exclusively. Employees were frequently not given an option in terms of which gadget they would use. In today's high-connectivity, cloud-enabled environment, COBO is mostly obsolete because it's difficult for employees to access numerous sorts of content from the same device. COBO is more likely to be used by organizations with a complex set of compliance standards and the risk of data leakage. This method returns control to IT departments and limits smartphone use to work-related tasks. Companies can effectively limit their risk while yet allowing employees to move around. [16,17]

3.4 Possible limitations

In the scope of this concrete research, where the proposal is made for the governmental public organization, there may arouse the problems in which standard to use. During the analysis part, where thesis will outline beneficial functions of various existing third-party solutions in terms of MDM software, it is already decided that using one of them would not be the best solution, because it is possibly restricted by the security policy in public organizations and the thesis will stick to this limitation during the research. Furthermore, these institutions have various restrictions for using outsourced services, and cloud-based platforms are frequently not authorized. However, some of the restrictions might be mitigated. As an example, we can bring out the BYOD policy, which is not considered to be the best solution for public organization or large enterprises. [16]

“Allowing users to bring their own devices (BYOD) needn't be difficult, even for the government, according to the senior manager for the ACT Government's IT security, Peter Major”. [21]

This also doesn't mean that users have free rein of their devices, with other security constraints in place; for example, to prevent users from rooting or jailbreaking their phones.

"If you jailbreak ... or root the phone, we will serve a bullet. We will blow it away. We will not hesitate. We will blow your personal information away. We will do the whole lot. You will have a blank device; you will have to reload."[21]

This small example shows that even government sector is able to perform with BYOD policy, however, there are have to be special policy changes implemented for employees as well, because they have to know, what they are going to be dealing with during their work. If an employee decides to use a mobile device for work purposes and then creating a risk by installing some software which may endanger both device holder and corporate data, then the policy of MDM will take an action in this case and perform the necessary actions regarding the violations of the rules.

3.5 Common outline of benefits

Up to now it was given a short description of what is MDM and described in a simple way how does it control devices in the organization infrastructure. At this point, it would be beneficial to give some advanced features that usage of MDM software may bring for the organization and have an additional insight on why it is so popular today. Obviously, depending on the many popular solutions nowadays, every software developed till today, has its own advantages and disadvantages compared to each other, however, the overall purpose constantly remains the same.

1) ***Remote management:*** The main advantage of mobile device management is that it allows administrators to keep track of and control portable devices from anywhere. In some ways, MDM is designed to outsmart mobile devices. This agility reinforces healthy devices while bolstering those that may require assistance.

   Remote administration also improves network security by allowing administrators to disable specific users, even if they are not on-site. Updated regulations are also replicated across all networked devices, resulting in seamless protection and assistance. [22,23,24]

2) ***Support of fast-growing BYOD concept***: Traditional systems reject any unfamiliar devices that have not been previously identified, which is a major issue for firms with a large number of employees who bring two or three gadgets from home.

   Mobile device management recognizes that not all unfamiliar devices are dangers, and it assists MSPs in keeping track of them in order to strike a balance between security and flexibility. Companies don't have to pick between network security and employee liberties when using MDM. [22,23,24]

3) ***Up-to-date devices and applications:*** From time to time, everyone puts off software updates until the last possible moment. Employees that are overly complacent about upgrades, however, undermine the overall network's security. Hackers can acquire access to confidential information by exploiting the gaps created by insufficient updating or patching.

   Administrator can centrally control updates and deploy system changes to devices throughout the network with just a few clicks thanks to mobile device management. [22,23,24]

4) ***Enhancing the security of the network:*** In this sense, MDM best practices are important for enhancing network security. Most of this is due to the auto-update options and security features already mentioned. With MDM, MSPs can easily apply updates to hundreds of devices, encrypt sensitive corporate information, and create barriers between personal and corporate data.

   In addition, the remote ability to manage mobile devices makes it easy to adjust security remotely. The mobile device management platform can remotely retrieve, lock, and wipe data from devices to protect sensitive information in the event of loss or theft. [22,23,24]

5) ***Auto Backup for the devices:*** Data loss due to device crash or theft can cause serious business damage. You should back up regularly to avoid data loss. The backup server can be on-premises or in the cloud. it doesn't matter. It is important to back up your data. MDM software helps you schedule and protect your data during idle time. Thus, so data cannot be lost, and data can be restored to a new device and business can be continued. [22,23,24]

4 Qualitive analysis of MDM

This section will describe the statistical usage of MDM software, and popular existing solutions on the market, including the point what threats are endangering mobile security without using the MDM solution.

4.1 Market statistics of MDM usage

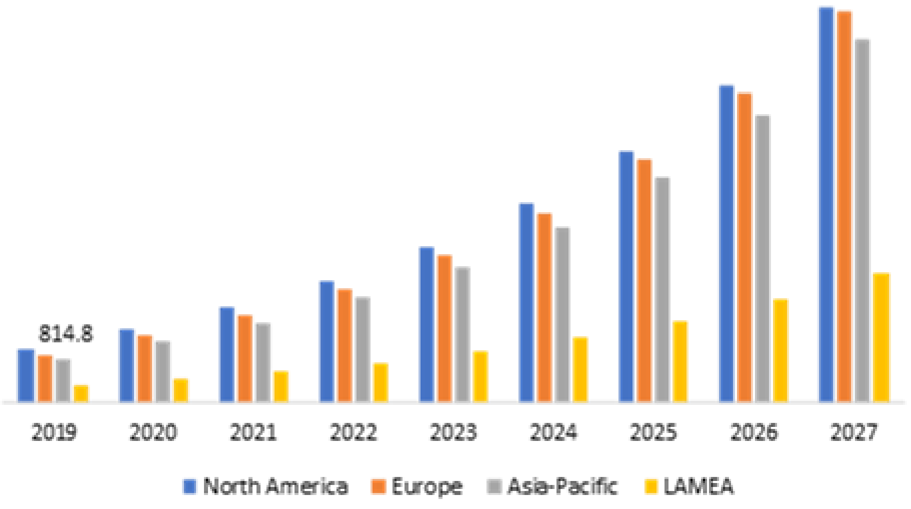


Figure 3. MDM market by regions. [29]

On the graph table above, it can be seen how MDM usage drastically increase in the current years and will continue the trend in the future years according to prediction, because it is hard to imagine that such technology would ever lose the worldwide interest, with the abilities such a software is providing, constantly evolving and obtaining new features in the functionality kit.

In addition, with the outbreak of COVID-19, private and public institutions are increasingly embracing the culture of working from home for their employees. Increasing the number of employees working remotely increases the risk of compliance bottlenecks and exposes organizations to the risk of sensitive data. To mitigate this risk, organizations are deploying mobile device management applications to enhance control and security capabilities. This provides a favorable opportunity to drive segment growth during the forecast period of the mobile device management market. [30]

According to trends in the mobile device management market, it is estimated that the significant increase in cloud-based deployments by SMEs will drive the growth of the mobile device management market in the coming years. In addition, the integration of mobile device management capabilities into the UEM suite is another key factor that is expected to accelerate the growth of Android device management in the near future. [30]

4.2 Main risks that may occur without MDM usage

In this paragraph it will be described why the usage of MDM is important and which risks will be mitigated by proper management of the devices, no matter which concept is going to be implemented as a solution for the organization: BYOD, CYOD, COPE or COBO.

The company's good MDM security policy ensures that commercial devices are not the victim of an attack. Mobile phone addiction has made them a prominent target for cyber-attacks. Previously, only computers and servers were damaged, but nowadays there is no damage that occurs in the world, and it is not suitable for mobile phones.

Despite all of our hometowns, people we meet, people involved, photos, movies, emails, etc., 97% of the world's population is simply not defending. Be yourself against attacks, especially business attacks. They focus primarily on computer devices but forget that mobile phones are still vulnerable to attacks. This trend is clear and growing. More than a quarter of the world's cyberattacks in 2019 were via mobile phones and they are still happening in 2022 and no doubts will be a problem in the future years as well. For businesses that manage mobile phones and tablets for business, device security must always be a top priority when it comes to managing mobile devices. [30,31]

***The list is as follows*:**

I. ***Spyware and phishing:***

Spyware is malicious software that is installed on your computer or mobile phone and collects data and sends it to third parties without your knowledge. This intrusion affects sensitive data such as credit card numbers, passwords, PIN codes, and browsing habit monitoring. This software adversely affects the entire network and reduces performance.

Spyware falls into four main categories. The Trojan horse impersonates the actual software. Cybercriminals access your system by tricking you into loading and running Trojan horses. You can then access and control the system through backdoors, spy on all sensitive data, steal, delete, modify, and even confuse its performance. It is important to know that this type of spyware concentrates the most common mobile threats and accounts for 95% of malicious programs. In addition to the backdoor, there are many types of malwares with different actions. Exploit bugs, rootkits, banking malware, DDoS malware, download malware, droppers, fake antivirus programs, or player data thieves are numerous to effectively protect your smartphone. The adware program is designed to display ads and collect marketing data. If adware collects them without your knowledge, it is considered malicious. These programs do not report their presence but can be removed using antivirus software. The tracking cookie file on the hard drive is placed there by the website where the user logs in. They contain a lot of information that can compromise the confidentiality of your data and provide your website with a lot of information about your browsing habits. It is important to remove them on a regular basis. [34,35]

II. *Loss of a device:*

If an employee's device is stolen or lost, it is inconvenient at best. But in the worst case, you are dealing with a complete disaster. Loss or theft can lead to serious breaches if employees do not follow company security protocols when using the device. For example, employees can store their passwords (both personal and work) in an insecure memo application. This makes it easier for anyone who gets the device to hack a corporate account.

Even if employees adhere to the guidelines to the end, hacking technology has become so sophisticated in recent years that strong password or fingerprint authentication requirements may not be sufficient to leave the device. Mobile device management (MDM) software provides a solution to this problem, and organizations can often wipe devices remotely, eliminating the opportunity for hackers to access sensitive data. [31,32]

III. Attacks through SMS:

SMS attacks are malicious threats that use short message services (SMS) and other mobile messaging applications to launch cyber-attacks. These attacks use malicious software and websites to harm users.

SMS attacks can lead to the theft of personal data and spread malware to other users. For SMS and other text message-based attacks, many tools can be used to carry out the attack. However, most of these attacks use malicious software or malware. Malware can be delivered to mobile devices by email and many other means, but SMS malware is advertised in text. This malicious software effort is aimed at harming and manipulating mobile devices without the user's permission.

If anything, these threats underscore the importance of malware protection on mobile devices. The threat of SMS-based malware continues to increase each year and will continue to pose a significant risk to mobile device users over the next few years. As a type of SMS attack, this threat and other threats in this category pose a serious threat to all mobile users. [33]

IV. Wi-Fi based attacks

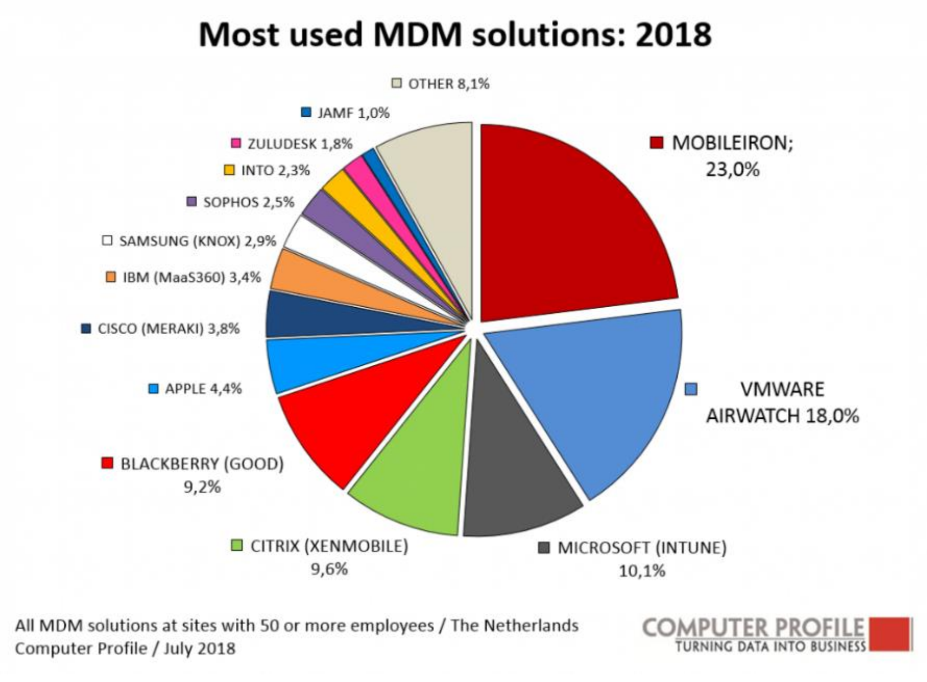
There are types of public wireless networks that your organization may use, when using a mobile device. A public network as it is called, and therefore not a secure network. Once you enter this network, you will join a public network space to which various other computers are connected, whose problems you are not familiar with. Information security companies are constantly reporting attempts by hackers around the world, who are simply waiting for computers to connect to the public network, through which they plant viruses and software to collect personal information and users` passwords. [36]

V. Policy and Ownership of Data

Data ownership is critical for businesses. Whether it is sensitive, personal, or financial data, it must be protected. When stored on a phone, any type of hacking can breach the data and free the property. You should always secure your information as well, which is possible via MDM network security. This might seem like an easy task, but it's a good idea to regularly back up your business data (contacts, photos, videos, etc.) on the commercial device and encourage the entire organization to do the same. All information must be stored in a safe place, e.g., on an external medium (PC) or in the "cloud". Follow MDM Security Policy guidelines. Entrust your email to a mobile device management service so you know your data is always secure and always accessible. All business information should be readily available when needed. Ensuring that your customers and clients know their data is safe and secure gives them more confidence and allows you to continue working without fear of attack. [37,38]

4.3 Existing third-party solutions and criteria

Today, in terms of fast-growing need for mobile device management, we have obtained enormous amount of MDM software from various developers and describing them all would be infinitely complicated. Thus, we will overview only some of the most popular software depending on the reference’s relevance and criteria, and what features do they include.



All MDM solutions at sites with 50 or more employees / The Netherlands
Computer Profile / July 2018

Figure 4. Most used MDM solutions in 2018. [28]

As it can be seen from the figure, we can confirm the overwhelming number of solutions in the year 2018. However, it is already 2022, and technologies do not stay on the same level as before. There were many significant changes in the number of solutions and their usage rate.

Due to enormous number of the MDM software, it is hard to say which of them are deserved to be the best among themselves. Business needs of every organization are varied, based on many factors, like company size, number of devices that must be managed, funding expectations and so many more. The same problem arouses with the software as well: there are many popular solutions, differentiated by number of minor or advanced functionalities, that make the management more convenient or has its own pricing, compatibilities with devices. Despite this, after making comparisons in reviews from variant sources, the most repetitive ones were included in the investigation.

More detailed study will be concluded on the following solutions:

1) IBM MaaS360; 2) Microsoft Intune; 3) Workspace ONE by VMware; 4) Citrix Endpoint Management

4.3.1 IBM MaaS360

IBM® MaaS360® Mobile Device Management (SaaS) is an enterprise mobility management (EMM) platform that provides visibility and control over smartphones and tablets in the enterprise. IBM MaaS360 software is compatible with devices such as iPhone, iPad, Android and Windows Phone. [39] With IBM MaaS360, you can monitor real-time device data usage and provide mobile app updates from a central location. Application updates can be deployed to Windows and Mac OS devices for applications such as Java, Adobe, Flash, Apple iTunes and more. [40]

Here are some ley features that we can outline, in order to understand what makes it good solution and apply them to our future MDM software concept: ***Real-time data usage monitoring, Malware detection and remediation, single sign-in to web and cloud applications***. Whether you manage multiple device types or a mix of corporate-owned and bring-your-own-device (BYOD) endpoints, Enterprise Mobility Management (EMM) and MDM solutions help you protect apps, documents, content and data, while managing user identity and access to ensure the right people get the right access to data from the right devices. Usage OTA (over-the-air) device enrollment for fast deployment with the leading cloud MDM platform. Streamline the device onboarding process for

Apple devices, including iPhone, iPad, and Mac, with Apple Business Manager. Use Android Zerotouch enrollment to provide employees with secure, exceptional, and out-of-the-box device setup. [41] Even though, with supporting many platforms, Windows mobile devices have to be enrolled manually and has limited functionality compared to other ones. [25,26]

4.3.2 Microsoft Intune

Microsoft Intune is a cloud-based service focused on Mobile Device Management (MDM) and Mobile Application Management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. You can also configure specific policies to control applications. For example, you can prevent email from being sent to people outside your organization. Intune also lets people in your organization use their personal devices for school or work. On personal devices, Intune helps keep your organization's data secure, and you can isolate your organization's data from your personal data.   Intune is part of Microsoft's Enterprise Mobility + Security (EMS) suite. Intune integrates with Azure Active Directory (Azure AD) to control who has access and what they can access. It also integrates with Azure Information Protection for data protection. It can be used with the Microsoft 365 suite of products. For example, you can deploy Microsoft Teams, OneNote, and other Microsoft 365 Apps to devices. This feature enables your organization's employees to be productive on all your devices while your organization's information remains protected with the policies you create. [42]

Key features: Customizable App Protection Policies, Manage Office Mobile Apps, Centralized Control Portal, Microsoft Malware Protection Engine, Reports and System Logs, Customizable App Protection Policies, Task Creation and Management.

Intune seems to be a great solution from a great company, however there also drawbacks in this solution as well. Firstly, it is highly dependable on Microsoft products, and it will try to give you a promotion on further usage of similar products related to the Microsoft. Moreover to this issue, it has one great drawback in the case of using it in the public organization: On-cloud installation. In the scope of our future concept, we have to bear in mind that our software will be running on-premises governmental servers, located in the facility itself and controlled from the MDM server located here as well.

4.3.3 Workspace ONE by VMware

Workspace ONE is a cloud-based workplace management system. It combines application management, access control, and unified endpoint management to allow IT to distribute and manage any app on any device while maintaining complete control and security.

The system allows all devices and apps to be managed through a single interface, removing the need for specific expertise and tools. This helps to avoid the formation of silos and/or tribal organizational structures, which can limit the IT infrastructure's flexibility and scalability. ***Key features include Unified endpoint management, network access control, user self-service and Automated app management.***

Workspace ONE enforces access decisions based on device compliance and identity context to secure the most sensitive information. You may mix and combine inputs in our powerful policy engine to make dynamic judgments about the level of access end-users have. This implies that if you need to prevent remote users from accessing data on unmanaged devices, you may do so with a few clicks. Workspace ONE, on the other hand, doesn't only block access. It goes a step further and assist end-users in achieving compliance. This protects your data while giving end-users the access they require. [43]

4.3.4 Citrix Endpoint Management

Citrix Endpoint Management is an endpoint management solution that includes mobile device management (MDM) and mobile application management (MAM). Endpoint Management allows you to manage device and app policies as well as distribute programs to users.

Identity, devices, apps, data, and networks are all secured to keep your corporate information safe. Ability to monitor Windows 10, Mac OS, iOS, tvOS, iPadOS, Android, Android Enterprise, Chrome OS, and Citrix. The software was created to help the user keep track of their own conduct. To protect sensitive data, Citrix Endpoint Management employs user context controls based on role, location, or device. Machine learning and analytics are used in the solution to help identify high-risk user behavior. Some of the key features include cloud devices Integrations with Azure Active Directory and Okta, which will not have benefit in our case, however such technology helps many enterprises. Also includes ***Machine learning and Analytics, Unique micro-VPN capabilities, Citrix Secure Mail, Automated Management Tasks***. [44,45]

Soti MobiControl

Users can choose between remote viewing and remote control when monitoring devices to take control of them for a more hands-on approach to performance concerns. There is also a chat feature that allows the administrator to speak with the device's end-user.

The program can also be used to safeguard files and web content on mobile devices. You can upload Microsoft Office files to the SOTI Hub app and control which users have access to the resources. The application is extremely beneficial for controlling file access and ensuring that only relevant personnel have access to sensitive information.

SOTI MobiControl's application management features are also highly handy. Administrators can use blacklists and whitelists to govern which applications are allowed. ***Key features are Rapid Provisioning and Enrolment, Compliance/Alert Rules, Interactive App Catalog.*** [46]

5 Practical analysis

This section will display whether MDM solutions are used in Azerbaijan in both private or public sector, including explanation on why third-party MDM solutions or BYOD concept is not the best fit for the governmental organization. Thus, all recommendations are also contained in this chapter.

5.1 Current situation in the country

After performing an interview with the IT team and Head of the IT department in the organization where research was performed at, it was clear that MDM solutions and concepts are not widely used in Azerbaijani governmental sectors in terms of employees. Such a solutions may be used in private companies and organizations, however, there is not much publicly disclosed or in other words, open-sourced information regarding this point. [49,50]

However, the concept of MDM is actually used in the Probation Service, which is closely related to the Ministry of Justice, in a way that special set of electronic surveillance equipment is given to the convicts to keep the track of their real-time location. This special kit consists of GPS bracelet on the leg and mobile device on Linux based OS. Obviously, all the actions done on this type of mobile devices are logged, tracked, and managed by special supervision teams, to be sure that allowed area of movement in the city was not violated by the convict or leg bracelet taken off, which will immediately sound an alarm in the monitoring center of Probation service, as well as in the case with the amount of battery left on the mobile device.[49,50]

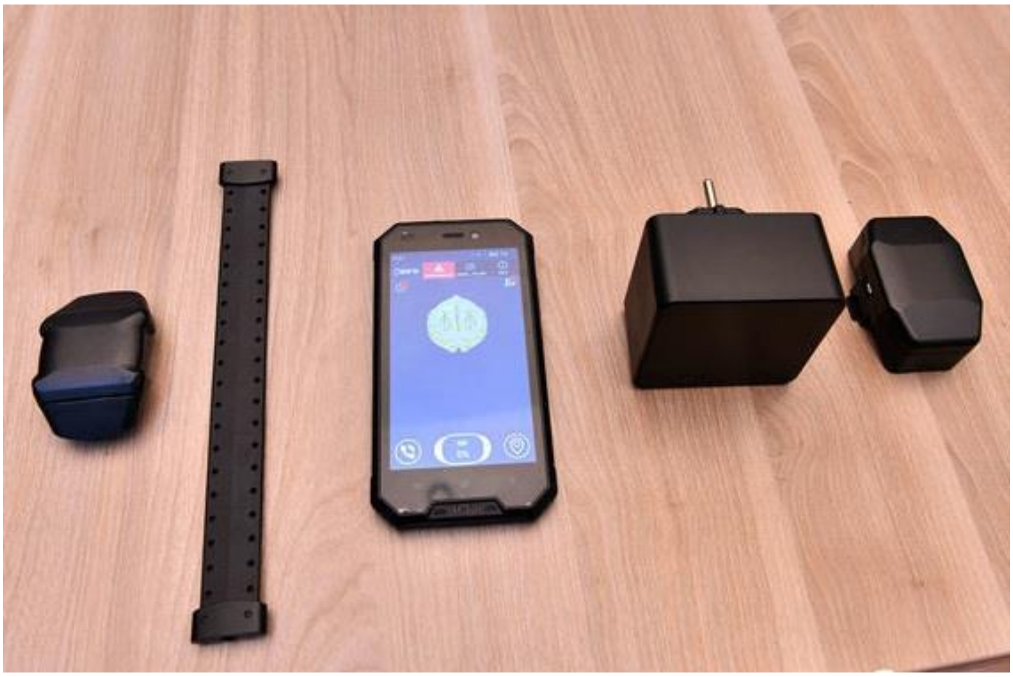


Figure 5. Surveillance equipment consists of Smartphone, bracelet and charging device

- Practically all probation programs abroad use this or any other type of electronic observation. Remote monitoring of those who have been sentenced and released prematurely as a condition of punishment is one of the most common ways to reduce the cost of the Penitentiary system. In addition to saving financial sources in the execution of alternative judgments, electronic monitoring has a number of advantages: lawbreakers keep jobs, are in the family, and do not lose social connections. Electronic surveillance allows you to use a multi-level measurement system and to monitor it in order to prevent residue. [47]

- Obviously, the sphere of use of electronic surveillance may be expanding. In October 2019, we began testing a new type of electronic equipment designed to monitor individuals convicted of public affairs, along with our colleagues at the Department of Justice's Information Communication Technology Administration. Once these devices arrive at work, they are given to convicts who activate it with fingerprints. [47]

This type of management is somehow similar to the MDM concepts that were mentioned before in the study. We have an organization, which performs “management” of the devices given out to the “employees”, which are convicts in this case, and monitoring them in real-time. This situation more or less gives us a picture of the COPE and COBO concepts, but this scenario will include the fact, that mobile devices are already configure by surveillance equipment technician and then transported to their "respective owners" and that leaves an option of describing it as a COBO concept.

The only question that arouses - Why the mobile device from later case is not used as a work device, which will be given out by the government facilities to the employees? This method seems to be logical indeed because we have a business only device, which can be monitored and managed by the already existing solutions that are used in the public right now.

Answer to the question before was found in the interview with the Head of IT department of Ministry of Justice facility branch. According to the interview question, it was outlined, that the mobile devices used by Probation service for tracking convicts are manufactured locally in the country, however not in the amount for supplying not only the country, but also for the city itself. Moreover, to the issue of manufactured device quantity, it is obvious that such a solution of using COBO concept will take not only the time but the great funding as well, especially in case of countless governmental organization located in the city an all over the country, because it would be essential to supply at least most of the employees in the facility, or the ones, who will have need to use this mobile device for concrete work purposes. As it was said before and confirmed in the talk, even if one of the facilities decides to implement a MDM solution, then this software must be created by the government itself. [50]

"It is very unlikely, that we will decide to use third-part solutions in terms of MDM, no matter what concept we will end up using, because we don't want to share the data of the whole country. It is our responsibility, and not someone else's. It may be true that we may be able to use the existing technologies utilized by Probation Service, but its current state of functionalities for that matter is not the best, to say for sure, because it was not planned to be developed for this kind of purpose. That leaves an option of creating the software by us from scratch, or, at least have some foundation taken from the convicts monitoring services." [50]

In addition, it was said that in order to come up with a future solution, a proper choice of the concept should be made by analyzing the amount of employees, approximate cost of the developing and implementing MDM software and other technologies or utilities related to it. Furthermore, at the current moment, Azerbaijani government have already their hands full, while bringing all the governmental structures in a single e-environment, for the convenience of all governmental structures and as an activity of such a kind, it takes enormous amount of time and effort which leaves small window for mobile security awareness for the public sector for now. [50]

Depending on the analysis research and information taken from interviews, it can be concluded that in case if MDM solutions will be implemented in the public sector in future, then there is a high possibility of it to be newly developed software, designed and ordered directly from the government agencies.

5.2 Choice of the MDM concept

For the current alignment of facts, it is possible to recommend the usage of two concepts to implement MDM strategy: Bring Your Own Device (BYOD) and Corporate Owned, Business Only (COBO).

Bring Your Own Device (BYOD) concept might seem to be a suitable solution, because of its fast-growing popularity, due to mobility and ability to connect both private and work life together in only one device. Several studies have demonstrated that allowing employees to carry their own devices improves staff morale and productivity. Why wouldn't businesses want to stick with a popular and cost-effective policy? While there are benefits and drawbacks to bringing your own device to work, we know it's a trend that's here to stay. On the other hand, it is important to bear in mind that there are issues with BYOD concept, especially if it is going to be implemented for public sector organization usage. Challenges of BYOD usage may occur in private organizations as well, which means public one will be endangered too.

True, bring-your-own-device lowers hardware expenses and relieves IT staff of some of the effort of managing employees' devices, but that benefit comes with one major drawback. Allowing employees to use their own devices means the IT department has no control over what apps are used, what data are downloaded, how frequently vulnerabilities are fixed, or what security precautions are done on those devices. When devices are not under the control of the IT department, it is far more difficult to prevent and remediate data breaches.

On top of that, even while workers' personal devices used for work are not part of the company, they still come into contact with the company's data, a firm's compliance responsibilities extend to them. Compliance is difficult to police due to the inherent security risks connected with BYOD and the greater potential that employees will disclose personal information with someone outside of the company network.

Besides, give an assumption that an employee has been dismissed. They may take sensitive information with them as they walk out the door if they previously accessed or saved it on their personal devices. To minimize security threats, the employer must erase company data from the ex-laptop employee's or phone as quickly as possible. To avoid a wild scramble, all workers should sign a contract addressing the use of corporate data when they start work, but there's no assurance they'll keep their half of the agreement.

The last, but not least, is the employee training. Employee errors are responsible for a large number of security breaches. When it comes to safeguarding their equipment, they may not completely comprehend organizational standards. Do you need your employees to participate in hands-on briefings or simply sign a document confirming that they are aware of company policies? Employees with insufficient training are more likely to make mistakes, endangering the security of the company's systems. This will require additional activities on creating special guidelines, thus creating financial and time expenses.

Meanwhile, **Corporate Owned, Business Only (COBO)** model provides the corporation complete control over the devices and programs in use, allowing it to provide the highest level of security imaginable which is most appropriate solution for governmental facilities. The substantially simpler procurement, administration, and support are also crucial advantages on the enterprise side in this paradigm, similar to the COPE model, with one additional advantage that devices are already ready for business usage and do not require any setup from employee, respectively reducing the needs in employee training of proper setup or installation of necessary applications on the device. Taking into the account an additional remark of having locally manufactured mobile devices used by Probation Service of Azerbaijan, could be supplied to the employees by the government.

There might be a pair of disadvantages as well in the usage of COBO, even though they can be mitigated with less efforts, rather than in BYOD case. Employees have a tendency to utilize technology less carefully because they are not allowed to use it for personal purposes. At the same time, when coworkers are required to carry two devices at all times, the chance of losing one of them grows. As a result, measures to protect data in the event of loss or theft are required.

With this being said, it can be concluded that the public organization in this research will be proposed with the usage of **Corporate Owned, Business Only (COBO)** method of managing the mobile devices, as it has more secure advantages and more tend to be used by the government in virtue of having already existing devices that can be used for this purpose.

5.3 Prototype of MDM solution

Considering a scenario, where government decided to create their own solution for mobile device management, whether it will be developed based on the Probation service convicts surveillance and device manager or built from the scratch, it must contain all the minimum needed features.

Table 1. Necessary features for MDM solution

1. The solution must be located on on-prem servers	2. Software must have both Mobile and Application management (MDM and MAM)
3. Admin console and proper level of security and/or hardening potential	4. Has its own database for storing the data on-prem
5. Has full control over managed COBO device	6. Mobile devices monitoring: check of OS version and overall system, ability to remote update if needed
7. Password change for devices occurring periodically.	8. Wipe feature in case of device loss or multiple password attempts

9. Ability to integrate with Security information and Event Management (SIEM).	10. Password control for managed devices
11. Encryption algorithms for data and/or applications	12. Must have a VPN solution
13. Device and network connection monitoring	14. Alert to the admin console in case of incidents
15. Perform necessary actions if incident occurred (restrict network usage or block access to the data on the phone)	16. E-mail phishing, SMS phishing and Man-in-the-Middle detection
17. WI-FI control	18. Bluetooth control
19. URL check for web	20. If organization decides to have Outlook as a mail service (not using currently), then Outlook Web Access restrictions required

5.4 Recommendations

All of the above features considered to be necessary for the development of the MDM solutions exclusively for the use of public organizations in Azerbaijan. Of course, the scope of this research is considered to be one of the branches of Ministry of Justice, however, because most of the governmental facilities will soon be connected altogether, this solution may be used for other public facilities as well.

After studying popular existing solutions in the market, making comparisons and outlining the features that will benefit this research, it is clearly seen that such a solution may be difficult to develop, however it is a must demand for governmental facility of such a level and the usage of COBO management policy is more profitable in this scenario rather than usage of the BYOD policy in the current scenario, which would brought up more problems in terms of defending both employees' and corporate data at the same time, bringing up more problems during the development of the software, when it should stay as lightweight as possible to prevent lags and stutters in the system, to maintain steady flow of working and monitoring processes, especially in emergency cases while dealing with the incidents.

As a goal of this research was to propose a usage of MDM software and concept for use in the public sector organization, this recommendation can be applied to other branches of governmental facilities as well, because the required concept and functionalities for the software that must be developed by the governmental initiative, to avoid using any third-party solutions and, if possible use the technologies of convicts' surveillance, both devices and their management system as a foundation for MDM software created for COBO concept, which is an only appropriate recommended solution in this scenario.

At the end, the main ideas for mobile security improvements are as follows:

- The requirement usage of MDM concept in the organization, in this case which is COBO. Usage of COPE or CYOD is also possible, however does not bring the most possible achieved security level for researched organization. BYOD concept must be avoided in this scenario.

- The requirement to develop and implement own MDM solution, including needed functionalities described in the Table 1

- Create proper documentation for the software and its implementation because it may be used in other governmental facilities as well.

- Usage of the existing technology for surveillance used by Probation Service for creating foundation for the developing a software of whole MDM for the organization

6 Conclusion

In the beginning, when collecting the data for the study, the initial plan was not to only propose the usage of Mobile Device Management, but also suggest using the Bring Your Own Device (BYOD) concept. At that moment of time, this idea remained the main motivation of the end result, because author was acquainted with all of the 4 main MDM concepts: BYOD, CYOD, COPE and COBO. However, it was not expected that my end result will differ from my initial expectation.

During composing this research, author have found out and used many references and performed interview directly with the persons, who are performing their duties in public sector of Azerbaijan. With the assistance of all information collected, it was clearly understandable that BYOD concept will not fit as the end solution for this concrete scenario, despite of it being so trending and growing popularity at the current moment, because many companies are permitting usage of personal devices and implementing the BYOD for working purposes. This may have seemed to be expected trend, as the technologies are updated/upgraded and developed every day in constant manner, however the impact of COVID pandemic played a big role in this process too. More and more employees are working remotely, and this is a fact nowadays. On top of this, it was also concluded that mobile devices are also in the same level of danger as well as any other device.

Management solutions and related technologies are evolving day by day and so are the threats. Phishing attacks in cooperation with malicious attachments has always been and stay very hazardous issues and there is enormous amount of successful attack cases all over the world. Even with the Multi Factor Authentication (MFA) activated, there are still incidents when cybercriminals were able to bypass it. Even in this particular research, where the scope is only one of the governmental branches, which has a little more than 60 employees, it is still important to consider the need in process automation for device management and supervision and/or data control indeed, because it may be almost impossible to handle all of these devices separately.

The evolve of Mobile Device Management expected to be trending upwards, as more and more mobile devices are used by employees. As the technologies develop, it is obvious that the cybersecurity hazards are not stagnating too and it is never late to enhance cybersecurity aspects of organization, no matter what size it is, however, ignoring this issue for a long period of time, may create catastrophic situations in the future.

References

1. Hari Subedi (May 1, 2021) Importance of Mobile Device Management For Small Businesses | Jones IT (itjones.com) 16.03.2022

2. Diksha Barthwal (June 2016) (PDF) Mobile Device Management (MDM) in Organizations (researchgate.net) 16.03.2022

3. Kamil Glowinski, Christian Gossmann, Dominik Strumpf. (December 7, 2019) Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects | SpringerLink

4. Martin Brodin (March 2, 2016), Academic Editor: Lasse Berntzen. Mobile Device Strategy: From a management Point of View: Microsoft Word - 593035fo (diva-portal.org)

5. Katja Keinänen: What is MDM? A Complete Guide to Mobile Device Management - Miradore 18.03.2022

6. Paul Ferrill (January 8, 2018) The Best Mobile Device Management (MDM) Solutions | PCMag 18.03.2022

7. Erica Mixon, Senior Site Editor,Colin Steele. What is Mobile Device Management (MDM)? (techtarget.com) 18.03.2022

8. Matt Kapko (Oct 9, 2017). What is EMM? Enterprise Mobility Management explained | Computerworld 19.03.2022

9.Lisa Elis/// Jefrrey Saret///Peter Weed. BYOD_means_so_long_to_company-issued_devices_March_2012.ashx (mckinsey.com) 19.03.2022

10. Matthew Finnegan(July 14,2021).What is UEM? Unified endpoint management explained | Computerworld 19.03.2022

11. What is Mobile Device Management? | VMware Glossary 18.03.2022

12. Lucas Mearian (Jul 10,2017) MDM, mobile app management and enterprise mobility management defined | Computerworld 20.03.2022

13. What is Mobile Device Management (MDM)? (techtarget.com) 20.03.2022

14. Daniel Hein (August 29, 2019). BYOD vs. CYOD vs. COPE: What's the Difference? (solutionsreview.com) 21.03.2022

15. Brenna Lee (Feb 2, 2022). Defining BYOD, COPE, COBO, and CYOD - JumpCloud 21.03.2022

16. Marje Salumets (29.04.2020). ISO 27001 Compliant Management of Mobile Devices in a Medium Size Private Enterprise.

17. Matt Williams (24.10.2017). BYOD vs COBO vs COPE vs CYOD: What's the Difference? Which is Right For Your Organization? - Faronics 23.03.2022

18. Murugiah Souppaya, Karen Scarfone(June 2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise (nist.gov) 25.03.2022

19. Mobile Device Management (MDM) solutions | Codeproof 25.03.2022

20. Extension of ISO/IEC27001 to Mobile Devices Security Management | SpringerLink 26.03.2022

21. Michael Lee (May 17, 2012). How government does BYOD | ZDNet 26.03.2022

22. Top Six Benefits of Mobile Device Management | N-able 26.03.2022

23. Top 10 Benefits of Mobile Device Management (MDM) (techfunnel.com) 29.03.2022

24. What are the Benefits of Mobile Device Management? (knowledgenile.com) 29.03.2022

25. Stephen Cooper (April 8, 2022). 11 Best Mobile Device Management (MDM) Solutions 2022 (Paid & Free) (comparitech.com) 30.03.2022

26. 10 Best MDM Software Solutions in 2022 [SELECTIVE ONLY] (softwaretestinghelp.com) 30.03.2022

27. David Nield, Brian Turner, Christian Cawley (December 8, 2021). Best MDM solutions in 2022 | TechRadar 30.03.2022

28. Mobile device management increasingly a standard part of IT policy - Smart Profile 01.04.2022

29. Mobile Device Management Market: Opportunity Analysis and Industry Forecast, 2019–2027 (researchdive.com) 01.04.2022

30. Divyanshi Tewari and Aishwarya Rajvaidya, Vineet Kumar (July 2021). Mobile Device Management Market Size, Share & Growth Analysis 2030 (alliedmarketresearch.com) 01.04.2022

31. 8 MDM Security Risks Businesses Cannot Compromise | AirDroid Blog 02.04.2022

32. Top 7 risks of bring your own device (BYOD) | N-able 02.04.2022

33. SMS Attacks and Mobile Malware Threats (kaspersky.com) 02.04.2022

34. Sam Geary. Malware, phishing, spyware and viruses - what's the difference? - PCS (pcs-systems.com) 04.04.2022

35. Spyware, Adware and Viruses | The ILR School | Cornell University 04.04.2022

36. Wireless Attacks and Their Types (examcollection.com) 04.04.2022

37. What is Data Ownership? - Definition from Techopedia 04.04.2022

38. John Powers (22 Jan 2020). Ownership scenario should dictate mobile device policies (techtarget.com) 07.04.2022

39. Introducing IBM MaaS360 Mobile Device Management (SaaS) - IBM Documentation 07.04.2022

40. 11 Best Mobile Device Management (MDM) Solutions 2022 (Paid & Free) (comparitech.com) 07.04.2022

41. Android – Android Enterprise Zero-touch enrollment 07.04.2022

42. What is Microsoft Intune | Microsoft Docs 08.04.2022

43. What is VMware Workspace ONE? 08.04.2022

44. Endpoint Management | Citrix Endpoint Management 08.04.2022

45. Citrix Endpoint Management - A Unified Endpoint Security Solution - Citrix 08.04.2022

46. SOTI MobiControl - EMM Solution | SOTI 08.04.2022

47. Akshin Ziyadov, Ministry of Justice of the Republic of Azerbaijan (20-11-2019) 14.04.2022

48. Azərbaycanda 230-dan çox məhkum elektron qolbaq daşıyır (trend.az) 14.04.2022

49. Anonymous, Surveillance equipment technician. (2022, April 3) 15.04.2022

50. Anonymous, Head of IT department (2022, April 3) 15.04.2022

51. Abdullahi Arabo and Bernardi Pranggono (2013) (PDF) Mobile Malware and Smart Device Security: Trends, Challenges and Solutions (researchgate.net) 16.04.2022

52. 7 BYOD Challenges to Know When Implementing BYOD Policies | N-able 16.04.2022

53. Garrett HollanderThe Top 7 Risks Involved With Bring Your Own Device (BYOD) (m-files.com) 16.04.2022

Appendix 1 - Interview questions

1. Are there any governmental facilities currently using Mobile Device Management solutions?

2. What are the limitations for usage of MDM in the case of public sector? Are there any restrictions in using third-party solutions?

3. How does this convict’s surveillance equipment by Probation Service work?

4. Would it be possible to use existing method of management of mobile management using the surveillance equipment from Probation Service?

5. Would you rather prefer BYOD or COBO concept in terms of management?

6. Why has government not discussed the need of implementation of MDM until this moment?

7. Would it be possible solution for government to create their own MDM solution?

8. If it was decided to create such a solution, how likely it will have foundation of Probation Service’s monitoring software or build it from the scratch?

9. In case the COBO concept will be used, and mobile devices from Probation Service will be chosen as the ones which will be given out to the employees, would it be possible to supply every employee with it?

10. Do our government use any third-party cloud storage solutions?

11. Are the restrictions on using third-party MDM solutions are also applied to implementing your own solution, if so, one is created for example, on third-party cloud storages?

Appendix 2 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Fakhri Ramazan

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Improvement Recommendations for the Mobile Device Management Policy of Public Sector Organization Employees in Azerbaijan, supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

23.04.2022

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.