BUSINESS AND IT ARCHITECTURAL REQUIREMENT ANALYSIS OF GENERIC BYOD PROGRAMS

CELAL ÜNALP

JANUARY 2017

BUSINESS AND IT ARCHITECTURAL REQUIREMENT ANALYSIS OF GENERIC BYOD PROGRAMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ÇANKAYA UNIVERSITY

BY

CELAL ÜNALP

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY

JANUARY 2017

Title of the thesis: **Business and IT Architectural Requirement Analysis of Generic BYOD Programs**

Submitted by **Celal ÜNALP**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University

Prof. Dr. Halil Tanyer EYYUBOĞLU
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Fahd JARAD
Department Chair

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asst. Prof Dr. Özgür Tolga PUSATLI
Supervisor

Examination Date : 20.01.2017

Examining Committee Members :

Asst. Prof. Dr. Özgür Tolga PUSATLI
Çankaya University

Asst. Prof. Dr. Tolga MEDENİ
Yıldırım Beyazıt University

Asst. Prof. Dr. Abdül Kadir GÖRÜR
Çankaya University

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Celal ÜNALP

Signature :

ABSTRACT

BUSINESS AND IT ARCHITECTURAL REQUIREMENT ANALYSIS OF GENERIC BYOD PROGRAMS

ÜNALP, Celal
MSc., Information Technologies
Supervisor: Asst. Prof. Dr. Özgür Tolga PUSATLI

January 2017, 84 pages

Bring Your Own Device (BYOD) is a contemporary concept and an enterprise mobility management paradigm by which organizations allow employees to connect their personal devices to the corporate network and access collaborative applications. It needs to be analysed and improved in relation to implementation, determination of program and scope, selection of policy and model and demonstration of strategic points. The main objective of this research is to find an answer to "what comprehensive strategy can be advised to organizations in the beginning phase of their first BYOD program?" Within the scope of this work, deciding on a BYOD strategy, determining identity management, defining access policies and implementation of a roadmap to a generic BYOD were examined and evaluated. Systematic literature review was conducted and real world business cases were reviewed. Personal privacy, corporate confidentiality, app wrapping, IAM, and new technology requirements for complex environments are acknowledged as research findings. Public governance bodies, private corporate secrecy, financial design prospect, budget considerations and ever changing legislative environment were primary limitations in this research. Choosing the baseline framework is the first step in this study. A potential benefit of this work is to provide such framework to organizations to decide which additional service and deployment model best meets their needs.

Keywords: Bring Your Own Device, BYOD, IAM, Identity Management

ÖZ

JENERİK "KENDİ CİHAZINI KENDİN GETİR" PROJELERİ İÇİN İŞ VE BT MİMARİ GEREKSİNİM ANALİZİ

ÜNALP, Celal
Yüksek Lisans, Bilgi Teknolojileri
Tez Yöneticisi: Yrd. Doç. Dr. Özgür Tolga PUSATLI

Ocak 2017, 84 sayfa

Bring Your Own Device (kısaca BYOD), çalışanların kendi akıllı cihazlarını iş yerine getirmelerine, kurum iç ağa bağlanmalarına ve kurumsal verilere erişmelerine müsade edilen, güncel bir kurumsal mobilite paradigmasıdır. Uygulama, uyarlama, programın ve kapsamın belirlenmesi, politika ve model seçiminin yapılması ve stratejik noktaların gösterilmesi konularında analiz ve geliştirme ihtiyacı bulunmaktadır. Araştırmamızın ana hedefi, "ilk BYOD programının başlangıcındaki kuruluşlara ne gibi kapsayıcı stratejiler önerilebilir?" sorusuna yanıt aramaktır. Bu çalışma kapsamında, BYOD stratejilerine karar verilmesi, kimlik yönetiminin belirlenmesi, erişim politikalarının tanımlanması ve jenerik BYOD uyarlama yol haritası incelenmiş ve kapsamlıca değerlendirilmiştir. Sistematik literatür taraması yapılmış ve iş dünyasından gerçek uyarlamalar gözden geçirilmiştir. Kişisel mahremiyet, kurumsal gizlilik, uygulama izolasyonu, kimlik, erişim ve yetkilendirme yönetimi ve kompleks ortamlarda ihtiyaç duyulacak teknoloji bileşenleri çalışma bulgularımız olarak kabul edilmiştir. Kamu sektörel kimliği ve kurumsal ketumiyet, finansal tasarım, bütçe kısıtlamaları ve sürekli değişim gösteren yasal durumlar sonuçlarımızı kısıtlayıcı olmuştur. Çalışmamızda, kavramsal iskelet ve çatının oluşturulması ilk aşamayı teşkil etmektedir. Kavramsal çatı ve iskeleti elde ederek çalışmalarımızdan faydalanacak olan kuruluşlar bu noktadan sonra, hangi ek servise ve kurulum modellerine ihtiyaç duyacaklarını daha kolay tespit edebileceklerdir.

Anahtar Kelimeler: Kendi Cihazını Kendin Getir, Erişim ve Kimlik Yönetimi, BYOD

To My Wife and Son

ACKNOWLEDGMENTS

The author wishes to express his deepest gratitude to his supervisor Assistant Professor Dr. Özgür Tolga PUSATLI for his guidance, advice, criticism, encouragement and insight throughout the research.

TABLE OF CONTENTS

CHAPTERS:

ACRONYMS AND ABBREVIATIONS

ADP	Apple Deployment Program
APN	Apple Push Notification
BYOD	Bring Your Own Device
DDI	DNS, DHCP, IPAM
DEP	Apple Device Enrollment Program
DLP	Data Loss Prevention
EAS	Microsoft Exchange ActiveSync
EMM	Enterprise Mobility Management
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDaaS	Identity as a Service
IPAM	IP Address Management
IPSec	Internet Protocol Security
ITAM	IT Asset Management
LAN	Local Area Network
LOB	Line of Business
MCM	Mobile Content Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MTA	Multi-Tenant Applications
NAC	Network Access Control
NDA	Non-Disclosure Agreement
PaaS	Platform as a Service
RBAC	Role-Based Access Control
SaaS	Software as a Service
SCEP	Simple Certificate Enrollment Protocol
SDN	Software Defined Networking
SIEM	System Information and Event Management
SLA	Service Level Agreement
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

1. INTRODUCTION

1.1. The Current State of BYOD in Business

Bring Your Own Device is a new approach that allows employees to use their own devices, with the business or educational networks, and access on-premises services. BYOD is also an increasingly common phenomenon for enterprises and institutions on the leading edge of mobile device management. It is opening up the potential of productivity gains, serving as a motivation for employee satisfaction and seeding innovation, while exposing the enterprise to data and device management risks.

Mobile device market has been expanding and substantial portion of end-users are contributing this formation. Common features of consumer devices and enterprise devices are now at the same level. Although in the past they were totally different. A recent consumer smart device can surpass the computational power of business equivalent. Additionally, enhancements in the mobile communications and improvements of the transmission speeds are helping industry to gain and maintain such momentum. These are important reasons for this shift towards BYOD. [12]

Consumerization of IT guides and drives the business world hereafter. Updates and upgrade speeds have always been easier and faster in the consumer goods and markets. Alignment with consumer markets within the mobility field bring efficiency rather than business technology adoption. Enterprise end-users can also enroll to special plans and utilize discounts only available for their corporate accounts.

Building automation devices and industrial Internet of Things (IoT) devices are leveraging the corporate networks, however enterprise IT has serious issues identifying these devices and placing them as part of the current network access policy. Internet of Things devices have exceeded employees and guests as the biggest portion of the enterprise network. Unification in consumer and business electronics spaces leaves small differences into only software layer.

Recently many businesses have little to no BYOD presence in their ecosystems. Formal BYOD offerings are new but also gaining official support from enterprise IT departments. BYOD programs create interest and attract attention. According to GARTNER's 2011 study for United States, CIOs were anticipating %38 of their workforce to be participated in a BYO program. [12]

However, well-formed BYOD programs can lead to greater participation and productivity by extending mobile computing to a whole new class of employees, enabling them to choose the tools best suited to the task, and creating new line of business mobilization opportunities.

Contrarily, it is important to determine whether there are any barriers to implement BYOD programs or not. Barriers may include the threat of data leakage in a sensitive environment, lack of operational awareness, inability to comply with laws or compliance requirements, and labor laws or social issues. If any of these barriers exist, work-arounds can include restricting BYOD programs only to those departments or classes of users that are not impacted, or implementing a choose your own device (CYOD) program where the organization retains ownership and full control of employee devices, however offers the employees a much wider range of choice in the type of devices.

Consumer devices are being integrated into corporate standards through the demand and action of unsatisfied workers who have previously complained about their old, slow and unfit corporate devices. From every level of corporate hierarchies, workers feel empowered by the consumerization of IT and, equipped with their innovative consumer mobile devices, find new ways around conservative IT rules, managing to access and use corporate resources. Organizations react by limiting the trend or by trying to capitalize on its benefits and minimize its drawbacks, by defining rules and setting control and management points, through comprehensive BYOD policies and programs.

There are several strategies for enterprise ITs approaching to BYOD, ranging from do-nothing to total-lockdown. However, the most effective strategy has determined for IT segmenting employees into groups, and providing access and appropriate support for each. BYOD implementations can be complex for enterprise IT with many moving parts. Therefore, there is value in leveraging the lessons from other implementers.

The US White house shared their suggestions in a comprehensive document in 2012. They have suggested that virtualized environments will have a great chance to succeed. Virtual desktop infrastructures that store and process critical information within secure data centers should be selected for federal agencies. They have also suggested that critical enterprise and end-user data should be stored and processed separately within mobile devices and handled with walled garden paradigms. [56]

Australian Signals Directorate (ASD), also known as the Defence Signals Directorate (DSD) has developed a document titled "Risk Management of Enterprise Mobility Including Bring Your Own Device" for Australian government agencies, to provide them with a list of enterprise mobility considerations. Considering legislative issues, budget and personnel plans, regulatory compliance, risk assessments and several controls for additional business cases. [54]

The European Network and Information Security Agency (ENISA) is serving to European Union member states as a central information technology and security institution and help them for better guidance, cooperation and coordination. ENISA has produced a report using real life experiences and best practices of IT organizations. [92] This report is an ENISA deliverable in the area of "Identifying & Responding to the Evolving Threat Environment". It briefly explains the risk and business assessment of "Consumerization of IT" (COIT) as a related term for BYOD. [93]

ISACA is a nonprofit global IT audit framework and guidance supplier organization. They produce, maintain and deliver best practices, industry guidance, knowledgebase, information libraries and periodic publications. ISACA has been placing emphasis to BYOD since 2013, and published several written materials to their subscribers. [94]

NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) is enhancing the cooperation, augmenting the defense partnership and bringing excellence in teaching capabilities for allied members. CCDCOE special study "Defending mobile devices for high level officials and decision-makers" describes security controls and data protection for smart devices. This material describes the risk mitigation, asset protection and cost reduction methods of unsecure use cases including BYOD. [95]

United Nations E-Government Survey 2014 summarizes "Mobile and other channels for inclusive multichannel service delivery" and states that innovative E-government can motivate new initiatives and support e-transformation for more effective public administrations. Demand for public online services which are time and place independent for the handicapped people, is also growing and cannot be taken outside of the BYOD discussion. [96]

A modern and comprehensive approach such as BYOD can be taken as an opportunity of the emerging technology and applicable solution for the transition to e-government and it allows decision makers to evaluate requirements and embrace disadvantaged and handicapped individuals and find new ways to participate them in social life.

Our ambition for this thesis to support IT organizations for better understanding the risks assessment and mitigation while fitting into BYOD. Non-corporate-owned equipment are not considered as secure and conformant due to the lack of their integrity, regulatory compliance and the budget resources.

1.2. Motivation

Enterprise IT is in transformation again. BYOD programs are reshaping the economics of end-user and corporate computing. Use of employee devices in a workplace is an emerging trend in a wide range of enterprises. The challenge for enterprise IT is to manage this transition to BYOD without exposing the enterprise to unnecessary device management, data security and cost control risks, and without stopping the innovation these devices may indicate.

Previous chapter, “The current state of BYOD in Business” offers an opportunity for us to sense and investigate major background aspects and perceptions of enterprise mobility in this study. BYOD is one of the new concepts that concerns organization, people and the technology at every level. Major hardware, software service provider vendors are also raising attention to this topic by supporting integration options.

In academic literature, little can be found about consumerization of IT and BYOD. Because BYOD is supposed to be ephemeral at the first occurrences. And first articles about BYOD were insufficient to measure of its intensity, determine implementation areas and possible real world opportunities.

On the other hand, consumerization of IT and BYOD became very attractive and famous in real life of business IT and related institutions. Many of these media describe and analyze IT consumerization and its impact on businesses. Our findings showed that BYOD is not transient, it is a real industry shift and represents a true revolution. There is a clear move towards a policy of BYOD to pursue enterprise mobility initiatives. The fundamental architectural components and definitions certainly acknowledge this; all describe the influence of IT consumerization on an enterprise.

Most white papers, journal articles and academic papers which have been published about BYOD, deal with the non-technical aspects, for example solution and strategies for security, privacy and employee productivity. A comprehensive approach, which reveals the expectations and technical requirements of a BYOD service from a customer perspective, was not available. Therefore, coherent literature review and proposal of the BYOD paradigms is needed. The results of this study can assist organizations and researchers by providing them with useful information about BYOD and the issues involved with technical implementation. It should be examined how the perception of a BYOD service varies due to different technical backgrounds of the IT organizations. At this point, the research of this master’s thesis starts.

Our primary motivation for this research were new BYOD strategies that can be used and integrated into existing ecosystems and support for requirement responses. In our framework of solution, we first match the correct methods for problem approaches and then fine tune the additional decision points. The entrance of consumer technologies into the enterprise and the BYOD trend has enlightened the IT organization and the enterprise end-users. Without such resolution, IT organizations may find it difficult to protect the organizational IT assets and intellectual property, control the costs of delivering support, security and other services, earn or sustain recognition as a valued partner to other business units and finally take advantage of modern ideas and concepts in the technology world.

Overall, the main driver and primary motivation to look into BYOD as a reaction to two trends: Consumerization of IT as well as the proliferation of mobility. In this sense, environmental requirements and infrastructure integrations of BYOD plays an important role in alignment of any company's business with its IT strategy. In parallel, we are considering that employees want more control over how, where, when, and with which device they perform their work.

1.3. Purpose and Scope

The introduction of BYOD policies is the corporate response to manage and leverage this trend. BYOD policies are answering the demand for the use of personal devices in the workplace. While driving the adoption of mobility, this trend places an added burden on mobile-first deployments. The resulting multitude of hardware, software, and configuration options that users can choose under a BYOD policy greatly inflates the complexity of a EMM deployment. The impact is significant, forcing the introduction of changes in requirements predefined goals for MDM.

The goal of this study is to provide checklists for project management, requirement analysis, implementation phases and critical process automations of compute and data facilities for BYOD applications. In this thesis, the detailed description of the proposed environment, infrastructure and architecture is carried out. Here we examine, extract and expanded the critical information within the generic BYOD solution.

BYOD is gaining popularity in most business disciplines, within the EMM suites and mobility spaces. This thesis focuses on four important requirements in enterprise mobility solution and defines them as a baseline checklist for a BYOD program.

- Deciding on a BYOD Strategy
- Determining Identity Management
- Defining Access Policies
- Roadmap to BYOD Implementation

For simplicity, our study is limited to mobile devices such as smartphones and tablets, however strategies may also be used for PCs.

We have also limited our focus on technical requirements, providing only MDM, MAM and EMM, plan, coordination and administration.

This study summarizes our recommendations and detailed principles to organizations who need policy preparation, strategic planning and project management reinforcement. We then go into the integration phase and we also assess the state of the art in management and security technologies.

Our considerations for solution, design and implementation are generic and can be applied to wide range of mobility topics. This study focuses on the technical environmental requirements and infrastructural integration from layered tier model and perspective.

Our purpose is to provide right mobility tools, enterprise technologies, application options and path selections to IT departments. Different payloads will be attributed in different parts for this document, however EMM suites are common requirement across all devices and use cases, so it will be discussed in detail.

In our cases, end-users always derive benefit from new and emerging technologies which are cheap and effortless, and organizations derive benefit from enterprise grade and business ready security environments while protecting existing investments.

After establishing a mobile security policy, an enterprise should prepare their mobile device management methodology and select a solution framework to put into practice.

1.4. Research Questions

In the context of consumerization's influence on IT, many of today's IT standards may appear dictatorial in nature, and focused on serving IT rather than end-user interests. As a result, business stakeholders may think of IT as obstructionist. End users are spending their money for using a favorite mobile phone, tablet device and productivity apps. They always search for and finds new ways to bypass IT policies. IT organization may discover underground user communities or "shadow IT" that bypass IT standards. Without a framework in place to address this trend, IT organizations are faced with unexpected support costs and management complexity.

The root of the problem lies in how IT approaches the responsibility for providing security and support to the enterprise. IT has traditionally operated with a command-and-control approach, using rigid policies and standards to ensure necessary safeguards and end-user support.

As a result, the main objective and research question of this research is to propose:

What comprehensive strategy can be advised to organizations in the beginning phase of their first BYOD program?

To achieve this objective more effectively, we can extend it under the following sub questions.

Q1: What are the participating roles of privacy for employee and security for organization in BYOD environments?

Q2: What coherent motivations do organizations have integrating mobile devices into workplaces?

1.5. Potential Benefits

Many organizations seek to start or extend an existing BYO program without fully examining the intended goals. Often, there is a misperception that BYO will reduce total cost of ownership, although in most cases the savings remain elusive, especially if additional security, manageability and support processes need to be developed.

The concept of BYOC can also offer benefits to end users and potentially to IT departments. IT leaders should research and understand the impact on management and support to make it successful.

Many organizations are investigating, piloting or implementing Hosted Virtual Desktop or Virtual Desktop Infrastructure (HVD/VDI) and BYOD programs. VDI and BYOD programs executed without considering licensing may incur unexpected software costs under traditional agreements. Endpoint computing and procurement managers should review terms and licensing alternatives as part of their preparation.

BYOD policies should be developed with broad involvement of all departments and should include program eligibility guidelines, end-user support and service level agreements, risk assessment, initial training and education, funding strategies, and IT publishing preparation and customization of code of conduct, code of practice and code of ethics.

2. BACKGROUND CHAPTER

2.1. Introduction to Remote Access and Teleworking

Remote access requirements and methods came into picture with the invention of computer like devices and numerical calculators in early 1940's. George Stibitz designed The Complex Number Calculator (CNC) and Bell Telephone Laboratories installed it in 1939. Mr. Stibitz demonstrated the remote calculation operations using a teletype device and this is considered to be the first occurrence of remote access computing. [1]

Since then rapidly advancing military technology and space age requires the use of computers. Many transactions and activities to be performed remotely gained great importance and extending until today matching the needs of the business world has become an indispensable use.

The first communication network had only two nodes and one of them is a dumb terminal. They could only enter some text and then display it remotely over the wires. With the addition of smarter and faster nodes these networks got larger and gained importance. Less expensive equipment allowed IT departments to use them for daily tasks. Desktop computing spreads the workload and brings flexibility, but this way all the corporate data was sprawled. [2]

The real communication network came into practice with local area networks, and wireless fidelity networks. As the networking technology got faster and easier, computers could reach others over distances, what is known as wide area networks. At the final stage, private and enterprise networks converged with the Internet under the name of cloud computing. [3]

After a long transformation, we have seen large desktop machines, portable laptops, tablets and now smartphones. With network expansion, Wi-Fi and cellular speed improvements, and software developments, remote access are more common and golden standard for IT.

Then organizations returned back to centralized storage, data and security management. Such phase in network development did not last, smart and powerful mobile devices gave workers freedom in and out of office. That is where IT industry is today, and the trend is growing. Consumerization of IT and proliferation of mobility are not only changing paradigms, but they are also a bringing new risks for organizations. [4]

Cloud computing, social media, mobility and big data analytics are collectively enablers of BYOD (Bring Your Own Device) in enterprise ecosystems and one of the prospects of innovation. [5] BYOD does not represent a new technology or product; it consists of multiple technological trends, approaches, frameworks and innovation. [6]

Consumerization is a shift towards a new level where requests, rules and limits are dictated by customers and all others aligned around it. With "mobile and wireless technologies" the fastest growing area for technology investments, the new emergent technologies were also identified. Advancements in mobile device market have allowed consumer devices get into the enterprise world. [7]

Rapid changes in technology have affected the size of data and the ways of accessing it. Cloud computing and BYOD are bringing essential changes in the resource allocation, security disciplines and asset management. [8]

Two decades ago, only organizations had access to advanced and innovative computer technologies but nowadays consumers have direct access to these technologies. This shift is called "IT consumerization" or "consumerization of IT". Three aspects are key for this transition: manufacturers recognized the large consumer market, technology became affordable and user friendliness increased. A result of this phenomenon is that employees use their consumer technologies for work related activities, since organizations do not offer them the desired technologies. [10]

Consumerization of IT and the proliferation of mobility have changed the information handling and communication technologies. It has rapid transformative affects and causes serious changes in working, communicating, collaborating and conducting daily business. [11]

Mobile device market is growing rapidly and common features of consumer devices and enterprise devices are now at the same level. Although in the past they were totally different. A recent consumer smart device can surpass the computational power of business equivalent. Additionally, enhancements in the mobile communications and improvements of the transmission speeds are helping industry to gain and maintain such momentum. [12]

Enhancements in the mobile communications and improvements of the transmission speeds are helping smart devices to derive more benefits from cloud apps. [12] We can count the mobility as the new disruptive force next to cloud computing and software defined networking. [13]

As smart devices getting smaller and wireless speeds increase, people are putting more of their electronic personas into their pockets. Especially IT professionals are using multiple brand and model of devices at the same time for their daily tasks with different settings, accessibility, and capability. [14]

Using smart devices brings significant advantages and has become popular in private space. However, having more than one device for same purpose is not acceptable for every use case. The advantage is not to carry two different devices, one for private and one for professional issues. [15]

Our study examines the monitoring techniques, privacy concerns, and employee performance when evaluating whether to participate in a BYOD program or not. For a closer look at the components, tools and capabilities of an end-to-end BYOD solution, we will examine them further, one by one.

Three letter abbreviations technologies have emerged over the years to help industry and academics better define, manage and control devices, data and applications and this landscape of technologies continues to evolve.

In this chapter, we will make reader familiar with required background on people, organization and technology aspects and its fundamental concepts.

Readers might want to skip this chapter quickly and advance to the next chapter unless the reader is new to BYOD or want a refresh existing IT glossary.

2.2. Privacy Policy

Personal information stays in the center of major concerns when discussing BYOD, and the issues of privacy have more importance than ever. Mobile devices contain great amount of personal data with the enterprise data on the same software environment. Because of this, storage and processing isolation should be implemented between them. [14]

Privacy policies are protecting sensitive personal information by acting as legal aspects of computing and regulating the ways of acquiring, processing, reporting, and disposing data. It is an integral part of business IT and requirement to protect individual’s privacy. [16]

Privacy policy is the acknowledgment between enterprise corporate parties and individuals on how they collect, store, process and release personal information. It briefs, instructs and notifies the participants what personal information is collected, shared or sold to other parties or enterprises.

2.3. Mobile Device Policy

As the number of IT devices grow, the need for effective management technology and handling policies of them also grows. Mobile device policies help IT departments to align their new and essential security constraints.

BYOD is proving that the organization and the people are now at the new equilibrium. Employees accept the corporate policy and lose control, eventually that can mean the remote erasure of their own device. At the other hand, they obtain the freedom to choose and use their own selection and option. [12]

Organizations find a variety of different assumptions for their mobile device policies:

- It was not long ago that a mobile phone was just a phone; however today, they are advanced smart devices with a wide array of uses and form factors.
- If employees had BlackBerry devices, then their management needs could be satisfied by BlackBerry Enterprise Server (BES).
- In the past, when the only major mobile request was email, Microsoft Exchange ActiveSync(EAS) provided basic controls.
- Companies still regard mobile devices as accessories, rather than significant IT systems and assets.

2.4. Terms of Acceptable Use Notifications and Disclaimers

Organizations define and enforce Terms of Acceptable Use notifications and legal disclaimers to ensure all users and related parties, read, understand, accept and agree to the appropriate handling and usage policies about IT assets.

Comprehensive policies can block risks and leverage benefits BYOD provide by defining the rules of the program, considering regulatory compliance and conforming company security standards. It should also protect personal information stored on personal devices and prevent them from disclosure. Terms of Acceptable Use notification, is agreed upon procedure by IT departments, executive levels and legal parties to ensure all concerns are heard and all needs are met. [17]

For software applications, administrators can set Terms of Use version numbers, create language-specific copies of the Terms of Use, and set a grace period to remove associated apps if the Terms of Use is not accepted. When users launch these applications from enterprise App Catalog, they follow an acceptance process and the agreement to access the application.

2.5. Non-Disclosure Agreements (NDA)

Employee-owned devices are recognized as a less secure storage for critical corporate assets and private data of individual's. [7]

Agreements for exchange of confidential information should always be discussed. These agreements protect confidential information while maintaining each involved party's ability to conduct its respective business, education, training, or visiting activities.

2.6. Service Level Agreements (SLA)

Service level agreements are essential and integral parts of modern business IT world and are defenders of consumer rights.

Service levels that can be acceptable for both sides should be written to SLAs in measurable terms. The most important key performance indicator of an IT organization is the ability to comply with its SLAs. [18]

2.7. Cloud Service Model and Multi-Tenancy

Organizations or sub-organizational units such as departments which are accepted as a single entity and cost center introduced as a tenant. With multi-tenant architectures, multiple customers occupy and utilize only one instance of same software. [19]

Multi-tenant applications serve different departments, divisions or branches of customers with one copy of application. MTA emphasize resource handling commonality and promotes shared database, shared processing, and shared hardware economies of scale to provide cost efficient computing.

Software-as-a-Service (SaaS) is a new model for cloud service delivery. SaaS introduces a running, out-of-the-box commodity hosted application like a web hosting or public web mail system. Such allocation reduces the time to deploy and initial cost.

2.8. Custom Branding

MTA achieves differentiation with custom branding to support each customer's needs. Customization typically includes user interface themes and rebranding. They can be discussed in support of multi-tenancy so different departments, divisions or branches of any enterprise can have their unique look and feel at their organization group level. [20]

Software environment should be easily customizable to support additional languages, time zones, work hours, holidays and devices for detailed definitions of sub-authority zones.

2.9. Regulatory Compliance, Computer Forensics and Key Escrow

Organizations have obligations and formal rules to conform, guide lining specifications, and standard policies, and commitments to laws. Regulatory compliance describes the objectives that enterprises pursue and achieve to comply with relevant laws and regulations. [7]

Mobile computing comes with additional challenges to the digital forensics, and adds complexity to cybercrime investigations. Law enforcement agencies utilize computer forensic tools and receive trainings for new cloud ecosystems and help organizations and individuals to reduce security risks. [21]

Key escrow is a fair crypto-key exchange or crypto-key recovery management, and is a part of lawful interception in which the encryption keys are handled and pass through under certain legal circumstances.

2.10. Mobile Device Management (MDM)

Mobile Device Management is a capability that consists of the enterprise infrastructure software to secure, monitor and support the increasing number of mobile devices. MDM can also be defined as the policy and configuration management tool for smartphones and tablets. MDM helps enterprises manage things like network connectivity, the security parameters associated with a given device, hardware and software. [22]

MDM solutions are core components and integral parts of the BYOD strategy and frameworks. Understanding the different areas of managing mobile devices is important when designing the BYOD solution. [16]

Overall MDM lifecycle stages are enrollment, initial configuration, establishing and enforcing security policy, remote management of mobile resources, continuously monitoring and decommissioning devices. Each stage has unique requirements and questions for us to consider when planning the complete solution.

MDM starts with the initial enrollment and registration of devices into a new ecosystem and solution framework. Simplicity, ease of registration, and enrollment are the key factors for success in the MDM lifecycle.

Device enrollment in MDM solutions are typically initiated in two ways: [23]

- Administrator-managed enrollment
- User or owner self-enrollment

Centrally managed enrollment is used for bulk enrollment of multiple devices using messaging and pull mechanisms where devices are automatically triggered to enroll in the MDM solution. This is the primary option to enroll many devices into MDM solution at once.

However typical BYOD scenarios use self-enrollment where the device user or owner enrolls their device in the MDM solution. This type of enrollment uses a "push-based” mechanisms when the user tries to connect to the corporate network or resources.

Organizations aim for a variety of different MDM lifecycle functions:

- **Forced PIN –** Enforcing a PIN lock is the basic but also powerful step preventing unauthorized access to an unattended device. Complex passwords can also be enforced by an MDM, preventing several types of brute-force attacks.
- **Jailbreak/Root Detection** – Jailbreaking and rooting illegally alters official device software and render them into unsupported configuration. MDMs can detect such bypasses and prevent corporate access.
- **Data Encryption** – Recent devices have embedded crypto capabilities integrated into operating system. MDMs can utilize that function to support data encryption for privacy and isolation.
- **Selective Data Wipe** – Lost and stolen devices must be immediately wiped, (user initiated, admin forced, partially, complete) with the MDM.
- **Data Loss Prevention (DLP)** – MDM with DLP prevents uncontrolled data ingress and egress to and from corporate resources.
- **Application Tunnels** – Secure connections to corporate networks can be established by MDM layer.

In recent years, IT industry has even started to expand the definition of MDM to a broader set of capabilities that are rapidly becoming known as Enterprise Mobility Management (EMM). EMM includes things that start to move into the mobile application management space and mobile content management. They are even expanding to more traditional compute devices such as personal computers and Apple Macs as well.

2.11. BlackBerry Enterprise Server (BES)

BlackBerry Limited, (earlier Research in Motion), is the first and most inventive mobile device, smartphone and management software vendor. BlackBerry Enterprise

Server (know as BES) was the first and only middleware software solution focused on MDM technologies. BlackBerry introduced “email push technology” for only BlackBerry wireless devices and mobile phones. BES connects to messaging and collaboration backend of enterprise networks and redirects emails instantaneously to mobile devices. BES smartphone integration also provides seamless VPN to corporate internal network, remotely accessing files, and resources on the corporate intranets.

BES offered MDM support for iOS and Android devices recently, but it was not enough for competition with specialized MDM vendors. [24]

2.12. Microsoft Exchange ActiveSync (EAS)

Microsoft Exchange ActiveSync commonly known as EAS, included with Microsoft Exchange Server since 2003 SP2 and with Office 365 since inception, can provide secure connectivity to emails but can also do so much more.

EAS is optimized for high-latency and low-speed networks. EAS is using HTTP protocol and XML schemas, for accessing Microsoft Exchange server information stores. EAS is primarily used to synchronize mobile email, calendar events, and contacts with Microsoft Exchange server. When properly configured and certified, ActiveSync can also provide the foundational MDM features mentioned in MDM section. EAS is supported by universal WebDAV and should be used over HTTPS.

EAS delivers the baseline tools necessary to begin BYOD enablement programs for IT organizations. EAS not only support Windows Phone, but iOS, Android, and BlackBerry platforms without any agent software installation pre-requirements.

Policing capabilities provided by EAS:

- **Remote wipe** – User or admin started
- **Encryption** – SSL transmission, encrypt storage card, require device encryption

- **Password Policy** – Min. Length, complexity, allow simple, expiration, enforce history
- **Bandwidth Reduction** – Allow attachment download, maximum size

One additional item to make mention of which is natively available in Exchange 2010 and up is the ability to Allow, Block or Quarantine (ABQ) devices attempting to connect to any organization's infrastructure through EAS. This function allows IT departments the ability to allow approved devices, block devices that do not meet the specific requirements as agreed to by the organization, or to quarantine, in essence await access approval, devices pending further investigation around device capabilities.

2.13. Apple Device Enrollment Program (DEP)

Apple Deployment Programs (ADP) help IT departments for mass deployment and baseline configuration via Apple Device Enrollment Program (DEP). DEP is valid option for only devices and computers that are purchased directly from Apple or participating Apple Authorized Resellers or carriers.

2.14. Mobile Application Management (MAM)

Unlike MDM which looks at device management, MAM is adapting, provisioning, managing, monitoring and removing enterprise software applications and critical data on mobile devices. With MAM, applications are isolated within their own sandboxes or containers and policies can be set around these isolated applications. Most popular approach today to MAM is through application wrapping. Typically, application wrapping enables IT to insert policies without changing the way that the application works. [25]

IT departments can also decide to enforce a PIN for access to specific applications, dictate which applications can be used to open attachments and limit an employee's ability to copy and paste between applications. They can even intercept a communication and force it through their network, VPN or prevent it from going through to a given application.

Enterprise application catalogs or “internal app store portals” are essential and core component of an organization’s MAM solution. An enterprise app store is an internal software catalog that which authorized users can access, download and install pre-approved software or e-books.

Enterprise in-house application stores balance usage and synchronize contents of Apple's App Store, Google Play and Microsoft Store. IT departments can manage desktop, mobile, cloud and end user license agreements, as well as control over security by establishing corporate app stores.

MAM simplifies management of the mobile apps by pushing them to the user devices for installation, collecting license usage information and updating them regularly. [26]

Public app stores can be perceived less secure software catalogs next to enterprise in-house application stores. Apple and Google app stores delivering around two million different applications and it is hard for IT departments to ensure the security and suitability of every app that employees download. [27]

Beyond these defensive reasons, organizations may find a variety of benefits from enterprise app store:

- By controlling apps and licenses, enterprise app stores can reduce costs. With detailed internal app ratings, IT departments can eliminate license costs of apps that are criticized.
- Integration with Apple App Store offers mass distribution with Apple VPP.
- Enterprise app stores can report user name, date, time and usage summary for IT regulations to ensure application of corporate security policies.
- Enterprise app stores can even provide Role Bases Access Control (RBAC), thus apps are only accessible by approved personas.

2.15. Mobile Content Management (MCM)

Mobile Content Management (MCM) is also referred to as MIM (Mobile Information Management), enables mobile users to securely access, edit and share information with other users across devices and locations. MCM is a growing trend to manage critical content outside of corporate repositories as well as mobile apps. [28]

Many public file sharing sites are available for people frustrated with conventional FTP and business oriented SharePoint Portal repositories. Apple iCloud, Dropbox, Microsoft OneDrive and Google have all managed to attract end users with their usefulness and usability. While these sites and services provide a way to collaborate, they tend to leave IT departments out of the equation as IT cannot control any of the data on the cloud.

End users tend to use these sites and services without asking IT departments for permission. If file sharing is in the cloud, IT departments need to concern for the legal aspects of the data as well due to the laws of that country, wherever the date center is, apply. [16]

Organizations look for some fundamental roles of MCM function:

- **Content access** – Preliminary function to access a back-end repository.
- **Content push** – Push file distribution, push file replacement and push item deletion.
- **Content security** – Client-side restrictions for storage, crypto, sharing and copy-paste.
- **Policy enforcement** – Implementing and administering file level protection, sharing, authentication, encryption and restriction policies are integral parts of BYOD infrastructures.
- **File-level protection** – EMM tools can compensate DLP and IRM solutions.
- **Integration** – Compatibility in mobility for third party systems and enterprise infrastructures.

Unified communications (UC) platforms are also collaborative and complimentary standpoints of an organization MAM solution framework. UC is popular definition of instant messaging as a real-time enterprise communication service integrating Voice over Internet Protocol (VoIP), webcasting, webinar, remote desktop sharing and speech recognition. [29]

UC is usually spreading across multiple software and hardware products, devices and media types. Voice over Long Term Evolution (VoLTE) can be used for calls over the data connections of cellular wide-area networks as an alternative to the cellular legacy circuit-switched voice technology. Over-the-top (OTT) applications, softphone clients and handset VoIP clients provided by cellular service providers enable inexpensive VoIP calls over cellular data connections.

Microsoft has rebranded UCS and then Lync to "Skype for Business," updating several user interface components and internal parts. Transition has resulted the consumer-based Skype and enterprise-based Lync closer to uniformity. Skype for Business enables secure communications for smartphone, laptop, tablet and tele-conference systems anywhere with Internet access. [30]

Skype for Business supports Citrix XenDesktop and XenApp, Microsoft App-V and Remote Desktop Protocol, and VMware View Virtual Desktop Infrastructure (VDI) technologies. Desktop media including voice and video is supported in VDI environments where the thin client has a USB video camera and audio device, such as a headset or handset. Lync Room System Edition is designed by Microsoft and developed as a native Skype for Business client. The Skype for Business client is available for Windows, Mac, iOS and Android OSs and as a browser-based client for Skype for Business Meetings.

2.16. Enterprise Mobility Management (EMM)

When combined, MDM, MAM and MCM we get comprehensive Enterprise Mobility Management or EMM, which brings together the best of device management, application management and file management under one roof.

Enterprise mobility management (EMM) suites consist of policy and configuration management software and tools. They provide a framework of application delivery and integrated content management for mobile platforms. They are inheriting from MDM products and also compensating lacked features of application and content management. [31]

Organizations score and choose EMM suites which allow the following use cases: [27]

- Scalability, cloud architecture and SaaS deployment compatibility
- IT administration overhead, training and usability requirements
- Access control to services using central IM
- Mobile device configuration management (MDM)
- Hardware and application inventory (MAM)
- Mobile app distribution, installation, update and removal (MAM)
- Mobile app config and policy enforcement (MAM)
- Troubleshooting, remote help and support (MDM)
- Remote control and remote wipe (MDM)
- Content access, collaboration and distribution (MCM)
- Mobile content management and integration (MCM)
- Audit and reporting capabilities of who did what, where and when (MAM)
- Support encryption, MFA, DLP, IRM and risk management policies

This is not a comprehensive list, however ensures that IT organizations have all the items on here as a minimum to a successful BYOD solution.

Some EMM vendors pay more attention to security while enabling enterprise mobility. Some vendors focus largely on device management functions, while others focus mainly on managing and securing applications. EMM suites are conceiving mobility and gaining deep insight. Consequently, EMM suites will cover and incorporate every aspect of evolving mobility.

EMM solution helps IT organizations respond to new mobility challenges. It enables end users with a modern digital workspace, provides line of business with an agile platform and competitive advantage, and strengthen their IT team with the complete mobility platform. [21] Enterprise mobility use cases, motivate individuals and encourage organizations by enabling new ways to empower people and transform organizations.

Competitive agility, operational efficiency, innovative and creative customer engagements are important organizational advantages of business mobility. With the EMM in place, business mobility gives line of businesses with new powers to innovate. End-user and enterprise expectations reshape EMM suites to fit into a centralized and simplified cloud-ready architecture.

2.17. Central Identity and Access Management (IAM)

Identity Management (IM) is a new industry trend which focuses on identities of persons and devices. IM also centralized policies that relate to identities and their activities. IM can use LDAP servers as a backend to store its data, it can have specific set of schema that defines IM objects and their properties.

Having only purpose-required entry types and correlation points place IM as relatively flat and simple directory tree. It has rules and limitations for a specific purpose, which is managing identities. [32]

There are some differences and similarities between standard LDAP server and IM platform due to their use cases and project intentions. A directory service is a highly specific information store and consists of generic services that can store, retrieve and distribute any kind of information such as computer names, user accounts, organizational units and groups.

LDAP servers are collections of generic objects relative to real world entities. Collections are aligned with schemas that represent user accounts, machine names, network definitions and departments. LDAP directory servers are highly extensible services and frequently facilitated as central authority for other applications in the same environment.

Using hierarchical structures such as a directory trees, root, intermediate and leaf entries is a common way to organize information with LDAP schemas. LDAP directory servers are known for their generality. LDAP directory servers are very capable of powering other enterprise applications. [33]

For many organizations, Microsoft Active Directory (AD) or standard LDAP directory servers are playing the central authoritative role in coordinating identity and access policies. Generic LAN use cases are practiced repeatedly and working well inside a closed security perimeter. However, as the number of cloud-based applications grow this model need to be changed accordingly.

IM platforms have highly specific purposes, limitations, practices on dedicated task areas. Restrictions on the central identity give it administrative simplicity. Clear role definitions and task controls made them easy to integrate exiting processes. Enterprise wide single sign-on services and identity/authentication functions are easier to accomplish with IM platforms than with LDAP servers.

2.18. RBAC and Complex Authorization Models

A persona was once thought to be only a marketing tool, having origins in the world of marketing. It was used as a tool to categorize customer segments beyond the traditional methods with the expectation of more detailed customer experience and feedback. Personas are used to aid strategists, enterprise architects and senior leaders in learning how they can offer more engaging digital services, campaigns and user experiences. However, as personas proliferate within marketing organizations, the value of personas can potentially be diluted. Personas, if used appropriately, are a powerful diagnostic deliverable that enterprise architecture (EA) practitioners can use to make decisions, take actions and provide recommendations, whereby increasing understanding about many people through abstracting them into an archetype. [34]

Role Based Access Control (RBAC) is an operational model for managing access in a complex environment. Instead of determining and assigning exactly the entitlements needed by each and every user, and adjusting those assignments as circumstances and job responsibilities change, cohesive sets of entitlements that represent patterns of usage are assigned to named roles. Users can then be associated with roles to get the access they need in a more efficient manner than is possible with managing individual entitlements. Most RBAC systems are designed with the expectation that users will be associated with multiple roles, meaning that users are granted the sum total of entitlements belonging to the roles with which they are associated.

Roles help to simplify the administration of systems with complex authorization models, but they are not always the only factors involved in determining the specific access for user’s attributes often play a role in determining access as well. For example, an entitlement might be defined to allow access to orders only within a user's region. This means that the results of the authorization involving this entitlement would depend on the value of some attribute associated with the user. A user in Europe would have access only to European orders, and a user in the U.S. would have access only to U.S. orders, even if both users were assigned the same role that included this entitlement.

2.19. Multi-Step Verification Techniques and Single Sign-On (SSO)

Most applications start with a standalone model where users and their credentials are created, stored and managed within the application itself. Each application the enterprise adds to its portfolio also adds to these identity islands. Dealing with multiple applications and guest users becomes a hassle both for the end-users and for administrators fielding all the issues from password resets to account lockouts.

Storing confidential information on cloud systems are gaining popularity due to advancements and improvements in internet and mobile communications. Hackers always find easy to capture static, weak and guessable passwords with brute force attacks. Multi step verification techniques has been developed for hardening the security by requiring additional information with basic user name and passwords.

One Time password (OTP) can only be used once and automatically invalidated after its use. It can be part of additional step of verification such as OTP calculator device or SMS and prevent drawbacks of static password authentication. [35]

Google Authenticator, Microsoft Azure Authenticator or Okta soft tokens are featuring simplicity and accuracy for BYOD administrators. Self-configuring, ready to use soft token apps are available through Android and Apple App Stores. They can use device camera, QRCode, expiry-based One-Time-Password algorithms and used as MFA for protected resources.

Generic security questions can always be used for extended level of protection. They require users to supply additional authentication data and they require no hard tokens and user intervention.

Active Directory can be used as Single sign-on (SSO) user authenticator for local network services and provide consistent experience for users. Users log in to the domain once and automatically granted access for consequent requests. [36]

2.20. Strong Multi-Factor Authentication (MFA)

Multi-factor authentication and virtual private networking for enterprise mobility have been introduced for mobile apps that involve sensitive personal or corporate data. New regulations and legislations, have also involved and established to ensure delivery of secure applications. [35]

Due to the insufficient measures within mobile applications, a new security perspective and solution has to be developed which coordinates multiple protection technologies, standards and system components.

MFA is designed to protect infrastructures from several kinds of attacks that use stolen, lost or weak credentials. MFA requires users to supply additional proofing with primary credential, something he or she is, has, or knows, before final authentication. With MFA, a stolen password is not a problem. Sensitive information is protected from unauthorized access by requiring an additional factor.

Extending MFA protection to new applications and adding new users is complex, so scaling implementations is difficult without modern IM solutions. Building one-off point integrations is prone to creating coverage gaps as administrators either forget to enable, or are unaware MFA protection is required for new resources. Legacy standalone MFA products are hard to implement. IT departments need to integrate the MFA product with each application and system individually. With standalone MFA products, organizations are dependent on applications and systems supporting vendor-specific integrations, inhibiting broad MFA protection for all apps and resources. [37]

As more organizations adopt cloud applications, they are finding many cloud apps do not support built-in integrations for their MFA vendor. Instead these cloud applications either do not support MFA, or use a native mechanism such as SMS-based passcodes or security questions. This adds confusion for end users who have to navigate separate credentials, and separate MFA factors for the various applications and services they access.

Apple offers two-factor authentication option to its customers for additional Apple ID account security even if someone else knows their passwords. At the first entry of Apple ID a verification dialog appears and asks six-digit code which is shown automatically on trusted Apple device. [38]

Two-factor authentication is built directly into Android, iOS, macOS, Google and Apple official web sites and currently available to users with a smartphone or internet device. They are forcing two-factor authentication for several critical tasks to improve security.

2.21. Identity as a Service (IDaaS)

Identity as a Service (IDaaS), Federated Single Sign-On or Identity Federation is a new common approach when the organization wants an application to rely on an existing cloud identity provider. In a federated scenario, rather than authenticating a user within the application, application establishes a trust relationship with the organizations' chosen external or internal identity provider and allows any user authenticated through the identity provider to have access to their application. [39]

For example, if the application relies on Facebook or Google as the identity provider, any user with a Facebook account or Google account who has been authenticated through Facebook or Google will have access to the application accordingly. This identity provider may be another trusted application, a connection broker, a single sign-on solution or any other system that is aware of all the users and has the ability to authenticate and maintain an authenticated session. [32]

Another way to centralize authentication is through delegated authentication. In a delegated authentication scenario, a user is still being authenticated in their application. Instead of using local credentials in the application, organizations would like to leverage user credentials residing in an existing identity provider.

Which is different from the federated use case is the application entitles access to a user based on a validated account with the identity provider. With delegated authentication, users are authenticating directly to the application itself. The validation of user credentials is simply delegated or outsourced to an existing identity provider.

Security Assertion Markup Language (SAML) has been the most widely used standard for implementing federated single sign-on and/or delegated authentication. In the SAML terminology, the identity provider authenticates the users for the relying parties. In this case, the application is the relying party integrated with the organizations' identity provider of choice. [39]

In a typical implementation, the vendor would send a request to the identity provider containing the user and relevant credentials to be authenticated by the identity provider. The format of the message should be determined by the application and made available to identity providers in order to implement the appropriate integration.

2.22. Microsoft and Third-Party Certificate Services (SCEP)

Strong security requires IT to verify that users and devices can be trusted to access the company network and its applications and data. Even if IT strictly limits the applications available to users, authenticating users is still a priority.

Digital certificates represent stronger form of validation than static passwords or shared secret credentials. Digital certificates are recognized as common standard for higher security, authentication, digital signature and trust relationship between enterprises, government organizations, and digital communities. [40]

Critical assets protection methods of digital certificates:

- **Authentication** – Computer name or user account identity validation.
- **Encryption** – Encoding stored and transmitted data for eavesdropping.
- **Digital signing** - Computer equivalent of a hand signature.
- **Access control** – Authorizing data, handling method, user, date and time.
- **Non-repudiation** – Ensures persistent transactions, irrevocable legal exchanges.

Simple Certificate Enrollment Protocol (SCEP) has been used for years in Virtual Private Network (VPN) environments in order to facilitate certificate enrollment and distribution to remote access clients and routers.

The enablement of SCEP functionality on a Microsoft Windows 2012 R2 server requires the installation of the Network Device Enrollment Services (NDES) and utilizes existing Microsoft certificate infrastructure or imports third party certificate management systems to be managed for BYOD deployment.

2.23. Microsoft Workplace Join

User expectations and growing demand for accessing online services independent from time and place is the most important motivation mobility transformation. Thus, IT departments are facing with new security challenges accessing to internal resources that was only possible from enterprise owned and Active Directory member computers.

Microsoft Windows Server 2012 R2 and Microsoft Windows 8.1 addresses this new challenge of BYOD and features management function for that, which is called Workplace Join. [41]

Microsoft Active Directory Federation Service (ADFS) role is required for Microsoft Workplace Join to work with the new Device Registration Service. Device that runs Windows 8.1, Linux, Apple iOS and Google Android operating systems can perform Workplace Join.

User accounts can also enroll to Windows Intune device management cloud option, to gather managed access to applications and links to public app stores.

2.24. DDI (DNS, DHCP, IPAM)

IT Infrastructure and operations personnel use DNS, DHCP and IP address management (IPAM) solutions to improve network availability, reduce operational expenditure, and simplify and streamline administration of BYOD infrastructure. Gartner Inc. called the term “DDI” when they released their first MarketScope report in 2009.

DDI consists of DNS, DHCP and IPAM solutions that help organizations manage their IP address space, DNS and DHCP services to improve overall availability and reduce operational expenditure, thus facilitating scalability to support business growth. Increasing number of IP addresses needed for modern networks and complex metadata about them bring attention and great importance to IPAM. [42]

IPAM defines the resource database by metadata and brings the results into a centralized, authoritative facility. This is an important business and regulatory requirement for many dispersed organizations.

2.25. Software Defined Networks (SDN)

Software-defined networking (SDN) technologies include overlay or network virtualization, as well as the full separation of control and data planes, moving the intelligence from routers and switches into software modules that can run several controller programs at once to make better decisions in packet routing.

SDN brings business agility at designing, building and operating phases of a network infrastructure, and lowers capital expenditure and operational expenditure. SDN solutions include an abstraction of network topology that allows a single control point for the network and a centralized controller that uses one or more device control protocols to communicate with the infrastructure.

2.26. The Domain Name System (DNS)

Domain Name System (DNS) is a disperse IP resolution and conversion system for computer or service names of any networked object. DNS associates meta information with fully qualified domain names assigned to each entity and it is used by every client on the network as a locator of other systems.

DNS is one of the oldest protocols on the Internet, being over 30 years old. DNS was designed to be robust, hierarchical, and distributed. All activities in the network today are dependent on DNS to resolve IP addresses into a human readable and useable naming scheme.

PCs, laptops, tablets and also application servers are generating DNS queries for resolving each other's addresses in enterprise networks. Each end can have some service problems and this can lead the situation into severe failure. [18]

And with the introduction of IPv6 into today's enterprise networks, the need for naming schemes versus IP will only get stronger. Introduction of hard to learn and remember IPv6 addresses are bringing complexity and massive increase in DNS queries.

DNS hijacking redirects the resolution requests to a special responder for BYOD case, to a welcoming page or guest registration site known as captive portals. Hijacking mechanism monitors traffic for DNS requests and redirects them to a captive portal where the user self-registration occurs.

2.27. The Dynamic Host Configuration Protocol (DHCP)

Every item operating in the IP network must have a valid IP address before joining the topology. Special hardware and software appliances called Dynamic Host Configuration Protocol (DHCP) servers, provide services for automatically obtaining valid IP address from the network. Every time a new object joins the network, it will discover, request and obtain an IP address from a DHCP server.

DHCP is the critical component that IT departments need for a large workstation environment is an automated way to distribute IP addresses and update network parameters which happens before the computer boots. Highly customized client information and automated system configuration for all or parts of a network usually depends on well-managed DHCP servers. [18]

In a BYOD scenario, DHCP infrastructure is vital by providing the correct IP address and other critical supplements such as the DNS and NTP server IP addresses.

2.28. The Network Time Protocol (NTP)

Accurate timing and signaling correct date to systems are carried by the Network Time Protocol (NTP). Server hardware and device clocks will be inaccurate and unsynchronized without a NTP server. Digital clocks which are typically based on mainboard circuits have tendency for drifting. Drifting several seconds per day can accumulate significant errors over time. [43]

Distributed computing, network infrastructures, mission critical operations and commercial applications are prone to problems of time synchronization and strictly require a professional NTP solution. NTP servers act as central and accurate time source and all of client devices sync their times with it. If highly accurate timing is a requirement for the organization then they can choose a high-end NTP appliance that synchronizes time from internal Rubidium atomic oscillator or another official source, such as the GPS or GloNAS satellite broadcasts.

2.29. Application Proxy Servers

Web Application Proxy (WAP) servers are intermediate software layers which provide gateway, cache or connector services for clients accessing resources from remote servers. WAP servers collect file, data, web or e-mail requests from clients, forward the requests on behalf of them, cache the returned data and deliver results to clients. WAP servers evaluate the request and utilize the cache facility and never access directly to the same resource for different clients again. WAP servers simplify control of connections and provide bandwidth reduction and connection throttling.

WAP can run and be deployed in several topologies. WAP can run in the local network or in DMZ, acting as a cache proxy, DoS protection or isolation member that securely transmits requests from BYOD clients to the organization's critical enterprise infrastructure components.

WAP provides a protection layer against malicious user or HTTP requests that originate from the clients through the following features: [44]

- **Preauthentication** – Ingress and egress flows are always authenticated.
- **Network Isolation** – Direct access to backend or proxy bypass is forbidden.
- **Selective Publishing** – Application, URL or path whitelisting or blacklisting.
- **DoS Protection** – Undefined or malicious traffics terminated at WAP.

Depending on network configuration, IT may require a proxy server that allows mobile devices to receive certificates using an Internet connection and without directly connecting to their internal corporate network.

2.30. Wireless LAN (WLAN)

Wireless access to corporate resources is typically provided as an on-premises network extension service for devices that are in close physical proximity to the on-premises network. Growth in the number and types of devices that will connect to the enterprise will force network planners to design and provision wireless solutions at the

LAN access layer in ways that differ from current practices. Employees will be connecting their smartphones, tablets, notebooks and laptops to the enterprise WLAN, expecting to be able to access their business applications, communication and collaboration tools, and their private social apps. [16]

This usually involves allowing mobile devices to connect to network resources as users roam from location to location in an on-premises campus, such as conference and meeting rooms, different offices, or other on-premises areas. It can also include wireless access from remote locations over non-corporate managed wireless network access points, such as the user's home network or a public wireless access point.

Ease of connectivity is an integral part of wireless networks. IT departments usually maintain wireless connections using predefined profiles that streamline the settings for devices and users. Wi-Fi profiles usually include custom network name, Service Set Identifier (SSID), security settings, web proxy, and ad-hoc connectivity for wireless devices in range.

Using WPA2 Enterprise with Transport Layer Security (TLS) for authentication is also important. If TLS support is not available, Protected Extensible Authentication Protocol (PEAP) should be the next option. WAP servers can also provide control for the Wi-Fi connection and places additional protection layer. [18]

Multiple SSIDs complicate life for IT departments and users alike. With effective policy management enforcement in place, BYOD and corporate-owned devices can connect to common SSIDs. Consolidation of SSIDs can also improve Wi-Fi performance. Wi-Fi auto join prevents user from intentional SSID selection and advisable WLAN usage. When personal devices are connected to a common 802.1X network, IT can provide Internet only access if appropriate.

2.31. Virtual Private Networks (VPN)

High security mobility management is a subset of the EMM that serves organizations with the most stringent requirements if security is the highest priority.

A VPN connection is the indispensable way for the modern workers and the first step for secure remote access of corporate resources. [18]

Secure remote access to corporate resources often requires using a VPN connection from mobile devices and includes the installation of a VPN application on the mobile platforms. Modern mobile VPN applications usually use digital certificates or IM credentials to authenticate the VPN connection.

IT departments also manage these connections using VPN profiles for ease of connectivity and user satisfaction. Supporting VPN connections with the EMM solution may be an option with certain VPN platforms.

Mobile VPNs are essential to keep data in motion private and safe from hackers, and to continuously verify the trustworthiness of remote connections subject to Man in the Middle (MITM) attacks. Vendors are expected to have strong validation for VPN sessions and to support several methods of VPN operation. VPN can include manual start/stop, activation by domain, activation by an app or container, known as per app VPN or location aware VPN. [45]

SSL and IPsec are two main types of VPNs that are available for enterprise usage and infrastructures. In the context of the BYOD trend, SSL VPN technologies are based on HTTPS protocol and use web browser as a client application which brings granular security control, solves many problems of IPSec and enables mobility.

Specific apps or particular user can utilize SSL VPN and precisely controllable by IT departments. End user applications and their requirements determine the VPN selection. Browser based SSL VPN supports most devices and platforms and provide compatibility for BYOD scenarios. For granular account management and greater flexibility, organizations can choose hybrid VPN technologies.

2.32. VLAN Isolation and Micro Segmentation

Manageable layer 2 (L2) ethernet switches are usually employ virtual LANs or VLANs for isolating network ports into virtual broadcast domains. Separating networks offers traffic containment within a port group, and segmentation provides security by restricting endpoints in different VLANs. [46]

Software defined data center (SDDC) is a new and noteworthy concept that covers operational IT agility, fast infrastructure deployment and organizational efficiency for other areas of improvement such as Software Defined Networks (SDN).

VLANs and routers are used for network packet broadcast containment within a unique IP subnet of hosts. Where customers build their SDN with the automation they have discovered some significant security benefits from micro segmentation of enterprise data networks. [47]

Security strategies which focused on network perimeter has proven to be weak and modern attackers pass this perimeter only defense in minutes, exploiting authorized users, then moving into the data network from computer to computer with little or no controls to block their propagation. Most network security mechanisms use isolation and it separates guest, test, and production VLANs.

Multi-tier virtual networks use segmentation as an isolation mechanism. Traditional network protection employs firewall and routers, and uses ACLs for allow or deny rules to manage traffic between security zones. BYOD environments require advanced network security practices where organizations can employ SDN platforms to demonstrate such services.

2.33. Network Access Control (NAC)

Network Access Control(NAC) is an advancement to computer security that attempts to give a verdict for endpoint supplicants, such as antivirus status, client intrusion prevention, firewall settings and finally vulnerability assessment. [32]

IEEE 802.1x is the standard way to user or system authentication and network security enforcement. NAC standards permit or forbid host connections on wired or wireless network layers.

Higher IT maturity levels require organizations to use and benefit from more sophisticated authentication mechanisms such as IEEE 802.1X, WPA2 Enterprise and public key infrastructure as well. When the user takes the right of initiative, IT should also provide adequate training for self-sufficient support requirements.

Manageable Ethernet switches that support 802.1x keep connected host in quarantine from the network while performing some kind of checks and pre-authentications. Depending on final authentication verdict, traffic is permitted, or the host is denied access to the network. [48]

2.34. Apple Push Notification Service (APN)

EMM for Apple devices uses the push service to locate and notify the device of changes to the MDM policy. In addition to inbound sessions from the users and devices, the EMM needs to establish outbound connections to the Apple push servers. Apple refers their service as the Apple Push Notification Service and requires an Apple signed certificate to authenticate the MDM sessions.

Remote notifications feature of Apple products such as iOS, watchOS, tvOS, and OS X depend on APNS. Device information advertisements and change notifications are distributed via push based Apple cloud services. APNS and Apple devices communicate over encrypted and persistent IP connections starting from initial product activation. [49]

Google refers to their service as Google Cloud Messaging for Android (GCM). This service replaces the older Cloud to Device Messaging Framework (C2DM). Both Apple and Android incorporate the push service into the device's operating system to allow the MDM server to communicate with the MDM client application.

Apple devices also allow the MDM to communicate with the OS MDM API with the appropriate credentials. Both require the end user to establish an account with either Google or Apple respectively. This account effectively binds a device list to a user.

2.35. System Information and Event Management (SIEM)

Security information and event management (SIEM) technology leverages threat detection for security incident response by collecting and correlating real-time logs and historical analysis of events from a wide variety of data sources.

SIEM collects end analyze events from different sources and delivers comprehensive reports for incident handling and administrative dashboards. [50]

IT organizations consider SIEM deployment as a central log management, user access and resource monitoring, threat mitigation, security incident response and compliance reporting. It may also require SIEM integration with data sources that provide context for security monitoring, such as user directories, configuration management databases (CMDB) and vulnerability scanning products.

Organizations should document their network and system deployment topology, anticipate deployment growth and analytic requirements and, estimate log volumes and event rates for possible BYOD topologies.

2.36. IT Asset Management (ITAM)

The IT asset management (ITAM) process collects, processes, stores and reports data associated with the IT asset life cycle.

Simplified tracking of contract terms and conditions, costs controls, system ownership, vendor management, monitoring service, support and warranty periods and user entitlements with inventory items can be accomplished by ITAM. Integrating physical, financial and contractual data into a central data hub supports functions for managing and optimizing a software and hardware asset portfolio.

ITAM is evolving from traditional inventory monitoring and asset reporting role to a core financial practice and critical IT management solution. Accurate and timely delivery of critical infrastructure component metadata via ITAM can be seen in higher IT maturity levels. [51]

IT departments usually search for location, usage, asset tag and warranty coverage dates of items and meta information about them. ITAM provides detailed search and retrieval of critical data, operational status and change management analysis to operation teams through the following meta information:

- **Server Team** – Device type, name, operating system, updates, services.
- **Network Team** – IP addresses, gateway, netmask, VLAN tag, switch port.
- **Operations and Facilities** – Licensing, support, maintenance contract renewal, ownership information, depreciation and warranty lifecycle.

2.37. Chapter Conclusion

BYOD is one of the new concepts that involves and refers organizations and employees on several aspects. Major cloud providers, hardware, software and integration vendors are now on this topic and BYOD is still gaining technical and practical attention from global IT industry.

Providing IT professionals and related readers with enough background and guidance in mobility issues is our technical and academic goal in this study.

Smaller and smarter devices are replacing notebooks and laptop computers for accessing applications and processing corporate data. Mobile devices are becoming smarter choices for enterprise IT departments while they are getting lighter, smaller and cheaper. They are also becoming more popular with low power consumption, processing efficiency for getting agile results. They can be moved from one place to another easily and not requiring new settings. Historically, many of these devices have been isolated on separate networks that use proprietary wired and wireless protocols. With the invention of more platform independent applications, price of the mobile device also reduced at lower costs that which every high-end application is also available on mobile network.

Especially in academic literature little can be found about consumerization of IT and BYOD. On the other hand, they became a popular subject for many market research institutes and industry business media focused on practitioners. Many of these media describe and analyze IT consumerization and its impact on businesses. The Fundamental architectural components and definitions above certainly acknowledge this; all describe the influence of IT consumerization on an enterprise.

3. ENVIRONMENTAL REQUIREMENTS AND INFRASTRUCTURE INTEGRATIONS

3.1. Legal Aspects of BYOD

Bring Your Own Device (BYOD) is an enterprise information technology that depends on consistent policies and user engagement to interact with enterprise IT infrastructure and access sensitive corporate data for work purposes. [52] Mobile devices are a cost of doing effective business, and the only way to get better results is to have a comprehensive policy for them. This chapter provides an introduction to the legislative planning steps required to deploy BYOD infrastructures and to publish applications through it.

Configuring and enforcing privacy settings to define how device and user information are handled is particularly useful in BYOD deployments. Management tools allow administrators to fully customize and assign a unique Terms of Use to each organization group. IT administrators can also create application based Terms of Use to notify end users when a specific application collects data or when it imposes restrictions. Organizations should inform their end users about how their data is collected and stored when they use BYOD infrastructure. IT administrators can create a customized privacy notification to inform their users about what data their organization collects from their enrolled devices. [15]

After examining historical and contemporary privacy matters we have discovered domestic and international legislative approaches to sensitive personal information, thus we have identified that in general, it is not appropriate to collect telecom data, GPS data, application usage information, display user information such as first name and last name and to push unattended remote commands for employee owned devices.

This is because private apps may be installed on a device, and if viewed by IT administrators, can be considered personally identifiable information.

Support capabilities, training, and constantly deployment must have priority over other aspects while planning and programming BYOD security in corporate IT management policies. [53] Organization should explicitly mention sensitive issues in their Terms of Use agreement and may work with their legal department to determine what message about data collection they should communicate to their end users. While compliance policies can be set up to help enforce Terms of Use, IT administrators can view a summary page of exactly who has and has not accepted the agreement. Then, if necessary, legal department can contact those individuals directly. [54]

At the other hand, Software as a Service (SaaS) model has been widely supported by EMM vendors and newly used by customers. Most EMM suites have both on-premises and identical cloud offerings for efficiency and easy transition for multitenancy. Organizations evaluate, chose and use scalable, flexible multi-tenancy solutions for their support for exponential growth. With multi-tenancy, organizations create groups that function as independent environments and streamline the setup process by setting child groups to inherit parent configurations. Most EMM platforms deliver multitenancy features and control across different customer systems under same management framework known as SaaS. [14]

Some organizations working in regulated industries also require users to sign non-disclosure agreements (NDA) when dealing with data and devices. They need to consider the detailed requirements and enforceability of NDA with their personnel. External audit, regulatory compliance and fraud investigation situations demand computer forensic practices and these investigations should be conducted with or without user intervention and integrity of critical data should be safeguarded as well. Crypto key exchange, deciphering data and chain of custody issues should be carefully evaluated by organizations prior to BYOD implementation. [55]

IT departments should consider new and growing security risks and BYOD trends by reviewing their mobility plans and security policies. [32]

3.2. Empower Business and Improve Productivity with EMM Suites

Consumerization of IT and proliferation of mobility bring new expectations and new needs, such as BYOD brings requirements that span the enterprise, including those of end users, lines of business, and IT administrators. Users are accustomed to a consumer experience that is simple and convenient. They expect the same level of ease when working with corporate devices and apps that they experience when using their personal devices and apps. They also expect their privacy to be protected. Line of business managers provide the business with unprecedented opportunities and they are investing in mobility as a form of differentiation. By enabling employees to easily access their applications on mobile devices to get their work done whenever and wherever they are. [55]

User expectations have increased the pressure on IT to enable consumer grade simplicity for employees using corporate apps and content, across any device they choose, while ensuring enterprise grade security. When expectations are not addressed correctly, users come up with workarounds or implement shadow IT, which means rogue systems and informal solutions built and used inside organization without explicit approval, creating security vulnerabilities that leave sensitive corporate data exposed. [56]

At the other hand, when policies are stringent, user acceptance is always low. Also, users do not want to be left alone or unmanaged. They want transparency and freedom of choice. They want to know what is being collected, and they want to have the choice to opt out. Embracing BYOD is beneficial for organizations who have millennial employees, by meeting the mobility demands, realizing productivity gains and allowing their own devices in the workplace. [57]

With additional benefits, BYOD also brings new problems for organizations ahead of their existing discussion points. They must extend their security perimeter for new mobile devices and enhancing cloud computing. [32]

Moving high business impact applications and operations to mobile environments means critical intellectual property (IP) and information must be secured across a wide range of endpoints and the management and security challenges associated with enterprise mobility fall into the field of the IT. Successfully executing on a business mobility strategy creates tremendous opportunities for organizations, but it brings a comparable amount of risk, planning and requirement analysis. [7] Organizations and IT administrators should effectively manage a growing device population and protect corporate data on those devices as well. [58]

For this critical purpose, many devices now ship with built-in MDM functionality and MAM features such as profile and policy distribution, digital certificate assignment, application deployment, configuration and settings for multiple devices. MDM supported and managed devices include not only handheld devices, such as smartphones and tablets, but increasingly laptop and desktop computing devices as well. [5]

However, the real business requirements today are to go beyond MDM and into EMM. As businesses dive deeper into mobility, they are looking for the consolidated management approaches that only EMM offers. IT organizations are moving traditional PC management to cloud EMM platforms, and unifying management across all operating systems used to access business resources. BYOD devices and corporate-owned devices can be safely monitored, managed and protected by EMM suites. [59]

EMM suites provides seamless user experience for multiple devices, and it delivers security for high-business-impact applications, safely enabling BYOD and self-service capabilities. And it establishes a platform that scales to support new business processes. Individually, these gains are enormous and collectively, they can drive business transformation.

As part of this work, we examine the employees’ needs and the ways that they will be accessing company applications and data. Asking if they will be mobile or remote, what assets they will need and if IT will subsidize employees’ devices and monthly plans. We also need to decide how we are going to enable and control access to corporate assets, entitle policy, ensure compliance and support the end users on an ongoing basis.

3.2.1. The Rise and Fall of BlackBerry

Research in Motion Corporation has been a pioneer in MDM and mobile security markets. RIM dominated enterprise push e-mail market for many years. Back in the day when BlackBerry were everywhere, IT managed what they could do on them. But these were corporate issued and corporate owned, not BYO devices. If someone decided to part ways with that company, they also broke up with their phone. BlackBerry devices were only examples of delivering full status report after a complete remote wipe. BlackBerry has assumed pioneering role and delivered fundamental EMM functionality via BlackBerry Enterprise Server 10 (BES10). [60]

- **MDM** – BlackBerry, iOS, and Android devices can be managed.
- **Mobile Security** – Security settings and controls far beyond EAS.
- **Enterprise Application Management** – MAM for Apple, Google and BlackBerry.

Apple and Google have become the main player in mobility while many organizations allowing employees to use their own devices for work. BlackBerry has experienced a strong decline in its share of mobile device markets due to rapid end user transition to iOS and Android devices. BlackBerry has lost the dominant position and missed the recovery chance for enterprise segment and finally BES platform, faced devastating competition.

With the advent of Google Android and Apple iPhone and tablets, employees started to bring their own devices into work. Apple and Google developed a set of MDM application programming interfaces (API) that companies could write against to allow IT departments to manage these devices.

3.2.2. Accessing Information and Using Data

The first and most critical component of the contemporary business practices is the data that people need access to. As mobility and remote access expands user connection requests such as e-mail and teleworking also grows rapidly. This chapter shows how all these aspects have slightly different requirements but also much in common. [18]

Better availability, accessibility, and mobility of data in a cost saving perspective for organizations and employees can only be seen with growth of IT industry. [61] Bring Your Own Device is a new approach that allows employees to use their own devices, with the business or educational networks, and access on-premises services. BYOD is also a new paradigm shift that grants users to select, procure and bring their own electronic equipment and use them as their primary work tool. This will help improve cloud computing and mobile application market and eventually cost reduction. [9]

Working in geographically diverse locations, boosts user convenience and increases productivity and reduces information technology expense for organizations. [62] BYOD leverages personalized mobile business, removes restrictions of time and place, and allows ease of support, thus provides convenience and efficiency for continuous business operations. [22] Mixing personal and corporate workspaces for seamless access with multiple devices can be possible with BYOD. [53]

If IT departments made content available to their users via BYOD, they need to make sure that they can control the access of that data by users and applications. Ease of use and a well-defined identity infrastructure are very important and essential for users when accessing any resources or applications. IT has to strike a balance between ease of use and security. But just as important is the ability for each application to integrate with this infrastructure and with other applications. [58]

Technical support for multiple devices, operating systems, applications and conforming SLA are important IT requirements of a BYOD plan. Accessing enterprise applications and data from unknown devices can reduce security, affect device controls, and even utilize helpdesk resources. [61] Capturing application usage and account information helps IT departments to understand how the applications are being used across their ecosystem. Providing auditable and detailed reporting on user activities and permissions is also important in satisfying customer compliance initiatives. Executing these functions through MDM controls within platform OSs represented the early implementation of these functions. These tools have evolved to incorporate advanced MAM and MCM as well. The movement of management capability to applications, regardless of device control, represents the evolution from MDM to EMM.

Mobile device support and security policy enforcements can be maintained with EMM suites by IT organizations and service providers. One of the primary functions of EMM suites is to exploit and utilize special features of smart devices and to protect enterprise resources by policy enforcements.

Different strategies can be addressed and maintained for security-enabled enterprise mobility via EMM suites. [26] Some organizations focus largely on device management functions, while others focus mainly on managing applications and securing data. Consequently, EMM suites will cover and incorporate every aspect of evolving mobility. This is where integration of MCM and MAM gains importance.

3.2.3. Mobile Content Management for Collaboration

Content access and distribution are primary end-user motivations. MCM features help EMM suites to provide such baseline file sharing and offline syncing functionality as well. BYOD infrastructures employ MCM to manage content distribution and access on mobile devices. [53] MCM enables users to access content from their mobile devices. In this category, we look at the important MCM capabilities within the EMM suites.

Unified communication (UC) is typically the primary resource most users need access to on a corporate network, whether from a personally-owned or a company-owned mobile device. Accessing to email, voice and files is also the connection that triggers initial mobile device enrollment. Being able to manage messaging access for mobile devices across both existing non-MDM solution and the MDM solution helps avoid device coverage gaps and increases the protection for data stored on collaboration repository servers. [24]

MCM solutions provide email access by using one or both of the following features: [23]

- **Email profiles**: By setting up and deploying email profiles, administrators can automatically configure mobile devices with appropriate email server information for users to connect to their email mailboxes. This helps users connect to the correct email server and address books without having to remember the right email server endpoint names or network addresses. In addition, by removing an email profile, administrators can remove email and contacts information from devices as part of device reset or selective wipe process.
- **Conditional email access**: Managed-email access, typically focuses on security and compliance for accessing email on a mobile device rather than which endpoint the mobile device connects to. With conditional email access, a compliance policy is defined and assigned to individual users or devices or groups of users and devices. The policy outlines the prerequisites that have to be in place before a mobile device can connect to an email resource. For example, a PIN might be required on the device. The policy is typically enforced when the device first enrolls, but remains in place and active as long as the mobile device is enrolled in the MDM system.

Integrating EMM systems with content repositories enables administrators to deliver secure mobile access to corporate documents while managing document distribution and access permissions. This ensures the right content gets to the right employees without sacrificing the security of the documents themselves, which are distributed to mobile devices over encrypted connections. Files and documents usually are stored in corporate file servers and portals and synchronized regularly, so that the latest version of a document is automatically updated on mobile devices. To ensure storage and transmission security, users can be authenticated with strong passwords, MFA and certificates before accessing corporate content. Additionally, document metadata can be restricted on a per user basis. [54]

Advanced MCM tools require a good level of directory integration and IM platform for RBAC, records management, workflow and collaboration and more advanced policy management and integration with Microsoft SharePoint, WordPress, Joomla, Drupal, file servers, and conventional network shares. [31] EMM suites can also leverage enterprise file search, retrieve, share, organize and sync capabilities.

VoIP over wireless WAN is a subset of mobile voice communication. There are mobile applications or softphones that enable voice calls from mobile devices over data-centric 3G or 4G networks. BYOD users who want to avoid per minute charges can use Skype, Viber, FaceTime or other softphones for mobile VoIP services. While as consumers, users are very comfortable using Microsoft Skype and Apple Facetime as communications tools from a range of difference devices, there is more uncertainty over whether the experience is good enough to replace the reliability of the desk phone or mobile in the office. BYOD users can choose any softphone brand and SIP vendor for internet telephony, considering Session Initiation Protocol (SIP) supportability. [63]

Video calls are overtaking email messaging as the preferred way of communication in the workplace and more organizations are allowing their workers to bring their own devices for work. In bringing Skype to the business market, Microsoft is catering for the massive rise in mobile communications and the trend for BYOD. With its unified focus, BYOD infrastructures can be integrated with the full line of Microsoft MCM offerings such as SharePoint, Skype for Business and Exchange. [64]

3.2.4. Microsoft Work Folders

Microsoft Work Folders allows users to store and access work files on personal computers and smart devices from anywhere. Using internal file servers and information repositories provides control over critical data by specifying user device policies such as mandatory lock-screen pins and device encryption schemas. [41]

IT departments can combine Work Folders with existing file, folder, share, redirection, offline and roaming home solutions. Work Folders integrates file repositories with the server called a sync share which enables users to access them from anywhere, anytime vi an intuitive interface.

3.2.5. Visibility and Control for Mobile Data Leakage

Properly planned and implemented BYOD programs can provide great advantages to organizations beyond IT perspective. After a proper research the right tools and methods can be seen and chosen to ensure organization’s mobile worker connectivity goals. The new architecture native on smartphone OSs is known as a walled garden or sandbox architecture. With app wrapping each application and its data reside in a protected area called a sandbox. Wrapped applications cannot access to the sandboxes of other applications. If any application is infected or compromised, it cannot spread to other applications and connected backend systems. The sandbox architecture has largely made antivirus unnecessary, although malware remains a concern to violate privacy and other security threats. [8]

While the sandboxed architecture improves endpoint security, it makes some tasks more difficult. Sandboxing prevents security tools from gaining control over the device as well. It is therefore impossible, on many platforms, to enforce desired configuration standards. [56]

Personal apps and data can be easily classified, isolated and separated by App wrapping or sandboxing methods which allow some data to be safeguarded with strong encryption. However, the sandboxed smartphone architecture has also made some management tasks easier. Because mobile apps are isolated from each other, administrators do not have to test for application conflict. Additionally, the closed nature of the smartphone platform reduces the incidence of rogue, unlicensed application installation, thus reducing the burden of ongoing software auditing and license compliance processes.

As more applications are adapted to run in the container, the enterprise must provide service-based automation to dynamically deliver additional applications according to the roles and needs of the end user. This will require the integration of an application store client in the container that can then securely deliver approved applications into the container, which can wrapper applications to maintain container compliancy and interoperability and provide persona-based services and RBAC that can be used to filter applications by role, responsibility, and business function. An internal application store provides the necessary flexibility and security for delivering apps to the container, whereas allowing access to the public application store within the container lends itself to a potential breach in enterprise security. [45]

BYOD architectures also typically involve an element of Data Loss Prevention (DLP). If IT departments implement DLP with MCM, they need to make sure that users adhere to the policies, rules and limitations such as copy and paste across applications, printing, camera usage, location services, screenshot, backup and export data both online and offline. [65] [66]

3.2.6. Mobile Application Management for App Stores

The application can be on-premises, cloud-based, and hybrid model main door to access company data, and it is the place where users will spend time. Since the main reason to embrace mobility is to increase productivity, the applications used by employees must be able to run in all the mobile device operating systems used in the organization. This is an important point to consider, because while some companies might have their most important apps fully portable to run in a mobile environment, others might need to understand what options are available that can help them to deploy their apps to mobile devices. [67]

Following questions will assist identifying individual application requirements: [68]

- Internet access requirement?
- Personal information collection?
- Public cloud integration?
- Operating System dependency?
- Remote Desktop Protocol (RDP)?
- Full-Time Access?
- Social media integration?
- Available for BYOD users?
- Deployment scenario?
- Deployment and update options?

- Target device options and specifications?
- Storage space requirements?
- Encryption requirements?
- Remote uninstall or wipe?
- Low speed hig latency network usage?
- MFA capabilities?
- Proxy capabilities?

MAM simplifies management of the mobile apps by limiting the user to select only reviewed applications from the approved lists and from more reliable enterprise app stores. [69] [55]

With BYOD employees bring their mobile devices to work and they are running apps, and access corporate data as well. However, many of the business implications are not clear and IT organizations are striving with mobile devices. Modern EMM suites extend the mobile management to the apps and stores. Leading vendors are providing suites that integrate BYOD, MAM and enterprise app stores. [70]

Recent EMM suites compliment BYOD solutions with MAM integration by arranging enterprise app stores and public app stores in single interface. Thus, providing ease of deployment, update distribution, license and release management. Applying policies directly to mobile applications is better solution, rather than using the OS management layers. This is necessary when the OS does not provide enough security or when organizations prefer to limit the presence of a management agent on a user's device, which is typical in BYOD scenarios.

We have deeply evaluated the vendors, platforms, policies and use cases for MAM products that can support BYOD programs. This point is critically important, because public app store apps cannot be managed via MAM unless they expressly provide this permission. [28]

- **Application delivery from home-grown applications and trusted applications from public sources.** IT departments develop their own applications and need to deliver those to their end users along with apps for job functions from public app stores such as Google Marketplace or the Apple store. The MAM platform needs to be capable of delivering from both sources and integration of Apple Volume Purchase Program (VPP)
- **Application updates**. After IT departments have their applications on the device they need to manage applications through the entire lifecycle, and ensure that they are updated in a simple and seamless way.
- **User authentication**. The MAM solution needs to establish the flexibility of authentication for applications. Some could be simple passwords, some directory based, some MFA and others via security certificates.
- **Role Based Access Controls**. For administration purposes IT departments want to assign granular permissions to groups of users, defined as part of their user segmentation process.
- **Application based VPN**. MDM solutions offer device based VPN connections so everything is tied to the company network. Application based VPNs mean that IT departments set the specific applications that can trigger and connect to the office to get access to data.
- **Over the air (OTA) capabilities**. OTA makes BYOD possible when IT departments do not need to physically take each device and configure to the network. The MAM solution should enable users to self-enroll and leverage OTA as a way to simplify this.
- **Reporting and tracking**. IT departments need to be able to track usage and report back on the effectiveness of the BYOD implementation. IT departments need to be able to configure logging and filter logs on the severity of security breaches such as jailbroken devices, number of failed logons and inappropriate device usage.
- **License control**. IT departments want to make sure that they are not paying over the odds for applications or, do not have enough applications to support their end users.

3.2.7. Simplify Device Enrollment for On-Boarding

Organizations may simplify BYOD transition by controlling and guiding device selection, specification approval and configuration baselining. [55]

When organizations choose open device strategy, virtually anything employees want to use is allowed. Otherwise options are restricted and organization creates an approved list of supported devices. BYOD transition can be simplified with open acceptance and open device policies and this will prevent impractical controls and methods.

Open standards and software environment always simplify transition processes and represent more independent roadmap. Providing users with multiple alternatives, proper tools and open device strategy also reduce complexity of management. IT departments will likely want to distribute and monitor corporate applications based on device ownership models but IT also wants to provide their end users with a simple way of enrolling their BYOD devices themselves. Enabling end users to enroll on a self-service basis is a great way for IT departments to provide acceptable policies around usage while ensuring that end users are aware and convenient with them. [4]

When a mobile device is enrolled in BYOD solution, the device is automatically assigned policies and permissions that associated with the user's persona and the group the device itself is associated with in directory services. Depending on the MDM solution, most of the configuring and provisioning of device policies and permissions is done before device enrollment. Then policy and compliance settings take effect as soon as the devices enroll, avoiding gaps between enrollment and compliance. Such streamlined enrollment in the BYOD program makes the onboarding experience for users simple, and will increase the likelihood that they recommend the program to other employees. [71]

Enterprise mobility gives BYOD users a smooth experience across multiple devices. It delivers a secure workspace for business applications, safely enabling BYOD and self service capabilities. And it establishes a platform that scales to support new business expectations.

User perception, behaviors, similar patterns and models for new technologies in workplace are broadly described in Technology Acceptance Model (TAM). Perceived usefulness and perceived ease of use for BYOD are very similar to the relationship between cloud computing and social media. Perceptions of BYOD are efficiency in tasks, improved mobility and competitive advantages. [55] BYOD also perceives sense of privacy and freedom leading to increased productivity and employee satisfaction. [41] Companies can use BYOD paradigm to reduce costs, increase productivity and employee satisfaction. [72]

As soon as we start to consider BYOD projects we really need to think about EMM. MDM, MCM and MAM are working in favor of the organizations; however, they definitely are not the only element alone in a good BYOD implementation. New challenges can be met only with an end to end EMM platform built to meet today's needs and ready to adapt to an ever-changing range of devices and technologies. Enabling business process transformations, driving new revenue streams, and creating connections with customers and business partners can be possible with effective EMM suites. [56]

EMM enables IT organizations to securely manage the growing proliferation of mobile devices, while also laying the foundation for mobile business applications delivery and infrastructure. It helps IT departments gain control over mobility by unifying security and management. [54]

People benefit from

- Seamless experience across multiple mobile endpoints
- Secure workspace for business applications, email, content, and browsing
- Safe BYOD and self-service support capabilities
- Increased collaboration for corporate content without privacy or data loss risks.

Organization benefits from

- A platform that scales to support new business processes to serve a more mobile workforce and customer base
- Management and security beyond the device level, into creating policies on an application and information level

Collectively, these capabilities provide the features and functionalities we need to provide our users with a seamless digital workspace and empower IT with a future proof platform. The examples of business transformation through enterprise mobility are endless. These, and a multitude of other use cases, enable work to be done in new ways to empower the people and transform the organization. While the applications of the technology are diverse, enterprise mobility use cases all share a common need for end to end management of the mobile environment.

3.3. Identity and Access Management for Authorization

Identity Management construct the domain, define controls and entitle client machines with native applications and protocols by providing centralized structure that has previously been unavailable to multivendor environments. This chapter covers fundamental aspects of installing, configuring, and managing BYOD identity domains, including both servers, equipment, components and clients. IM is deeply associated with the necessity to build contextual information about the user which we will call persona in this chapter. Integrating the EMM solution into the company's IM environment allows employees to use a single common persona. [33]

Efficient security information frequently relates to identities of users, machines, and services and takes advantage of existing corporate groups to manage users and devices. Identity is verified once; service and resource access can be controlled afterwards. Identity domain creation and rapid user or machine enrollment mechanisms to a domain can be provided by new ways of IM platforms such as single sign on (SSO) authentication services. [58]

IT administrators usually choose central IM, authentication and united authorization platforms for simplicity, efficiency, ease of administration, risk mitigation and for lower management overhead. Using common tools to collect data, manage inventory, distribute information and apply policies designate a comprehensive IM discipline and create configuration harmony. In this scenario, having single account for representing identity and access authorization will always be easier. [73]

A persona is a role copy of a position, rank or degree of an organizational unit which represents major aspects and operational properties of an individual. It is used for prototyping and user experience measurement. It can be used for software assurance, process design, value proposition and issue examinations for efficiency. [74]

Risk Aware Role Based Access Control (RARBAC) is the improved version of RBAC approach that additionally calculates risks factors for traditional access mechanisms. Risk assessment methodology can include connection remoteness, user preferences, operating system, organizational unit and set some thresholds for each one. This method is well suited for new and modern paradigms such as BYOD. [32]

3.3.1. Business Transformation Starts with the User

IT departments have been delivering fixed solutions to employees regardless of their roles. In such cases, the focus is more on the technology than the people using it. While this approach may keep IT costs down by minimizing the complexity of the environment, it is slow to meet the evolving, specialized needs of the contemporary workforce. Transitioning from this one-size-fits-all IT strategy to one that optimizes the productivity of each type of employee or employee persona requires that IT departments shift their focus from what technology employees use and where they work to how they work. [75]

Every device and every app, whether it is home-grown or a best-of-breed cloud service, needs identity. As IT leaders focus on building new connections with customers, partners and intelligent objects, the challenge of IM quickly rises to the front. From IT perspective, users must be quickly brought onboard, securely authenticated, centrally managed and easily retired according to security policies and integration requirements. The same applies to devices and smart objects. [76]

In the past, identity and device management was typically handled by on premises solutions that were either proprietary or purchased from third parties. This approach had significant drawbacks, there were large upfront costs in developer time, license payments and hardware. Such solutions took many months to deploy, they were expensive to operate, maintain, and secure, and they required ongoing attention from IT departments. Frequently, they also suffered from the hidden problems of fragmentation as new systems were stood up across an enterprise.

In recent years, an additional shortcoming arose. As enterprises increasingly became mobile and moved to the cloud, and embraced services that needed to connect to large numbers of devices, traditional identity and device management couldn’t handle the requirements presented by cloud based applications and these connected devices. Flexible integrated identity and EMM solutions could easily and securely connect with all users and devices. Thus, enterprises bypass the challenges posed by legacy identity technologies. [77]

3.3.2. Integrations with Directory Services and Implementing Hybrid Identity

Transition to cloud applications causes the proliferation of separate user stores. Each cloud provider and application handle identities independently and therefore has its own unique database of user credentials. This is one of the small number of negative effects, however with the cloud computing extension IT organizations will face the user and account management limits and they may lose control over account creation, activation and deactivation processes. [36]

BYOD infrastructure and programs require seamless integration with IM platforms for access and authorization controls. Managing multiple separate user directories without an IM platform can lead to security vulnerabilities, blind spots and access management failures.

Microsoft Active Directory (AD) is the central user account authority and directory solution for most enterprise organizations. AD can also be combined with advanced IM platforms to control access to a broader set of business applications and IT systems. LDAP based corporate directory services can be extended, expanded and leveraged by EMMs to efficiently organize and manage user access. Administrators can assign device profiles, apps, and content to users based on their directory-group memberships. Additionally, some EMMs can detect directory changes and automatically update device-policies. For example, if a user is deactivated in a directory system, then the IM can remove device based corporate network access and according to previously agreed policies, can selectively wipe the device. [48]

The BYOD integration with IM address these challenges and provide:

- **Two-way user and group synchronization:** Object insertion and modification to and from IM, EMM and LDAP should be automatically synced.
- **Access provisioning and deprovisioning :** Object deletion should result automatic EMM revocation.
- **Single sign-on (SSO):** After first successful authentication, users should not enter same information or credentials again.

3.3.3. Flexible Secure Verification Options

Form based single factor authentications such as a static user name and simple passwords are industry standards for web sites. However, such ways of handling credentials are difficult to manage and vulnerable to sophisticated hacker attacks. Individuals are more prone to identity theft via targeted spear phishing attacks, while enterprise users can be compromised by social engineering attacks. [78]

Enterprise cloud adoption makes harder controlling such critical incidents because of high availability and accessibility of cloud applications to anyone on the Internet. By the nature of cloud computing, many cloud apps do not have appropriate interfaces for enterprise standards and integrations, which can make security adjustments harder than before. [79]

The growth of the mobile workforce has changed how organizations must secure access to applications and data. Users are accessing applications from home offices, coffee shops and hotels, and from mobile devices. Users demand the flexibility to connect from anywhere, and IT and security professionals should adapt to secure access from unknown networks and devices. [7] Several second factor options can be chosen by IT departments, which is suitable for their user base, sensitivity of their data and compatibility of their use case.

For organizations, especially those with a reliable authentication mechanism already in place, the solution is to centralize access. Rather than authenticating a user with another set of credentials, many customers prefer the infrastructure to provide the option to integrate with an existing identity provider of choice to authenticate and authorize a user. MFA can offer SMS option which will work with any cell phone for users without a smartphone. [76]

While the benefits of MFAs are significant, they can be disruptive to end users in a variety of ways and causes poor user experience. Solutions that depend on hard tokens are complex to manage and expensive to maintain. The cost of tracking and replacing tokens is significant. End users find carrying hard tokens and entering passcodes inconvenient. For businesses with strict MFA policies, end users have to re-authenticate frequently throughout the day, reducing productivity and frustrating users. As the number and types of users within organizations continue to grow, a single MFA type may not scale to mobile or international users, or to specific groups of users who do not have access to smartphones due to their job functions. [37]

3.3.4. Identity Federation and Delegated Authentication

The network supplicant provisioning is the most important process of the BYOD solution, which distribute the certificates to employee owned devices. Microsoft CA can be configured in order to automate the certificate enrollment process and satisfy this requirement with the SCEP. [88]

EMM suites provide OTA deployment models by authentication, encryption and integration with directory services, digital certificate SCEP servers, and a WAP servers. SCEP provides a stable, scalable, and highly secure method of authenticating devices and users. They not only verify the identity of the individual, they can also verify the legitimacy of the device and secure the transport of information across a LAN, wireless LAN (WLAN), Internet, or a mobile cellular network. [40]

Digital Certificate Authority (CA) integration ensures message integrity, authenticity and confidentiality and enables MFA, strong encryption and digital signatures. CA service providers, such as Microsoft CA or SCEP can be leveraged by EMMs to assign and verify certificates for advanced user authentication and to secure access to corporate systems. Furthermore, EMMs can also integrate with Public Key Infrastructure (PKI) or third party providers to configure certificates and distribute keys to devices without user interaction. One of the benefits of the PKI enabled BYOD implementation is the ability of the end users to perform self-service device registration and seamless enrollment. This eliminates the administrative burden on IT in order to distribute authentication credentials and enable devices on the network. [27]

BYOD users can register a non-Domain Joined device in AD with Microsoft Workplace Join, and can gain secure SSO access to corporate network resources from that device. After the initial Workplace Join process ends a new AD object for this device is created and digital certificate installation is completed automatically. Once Workplace Join is completed for a device, it is considered as a valid directory object and IT administrators can apply conditional access policies to provide appropriate access to users same as fully domain joined device. [41]

User account, identity, access and policy management for services, are core requirements for many enterprise IT infrastructures. Organizations may choose between a federated SSO approach and a delegated authentication to integrate the application. However, the two are not mutually exclusive and there are cases where a combination of both is needed. Most federated single sign on solutions today are tailored for web based applications as they rely on the browser to act as the liaison or the agent between the application and the identity provider. This restriction limits these federated solutions when handling authentication through mobile clients and other non-web based clients such as traditional thick clients. Delegated authentication provides an alternative by allowing logins from non-browser based clients to leverage the same credentials from a single identity provider.

3.4. Network Infrastructure and Operations for Ease of Connectivity

Easy network connectivity is main functionality of BYOD infrastructures. Network journey begins with DHCP discovery and a DNS record query, for smart devices as well as traditional desktops and laptops. Stable networking with DDI for BYOD is as important as wireless access and EMM suites. An IPv4 address is still the single and unique descriptor for every connected network entity. [42]

IP addresses are not relevant to the real-world business, actual resources and services bound to the IP addresses are main drivers. Ranges of IP addresses define the perimeters and networks themselves. Organizations who wants to be modern and flexible puts IP addresses and their management to a new level. Emerging solutions are hybrid solutions that take the superior elements of multiple vendors and combine them to maximize the benefits targeted by the solution. [80]

DDI is a new and advancing infrastructure management concept that provides detailed information and centralized meta-data visibility for mission-critical network resources. Dynamic network environments for BYOD programs, put DDI into critical place and require more feature set than out of the box commodity server products. [81]

Virtualization, IoT and cloud delivery shifted the network designs and deployments and alter the enterprise perspective. However traditional concerns remain as important as ever: [88]

- **Scalability** – Spanning, scaling up and extending to large cloud deployments.
- **Reliability** – High-availability and automatic failover for resilient operations.
- **Visibility** – Multiple datacenters, include visual representation of topologies.
- **Manageability** – United, distributed, physical and virtual.
- **Flexibility** – Dynamic load balancing between sites and services.

IT organizations can handle the new requirements associated with BYOD with automated network practices. Only proactive approaches to standards reduces the risk of unexpected consequences caused by the proliferation of devices, dynamic nature of BYOD phenomenon and practices, as well as other growing and evolving trends. [80]

3.4.1. Cloud and Modern Datacenter Networking

Business continuity, resource utilization, workload optimization, mobility and multi-tenant architectures are primary motivations of enterprise IT architects. Mature organizations are consolidating workloads and virtualized datacenters for rapid service provisioning, better automation and technology orchestration. [82]

Private clouds can deliver IT services with these attributes at considerable costs. Virtualized and software defined datacenters are becoming prevalent. Enterprise IT departments have been running VMware, Microsoft, or Linux based software hypervisors for their workloads. Moreover, they are evaluating public cloud providers and SDN functions for easy hybrid-clouds extensions. [46]

SDN creates a much more automated and programmatic network. Instead of manual, decentralized, device-based, command line interface (CLI)-driven changes, SDN enables the network to be centrally configured programmatically. Thus, organizations can utilize orchestration systems or cloud management platforms to set up appropriate network policy and path selection. SDN can increase network agility, simplify management and lead to the reduction of operational and capital costs, while fostering long-term innovation. [31]

Hybrid and complex workloads require agile edge services, scale out and location independence infrastructures. They also should be protected from infrastructure failures such as IP address collusion, DNS record mismatch, time zone differences as cloud expands. [81]

Modern data communications depend on emerging network technologies and these technologies are also enablers of the massive network expansion for the future IT. With the introduction of BYOD and IPv6 initiatives, the quantity of IP addresses and complexity of the network is going to increase. As complex technologies become defining attributes of the modern datacenter, IT will have new responsibilities. [16]

Core network infrastructure resources and requirements increase as the new IP dependent technologies enters the enterprise IT solutions. As the number of initial network connection requests rise, wider IP pools and longer DHCP lease times are also required for such expansion. [44]

Another important point for modern networks is central IP address management, tracking and reporting facility. Enterprise IP address spaces should be monitored for real-time entries, exits, topology changes and integrity checks. [41]

Network engineers are now closely interested in the utilization of the IP address as well as the type of resource each IP address consumes. With the BYOD trend on rise, enterprises today are witnessing a number of devices visiting their premises which are not a member of any of their local registered corporate domains. Using predefined DHCP templates is preferred practice for enterprise IP networks and repetitive configuration tasks for BYOD readiness. [23]

Templates are facilitative methods for mass deployment scenarios and repetitive task for ease of configuration by preventing basic human syntax errors into single configuration files. [18]

DHCP options are important tools for IT departments to distribute configuration updates and effective change management tasks. Standard DHCP requests are always finalized with successful IP address acquisition and dynamic lease provisioning. Static assignment of IP addresses or ranges may help IT departments to specify more granular settings for hosts and reduce their task loads.

Large IP address pools and dynamic assignment can be utilized for high turnover enterprise networks. Particular hosts such as servers can be statically assigned and locked to a specific IP address in small topologies. This technique is termed static assignment by the Request for Comments (RFCs) or permanent lease by Microsoft DHCP servers. Another reason for statically assigning IP addresses is that it improves the usability of logs. If clients always are assigned the same IP address, logs will consistently show them at a particular IP address. Enterprise DHCP servers can also share the same address pool for automatic failover and dynamic load balancing between datacenters.

Having the same and accurate time information is vital for enterprise networks. Time-based authentication mechanisms and digital certificates are highly dependent on time stamps for validation controls. Server log files and administrative reports are bearing time and date information as metadata. The integrity of security platforms, relative activities, any file system is also highly dependent on the name and dates of files. [43]

3.4.2. Network Connectivity Management

Enabling secure, managed access to a wide variety of corporate resources by mobile devices is an important feature of a EMM solution. While these resources have typically been located in on-premises networks, it is more common today for resources to be hosted in addition on cloud based web services and external networks.

Virtual private networks (VPNs), and corporate wireless (Wi-Fi) networks play an important role in keeping data and other resources protected from unauthorized access. Equally important is making it convenient and easy for mobile device users to have secure access these resources to avoid users finding a more convenient but not secure method of storing or accessing resources. [46]

Location and bandwidth were representing legacy IT service delivery models and do not adequately support the modern users. Proliferation of mobility and IT consumerization will dictate new paradigms such as SaaS and BYOD. Application environments and design patterns are in transition; demands and expectations are expanding beyond the capabilities of existing network topologies which can not supports new and changing business requirements. [10]

Networking teams need to address five dimensions in an engineering framework. [83]

- **Users** – Users are different personas, profiles and drivers behind technology.
- **Applications** – Applications are time sensitive and resource intensive.
- **Devices** – Devices are proliferating to the enterprise level as a business tool.
- **Location** – Enterprise mobility and high speed location aware apps.
- **Activity** – User interaction at the end of the line.

Specific latency and bandwidth requirements of virtualization, big data, cloud, mobility scenarios also need to be considered in detail. Re-engineering and optimization are required for increasing east-west (server to server) connections as well as north south (client to server) connections.

Mobile devices typically connect to corporate networks and resources by using the industry standard access technologies, such as NAC. BYOD infrastructure detects the new devices at the gateway level via NAC and scans them for vulnerabilities, device types, user personas and software updates before they connect to the production network. If a device fails to pass these test, NAC sends it to quarantine network and prevents access into the production network until the end of remediation. [84]

Access controls prior to connection are determining features of NAC methodologies for BYOD architectures. NAC only provisions access to production networks when the user registers and the device is checked for supported operating systems, antivirus and malware.

Integration with other enterprise security components, such as firewalls, SIEM and WAP is another important NAC feature. Deploying WAPs behind a firewall adds network level protection and reduces the attack surface of the WAP servers. WAP servers provide organizations the ability to integrate BYOD infrastructures with their back-end enterprise systems. This allows organizations to leverage the benefits of BYOD running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems. [84]

IT consumerization continues and will cause further accumulation of device types and mobile environments, and will push traffic from wired to wireless networks. Enterprises will not have a chance to known the list of devices or they will have control over them when designing network solutions. It is time to prepare the entire enterprise for this shift and to move toward a "wireless by default and wire by exception" model, taking advantage of the tremendous improvements in WLAN performance and security. [85]

Any Wi-Fi access point can now be an office, and since these networks have potential risks to the data and network, IT departments have to gain resources and guidelines in place to govern and handle the mobile workers. Network planners should thoroughly understand how the business intends to embrace mobility, BYOD trends and content access, to sidestep performance problems and subsequent WLAN upgrades. It is critical to create and maintain a central repository for deep network information and topology changes. [88]

Enterprises need a single repository for dynamically tracking and synchronizing network information and the ability to search and retrieve all this information in a timely manner enabling better and faster troubleshooting. Sparse traditional tools have several challenges preventing organizations to achieve this goal. [47]

Consumerization of IT and proliferation of mobility continue to be the major drivers for the adoption of NAC. BYOD implementations without NAC will suffer from unmanaged access, uncontrolled risks and eventually exposed to security vulnerabilities. Integrating EMM suites with NAC can bring broad visibility, policy implementation and enforcement capabilities to IT departments. [84]

3.4.3. Mobile Printing as BYOD Enabler

Enterprise IT departments demand agile business services that are easy to deploy and manage, always available and cost effective. Mobile devices are becoming almost ubiquitous. Printing and imaging market has been reshaped after rapid mobility adoption and increasing network bandwidth. The need for print on the move, away from the office, is increasing, and security in mobile printing is being requested more and more. Wireless printing solutions that use technologies like Apple AirPrint and Near Field Communication (NFC) are also becoming necessary. [86]

Printer providers have been focusing more on users' businesses and internal communications. They have been developing new applications and software to optimize and automate business processes. Further, they are incorporating new functions and software into their devices, such as improved scanning, direct Wi-Fi connections and remote monitoring capabilities. Properly chosen and adopted applications and software help to save costs and improve users' workflow and business processes such as BYOD.

Standards-based zero-configuration network protocols help IT departments to prepare networks for such new technologies that which enable devices to find services on a network automatically. Apple Bonjour protocol is used to discover networks and automatically connect iOS devices, Apple TVs and AirPrint compatible printers. [85]

3.5. Monitoring and Troubleshooting for Self-Support Environments

Monitoring and auditing are especially important for organizations that must comply with governmental regulatory requirements and industry compliance guidelines. Monitoring and capturing status and event information for mobile devices is vital to ensuring that users and devices are in compliance with your corporate policies and security strategy. Automation is also essential for both initial onboarding and to take action on non-compliant devices, for example, quarantining them until they are compliant. [12]

Personal devices are usually more hazardous than company-owned devices. However, companies with rules against personal devices can yield, at least under special circumstances, and based on perceptions of user needs. EMM solutions should share device posture with a NAC solution to ensure that devices meet compliance before being given access.

Reporting can also provide valuable information about software, hardware, and licenses in any organization to assist with inventory management. Where applications and data will reside on personal devices, companies should set limits on which personal platforms are supported and should be prepared to limit the types of information made available to personal devices. Organizations should resolve to require management opt in as a condition of getting access to sensitive information.

In general, EMM solutions divide monitoring into two general areas: [71]

- **Logging** – Capturing and storing mobile device status and information.
- **Reporting** – Brief summary and dashboard status reports.

Integrating with helpdesk applications and SIEM can provide an enhanced experience for the user and IT for improved problem resolution. Internal audit and compliance processes usually demand privileged user or admin activity reports that SIEM produces. SIEM also improves the IT security ability to quickly detect targeted attacks and data breaches, and improves incident investigation and response. [85]

Access control, inventory management, software update and license management will be getting difficult as the number of devices increase. All mobile devices used to access business resources should be detected and recorded in a centralized data repository. Devices should be identified as either business-owned or user-owned and detailed configuration and status information should be automatically collected and tracked. Administration should be simplified with an intuitive and customizable console interface that consolidates all EMM processes, dashboards, and reports.

Not only large global organizations employ IT asset management (ITAM) but also the businesses at high maturity levels. ITAM is critical to every business structure as organizations adopt cloud service delivery and BYOD models. It is the ideal business discipline for providing hugely useful visibility and insight into an organization that needs to bring clarity to determine what’s needed as they plan to scale and update processes, devices, and software. Demand for internal IT resources can be reduced by employing EMM solutions as a cost-effective mobile assets tracking. [87]

The processes for collecting asset and status data from mobile endpoints should be automated, requiring little or no administrator interaction, and trigger based automation should be available that remediates problems when certain predetermined conditions occur.

3.5.1. Community Assisted Self Service Support

One of the significant challenges of BYOD implementation is supporting user devices outside of corporate networks and policies. Majority of organizations deploying mobile management and security solutions without first teaching their employees how to use them effectively, impacting both support costs and end-user satisfaction. A best practice is that the IT organization holds one hour classes, during which users enroll their devices and learn how the system works. This can be an online tutorial-based, with a resource available to answer questions. [47]

EMM vendors have started offering additional training materials to assist beyond simply deploying and operating their products. The scope and depth of this material varies significantly, with the best offering extensive guidance covering vendor best practices, industry specific solutions, end user training and governance issues. Such type of self-training is critical to explain to employees not only how to use the new solution, but also the reasons why it is needed and the risks associated with using mobile devices. [16]

Mobile world changes continuously. As such, organizations need to be prepared for unexpected updates to mobile operating systems. Having a support contract with a vendor that is responsive in not only helping out with supporting its EMM product, but also the realities of mobile perpetual change. Organizations can potentially unburden the help desk by combining basic user training with a self-service portal to offload common tasks. This will enable users to take the stress off of IT by performing common tasks, such as locating, locking or wiping a device themselves, without the need to communicate to IT. A support wiki can also be associated with the help-desk to encourage users to share and check for community advice online. [10]

Self-Service Portals (SSP) are useful online tools used to remotely monitor and manage user problem tickets and devices. It can help reduce the hidden cost of managing a device fleet. By empowering and educating device users on how to perform basic device management tasks, investigate issues and fix problems, the organization may be able to reduce the number of help desk tickets and support issues. Device and application configuration must be intuitively self-serviceable because lacking this capability, end user adoption is stifled and IT helpdesk support could become strained. [85]

Such organizations should also ensure that IT performance is clearly specified in Service Level Agreement (SLA), and they are included into the corporate terms of use contract.

3.6. Chapter Conclusion

Meeting a new regulation, infrastructure modernization and e-transformation are the leading motivations that make an organization to shift strategies and take a new course. Taking the first steps such as framework selection and program preparation are not enough, it is also important for organizations to establish supplemental and complemental factors for successful implementation.

After establishing a mobile security policy, an enterprise should prepare their mobile device management methodology and select a solution framework to put into practice. This chapter focuses on the technical environmental requirements and infrastructural integration considerations.

Organizations should extend the scope of their preparations and choose to specify additional details and requirements of daily user activities. Work conditions always demand strict security policies and rigid controls for high-risk factors and uncertain situations such as accessing enterprise resources from unknown Wi-Fi hotspot.

In order to describe mobile adoption in business we have focused on consistent, open, simpler and native capabilities for configuration and security issues of mobile devices and apps. End users always derive benefit from new and emerging technologies which are cheap and effortless, and organizations derive benefit from enterprise grade and business ready security environments while protecting existing investments.

4. CONCLUSION

4.1. Findings

1) Organizations focused on confidentiality and corporate information security

Acting in accordance with enterprise corporate security policies is essential since personal devices used for work are part of the enterprise networks. (Section 2.9, Section 2.14) For the organization, data access strategy and device strategy need to manage risk and maintain IT compliance and information security. (Section 3.3.2, Section 2.32)

User compliance on previously well agreed upon terms and conditions is also an important assurance point when organizations implement BYOD programs. (Section 2.18, Section 3.4.2) Immediate and serious risks to IT security may be assessed and they may prevent organization's ability to meet compliance requirements when a decline occurs in mobile device policies and security objectives. (Section 2.19, Section 2.30, Section 2.31)

2) People criticizes privacy and the sensitivity of personal information

Legal, ethical issues and policy considerations appear around sensitive privacy of individuals. For the people, privacy policy expected to protect the sensitivity of personal information stored on the device, and be seamless enough to promote productivity. (Section 3.2)

Privacy of people is as important as security of organization while discussing BYOD programs. Mobile devices always contain private data of individuals such as family photos and must be handled with special and cautious ways, that can be implemented between personal and employer data. (Section 2.1 Section 2.4)

After examining historical and contemporary privacy matters we have discussed domestic and international legislative approaches to sensitive personal information. New and existing legal concerns present about protecting the privacy of consumers and personal identifiable information and will be persistent in the near future. (Section 2.6, Section 2.19)

3) Mobile operating environments are adopting walled garden paradigm

The protection of multitenancy in cloud computing is maintained by hard isolation mechanisms that which prevent data leakage from one customer to another. This is the similar internal sandboxing and protection technique for smart devices in BYOD scenarios. (Section 2.6)

The new and modern mobile operating environments benefit from a new approach known as a walled garden or sandbox architecture. BYOD privacy and security challenges can be met with an end to end EMM platform built to support walled garden paradigm and ready to adapt to an ever-changing range of devices, technologies and threats. (Section 3.2.5)

The rules of a sandbox architecture are that each application and its data must reside in a protected area called a sandbox. Applications wrapped in this way cannot read or write to the sandboxes of other applications. (Section 2.13)

4) IAM can be leveraged by EMM to efficiently organize and manage personas

LDAP based corporate directory services can be extended, expanded and leveraged by EMMs to efficiently organize and manage persona access. (Section 2.17, Section 3.3.4)

IAM is deeply associated with the necessity to build contextual information about the user which is called persona in business world. Integrating the EMM solution into the company's IM environment allows employees to use a single common persona. (Section 2.20, Section 3.4.1)

5) **Network tools are getting inadequate against new trends and use cases**

Virtualization, Internet of Things and Bring Your Own Device are sources of this expansion. BYOD infrastructure networking requires converged DDI solutions for composite IP addresses, multi-tenancy, public, private and hybrid clouds. (Section 3.2.3, Section 3.4.1)

6) **Self-Service Portals are enabler of BYOD and reduce cost of managing devices**

Users are accustomed to an experience that is simple and convenient. They now expect the same level of ease when working with corporate devices and apps that they experience when using their personal devices and apps. (Section 2.5, Section 2.9) Providing employees with options and clear communication are the keys.

Seamless user experience across multiple devices can be accomplished by EMM suites. They provide secure environments for critical data and applications, safely enabling BYOD and self service capabilities. And it can establish a community platform that scales to support new business processes. (Section 3.5.1)

4.2. Limitations and Future Works

This thesis is limited by a number of factors. This chapter presents the limitations of the study and discusses the overall implications of the findings and the current state of research and propose recommendations to improve the quality of future and further researches.

1) Public Enterprise Governance and Private Corporate Secrecy

Firstly, concerns about the potential adverse impact to an organization’s reputation in the market and ongoing relationships with customers limit the valuable type of information organizations are willing to disclose, either to industry partners or governments, about trade secret theft or internal vulnerabilities. (Finding 1, Finding 2)

2) Financial Design Prospect and Budget Considerations

Total money allocation for a project in a specific period of time is called budget. Organizations usually state and follow budget goals of their projects and control their costs. Budgeting is out of our scope. (Finding 1, Finding 2, Finding 3, Finding 4, Finding 5, Finding 6)

3) Ever Changing Legislative Environment

Due to the continuous renovation and recent legislative activity in Turkey, it was not possible to examine every legal aspects and requirements.

The newly published Private Data Protection Law No: 6698 harmonizes Turkey's data protection policy with the Council of Europe. At least until further guidance is issued by authorities and courts, it is generally considered that the Data Protection Law will obscure such new technologies. (Finding 1, Finding 2)

4) Language and Translation

We had only a small number of organizations in Turkey with BYOD lessons. They are naturally Turkish speaking entities and translating the research documents into English is a big validity problem. (Finding 4, Finding 5, Finding 6)

4.3. Conclusion

As we can see in preliminary phase, national and international organizations pursue enterprise mobility and cloud technologies closely and use them efficiently in order to improve services provided to its employees and customers. When we extracted the current state of BYOD in business, we have seen that BYOD is gaining popularity in most businesses disciplines under the influence of consumerization of IT as well as the proliferation of mobility.

With this motivation, our study has oriented examination several sides of contemporary mobility and information technology requirements of BYOD programs to understand and help mitigate the risks associated with implementation efforts. Risks are primarily due to the smart device technology use cases, poor separation between work and personal use and the lack of organizational assurance, legal integrity and security posture.

We have sensed the root of the problem lies in how IT approaches the responsibility for providing security and support to the organization. IT has traditionally operated with a centralized management approach, using strict policies and standards to ensure security of organization and has neglected end-user support, motivation and satisfaction.

Our thesis focuses on deciding on a BYOD strategies while determining identity management, defining access policies and implementation roadmap as important requirements in enterprise mobility solution and provides a checklist to follow when implementing a new BYOD program.

We have determined our main research question as “What comprehensive strategy can be advised to organizations in the beginning phase of their first BYOD program?” and examined our objective by extending it two sub questions as “What are the participating roles of privacy for employee and security for organization in BYOD environments?” and “What coherent motivations do organizations have integrating mobile devices into workplaces?”

We have found that many organizations seek to start or extend an existing BYO program without fully examining the intended goals. Often, there is a misperception that BYO will reduce total cost of ownership, although in most cases the savings remain elusive, especially if additional security, manageability and support processes need to be developed.

New and existing administrative, technical, legal and ethical concerns present about protecting the privacy of consumers and personal identifiable information and will be persistent in the near future. When organizations go into BYOD environments, they should ensure that users always conduct on previously well agreed upon terms and conditions. BYOD privacy and security challenges can be met with an end to end EMM platform built to support walled garden paradigm and ready to adapt to an ever-changing range of devices, technologies and threats.

We have also found that integrating the EMM solution into the existing IM environment allows employees to use a single common persona and seamless user experience across multiple devices can be accomplished by EMM suites. They provide secure environments for critical data and applications, safely enabling BYOD and self service capabilities. And it can establish a community platform that scales to support new business processes.

Enterprise mobility is an organic trend and emerging technologies are bringing digital workplace culture and ethical changes that only Gen-Y-Workers (or Millenials) can perfectly benefit from. Prevent, ban, block, forbid and restrict are not in their dictionaries. They need clear measurement of experience, context based management, personalized support and optimal balance between business requirements and IT opportunities by empowering people and trust.

REFERENCES

[1] D. Ritchie, “The Computer Pioneers,” 1986.

[2] S. Tanenbaum, “Modern Operating Systems,” 2014.

[3] J. Kurose, K. Ross, “Computer Networking: A Top-Down Approach,” 2013.

[4] C. Sandler, T. Badgett, “Enterprise Mobility for SAP Special Edition,” 2012.

[5] J. Lee, “The Future of Enterprise Computing,” IBM T. J. Watson Research Center, 2013.

[6] J. Hayes, “The Device Divide – Engineering and Technology,” October 2012.

[7] A. Dedeche, F. Liu, M. Le, “Emergent BYOD Security Challenges and Mitigation Strategy,” 2013.

[8] A. Scarfo, “New security perspectives around BYOD,” IEEE, 2012.

[9] G. Kulkarni, R. Shelke, R. Palwe, V. Solanke, S. “Mobile Cloud Computing,” IEEE, 2014.

[10] D. Nieuwenhuizen “Employee or anarchist!? Impact of IT consumerization on IT Governance,” 2012.

[11] C. Basole, “Enterprise mobility: Researching a new paradigm,” 2008.

[12] “Bring Your Own Device: New Opportunities, New Challenges,” Gartner, Inc., 16 Aug 2012.

[13] S. Kumar, “BYOD : the Big Picture,” IT Adviser, 2012.

[14] K. Miller, J. Voas, G. Hurlburt, “BYOD: Security and Privacy Considerations,” IEEE, 2012.

[15] “Understanding the BYOD Landscape,” Deloitte LLP., 2013.

[16] J. Keyes, “Bring Your Own Devices Survival Guide,” 2013.

[17] “The New BYOD: Best Practices for a Productive BYOD Program,” VMware, Inc., Sep. 2015.

[18] T. Limoncelli, C. Hogan, S. Chalup, “The Practice of System and Network Administration,” 2007.

[19] R. Krebs, C. Momm, S. Kounev, “Architectural Concerns in Multi-Tenant SaaS Applications,” 2014.

[20] R. Stair, G. Reynolds, “Principles of Information Systems, A Managerial Approach,” 2010.

[21] Y. Wang, J. Wei, K. Vangury, “Bring Your Own Device Security Issues and Challenges,” IEEE, 2014.

[22] M. Song, K. Lee, “Proposal of MDM Management Framework for BYOD of Large Companies,” 2014.

[23] “Mobile Device Management Design Considerations Guide,” Microsoft, Corp., Aug. 2015.

[24] “Industry Quotient: Australian Mobile Device Management Market,” Frost and Sullivan, Inc., 2014.

[25] “Top 10 Mobile Technologies and Capabilities for 2015 and 2016,” Gartner, Inc., 12 Feb 2014.

[26] “Critical Capabilities for Enterprise Mobility Management Suites,” Gartner, Inc., 13 Jun 2016.

[27] "Sector RoadMap: Enterprise mobility management," Giga Omni Media Research, 2013.

[28] J. Lundy, “The Aragon Research Globe for Enterprise Mobile Management Software,” 2014.

[29] “Critical Capabilities for Unified Communications,” Gartner, Inc., 30 Jul 2014.

[30] “Removing Identity Barriers for Office365,” Octa, Inc., 2015.

[31] “Magic Quadrant for Enterprise Mobility Management Suites,” Gartner, Inc., 8 Jun 2016.

[32] D. Rivera, G. George, P. Peter, S. Khanum, “Analysis of Security Controls for BYOD,” 2014.

[33] “Managing Identity and Authorization Policies for Linux-Based Infrastructures,” Red Hat, Inc., 2016.

[34] “Toolkit: Digital Transformation Playbook for IoT Strategies,” Gartner, Inc., 2016.

[35] G. Furtmüller, “An Approach to Secure Mobile Enterprise Architectures,” IJCSI, 2013.

[36] “Directory Integration with Okta An Architectural Overview,” Octa, Inc., 2015.

[37] N. Kaur, M. Devgan, “A Comparative Analysis of Various Multistep Login Authentication Mechanisms,” 2015.

[38] “Two-factor authentication for Apple ID,” Apple, Inc., 2015. Retrieved from support.apple.com/en-us/ HT204915

[39] “Identities management: an evolving landscape,” Octa, Inc., 2015.

[40] “Meeting Mobile and BYOD Security Challenges with Digital Certificates,” Symantec, Corp., 2015.

[41] “Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices,” Microsoft, Corp., 2015.

[42] “Automating Network Provisioning for Private Cloud,” Infoblox, Inc., 2014.

[43] “The Importance of Network Time Synchronization,” Symmetricom, Inc., 2003.

[44] “Reference Architecture for Citrix XenMobile 8.5,” Citrix Systems, Inc., 2013.

[45] “Cooperative solutions for Bring Your Own Device,” IBM Corp., 2015.

[46] “BYOD Agility through consistent delivery,” PricewaterhouseCoopers LLP, 2012.

[47] “Securing Inter VLAN traffic in layer 2 networks,” PaloAlt Networks, Inc., 2012.

[48] K. AlHarthy, W. Shawkat, “Implement Network Security Control Solutions in BYOD Environment,” IEEE, 2013.

[49] “Apple Deployment Programs Device Enrollment Program Guide,” Apple, Inc., 2015. Retrieved from : Business Device Enrollment Program: www.apple.com/business/dep/

[50] “Critical Capabilities for Security Information and Event Management Technology,” Gartner, Inc., 12 May 2011.

[51] “Hype Cycle for ITSM 2.0, 2015,” Gartner, Inc., 17 Jul 2015.

[52] W. Peng, F. Li, J. Han, X. Zou, J. Wu, “T-dominance: Prioritized Defense Deployment for BYOD Security,” IEEE, 2013.

[53] M. Chang, C. Ho, C. Chang, “Securing BYOD,” IEEE, 2014.

[54] “Risk Management of Enterprise Mobility Including Bring Your Own Device,” Australian Government, Department of Defense, Jun 2013.

[55] A. Yang, R. Vlas, “Risk Management in the Era of BYOD,” IEEE, 2013.

[56] “A Toolkit to Support Federal Agencies Implementing Bring Your Own Device Programs,” U.S. Federal CIO, 2012.

[57] C. Baratt, C. Burry, J. Venezia, “BYOD for VMware Special Edition,” 2014.

[58] M. Souppaya, K. Scarfone, “Guidelines for Managing the Security of Mobile Devices in the Enterprise,” NIST Special Publication 800-124, Jun 2013.

[59] B. Katz, A. Kesari, “Enterprise Mobility Management for Airwatch Special Edition,” 2016.

[60] “Enterprise Mobility Management – Market Quadrant,” The Radicati Group, Inc., 2013.

[61] M. Astani, K. Ready, M. Tessema, “BYOD Issues and Strategies in Organizations,” 2013.

[62] J. Lee, R. Crossler, M. Warkentin, “Implications of Monitoring Mechanisms on Bring Your Own Device Adoption,” 2013.

[63] J. Harris, B. Ives, I. Junglas, “IT Consumerization: When Gadgets Turn Into Enterprise IT Tools,” MIS Quarterly, Sep. 2012.

[64] J. Lundy, D. Smith, “The Aragon Research Globe for Social Software: Knowledge at the Core,” 2015.

[65] I. Woodring, M. El-Said, “An Economical Cluster Based System for Detecting Data Leakage from BYOD,” IEEE, 2014.

[66] “VMware Workspace One Reference Architecture: Validated Integration Design,” VMware, Inc., 2016.

[67] “Enabling Bring-Your-Own-Device using mobile application instrumentation,” IBM Corp., 2013.

[68] “Mobile Device Management Design Considerations Guide,” Microsoft, Corp., Aug. 2015.

[69] N. Leavitt, “Today’s Mobile Security Requires a New Approach,” IEEE, 2013.

[70] “Bring your own device, Security and risk considerations for your mobile device program,” Ernst & Young Global, Sep. 2013.

[71] “VMware AirWatch Mobile Device Management Guide,” VMware, Inc., 2016.

[72] C. Yin, L. Liu, L. Liu, “BYOD IMPLEMENTATION: Understanding Organizational Performance Through A Gift Perspective,” 2014.

[73] “Use commercial IAM Solutions To Achieve more Than 100% ROI Over manual Processes,” Forrester Research, Inc., 1 Oct. 2012.

[74] “Application Leaders Should Take the Lead in Creating and Managing Personas,” Gartner, Inc., 2013.

[75] “Five Best Practices for Taking a Persona-led Approach to IT Strategy and Delivery,” Unisys Corp, 2014.

[76] S. Chung, T. Escrig, Y. Bai, B. Popovsky, “2TAC: Distributed Access Control Architecture for BYOD Security,” IEEE, 2012.

[77] “A New World Order for IT,” Octa, Inc., 2015.

[78] K. Svensk, “Mobile Device Security Exploring the possibilities and limitations with Bring Your Own Device,” Dec. 2013.

[79] A. Armando, G. Verdarame, A. Merlo, “Securing Bring Your Own Device Paradigm,” IEEE, 2014.

[80] “Bring Your Own Device and the Network Infrastructure,” Infoblox, Inc., 2013.

[81] “Automating Network Provisioning for Private Cloud,” Infoblox, Inc., 2014.

[82] P. Mell, T. Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145, Sep. 2011.

[83] “Focus on Five Dimensions of Network Design to Improve Performance and Save Money,” Gartner, Inc., 28 Mar. 2013.

[84] “NAC Strategies for Supporting BYOD Environments,” Gartner, Inc., 22 Dec. 2011.

[85] “SOLVING THE BYOD CHALLENGE,” Aruba Networks, Inc., 2014.

[86] N. Pohlmann, M. Hertlein, P. Manaras, “Bring Your Own Device For Authentication (BYOD4A),” 2015.

[87] “The Secret Life of IT Assets,” Samanage, Inc., 2016.

[88] “Cisco Unified Access (UA) and Bring Your Own Device CVD,” Cisco Systems, Inc, 28 Aug. 2014.

[89] M. Uehara, “Proposal for BYOD based Virtual PC Classroom,” IEEE, 2013.

[90] V. Samaras, “A BYOD Enterprise Security Architecture for accessing SaaS cloud services,” 2014.

[91] G. Gilmore, P. Beardmore, “Mobile Security and BYOD,” 2013.

[92] “Consumerization of IT: Risk Mitigation Strategies,” ENISA, 2012.

[93] “Consumerization of IT: Top Risks and Opportunities,” ENISA, 2012.

[94] “Isaca Journal”, ISACA, Vol. 5, 2014.

[95] “Defending mobile devices for high level officials and decision-makers,” CCDCOE, 2015.

[96] “UNITED NATIONS E-GOVERNMENT SURVEY,” U.N. Economic and Social Affairs, 2014.