HEIMDAL™
SECURITY

MOBILE DEVICE SECURITY FOR COMPANIES WITH BYOD POLICY.

Casting some light upon the blurred lines of a BYOD Policy

Author

Elena Georgescu

Author
Elena Georgescu

TABLE OF CONTENTS

1.

INTRODUCTION

1. Introduction

Bring Your Own Device (BYOD) Policy refers to the trend of employees using their personal devices to connect to their companies' networks and accomplish their daily endeavours.

Before learning more about this policy, the dangers it imposes and what measures you can take to ensure the cybersecurity of your company, let us survey the history of the elements that made BYOD possible in the first place: the mobile devices and the Internet, as well as underlining the importance of cybersecurity.

1.1. Brief History of Mobile Devices

The (hi)story of mobile devices begins with the first twist given to letters communication: the introduction of telegraphs in the 1830s, which allowed messages to be transmitted through electrical channels. With telegraphs, communication could happen in hours, not days, but this was still not enough and way too expensive.

The sequel? The telephone - invented by the 29-year-old scientist Alexander Graham Bell. As How It Works explains, "Alexander Graham Bell's original telephone, patented in 1876, worked by converting sound into an electrical signal via a 'liquid transmitter'. This process centred around directing sound through a receiver and onto a thin membrane stretched over a drum. On the outside of the membrane a cork with a needle attached to a battery extended to a cup filled with sulphuric acid and a metal contact. When sound waves hit the membrane, it caused vibrations, varying the strength of the current passing between the needle and the contact. This created a varying strength electric signal that travelled down a wire to a receiver, where, through a reversed process, the sounds were re-created ." [1]

"Mr.Watson, come here - I want to see you!" are, apparently, the first words ever spoken through phone, as Science Musem notes. [2]

The 1891 year marked the invention of the first dial phone, when Almon Brown Strowger patented the automatic telephone exchange (dial service), thus eliminating the human switchboard operators necessary for making a phone call.

[1] The World Bank, 2020
[2] Science Museum, 2018

Other notable moments in the history of phones include:

- March 1926 - the first transatlantic phone call, made from London to New York.
- 1971 - the first mobile (cellular) phone is introduced by the Motorola employee Martin Cooper: "Communicating by radio waves, they permit a significant degree of mobility within a defined serving region that may range in area from a few city blocks to hundreds of square kilometres." [3]
- 1991 - second generation (2G) wireless telephone technology was introduced for the first time, in Finland. Encyclopaedia Britannica explains: "The analog cellular systems of the 1980s are now referred to as <<first-generation>> (or 1G) systems, and the digital systems that began to appear in the late 1980s and early '90s are known asthe <<second generation>> (2G). Since the introduction of 2G cell phones, various enhancements have been made in order to provide data services and applications such as Internet browsing, two-way text messaging, still-image transmission, and mobile access by personal computers."
- In the following year, 1992, the first text message was sent: it happened in England through Vodafone's GSM (Global System for Mobile Communication).

The 21 st century brought other significant additions to the communication revolution started in the 19 th : the 4G and 5G technologies. 4G devices provide, among others, mobile broadband Internet access and cloud computing. 5G is still under development at the moment, but it should offer several hundreds of thousands of simultaneous connections, better coverage and enhanced signalling efficiency.

Besides mobile phones, tablets are another type of devices commonly used in companies that adopt the BYOD policy. Tablets' history began decades before Apple's first iPad was launched in 2010. The first example of this revolutionary device was the Linus Write-Top in 1987.

It was the first handwriting-recognition tablet, on which you could write using its stylus. Two years later, the GridPad was launched.

Running MS-DOS, it caught the attention of the army - military bought a few of Jeff Hawkin's device, but it was pricey and heavy, so consumers mostly ignored it.

The next important step in the history of tablets came in 1993, when Apple launched the MessagePad.

It wasn't designed to replace the PC, but as a PDA (personal digital assistant) that would help you take your Calendar, To-do list and a few other applications with you wherever you go.

[3] Encyclopaedia Britannica, 2017

Microsoft took its chances with tablets too, and in 2000 Bill Gates introduced its first tablet prototype, which looked very similar to what we have today.

After Microsoft's Windows XP Tablet, Motion Computing LS800 si Lenovo ThinkPad of the mid 2000s, Steve Jobs introduced the iPad in 2010. With its delicate touchscreen, it won the heart of many customers and brought Apple millions of dollars.

From this point, the rest is history in the making, since many other companies continue to experiment in order to bring the public their best and most innovative variant of tablets.

1.2. Brief History of Mobile Devices

As the Internet Society says, "The Internet has revolutionized the computer andcommunications world like nothing before. The invention of the telegraph, the telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure." [4]

There could be hundreds of pages written about the Internet's history - since this is not the subject of this paper, I will resume to mentioning only a few milestones:

- the necessity of communication over a connected, distributed network starts to be felt during the Cold War. In the 1960's ARPA (Advanced Research Projects Agency) started working at ARPANET. ARPANET eventually connected military installations and certain US universities.

- the first message over ARPANET is sent from the University of California, Los Angeles, to Stanford University: "It was 10:30pm on October 29, 1969. The first message ever sent? <<LO.>> They were trying to type LOGIN, but it crashed before they could finish." [5]

- by the late 1980's, universities from around 25 countries were connected through the ARPANET.

[4] Brief History of the Internet, 1997
[5] GIZMODO, 2014

- in the late 1980's and early 1990's, more and more universities, businesses and even regular people got connected, as internet protocols and technologies were standardized.

- in 1989, Berners-Lee, "a researcher working at CERN, the Swiss nuclear research facility, came up with the concept of the World Wide Web , a decentralized repository of information, linked together and shareable with anyone who could connect to it. He built the first web page in 1993." [6]

- in the early 1990's, the first browsers were created: Nexus, Mosaic, Netscape Navigator.

- 1991 - the first wireless Internet access is possible due to mobile broadband connection as part of the second generation (2G) of mobile phone technology.

1.3. Importance of Cybersecurity

Cybersecurity refers to the measures that an individual or a company adopts to protect endpoints and systems against unauthorized access or attacks.

Cybersecurity refers to the measures that an individual or a company adopts to protect personal information, sensitive data, personally identifiable information, intellectual property.

Cybersecurity refers to the measures that an individual or a company should adopt in order to avoid: economic costs, reputational costs, regulatory costs.

These are the reasons why cybersecurity is important and should never be neglected. For the maximum of benefits, it should be applied on two dimensions:

- an educational one, since everyone in your company should be aware of cyberattacks' and social engineering's risks and what they can do to prevent them, and

- a technological one, by choosing the best software solutions to protect your home / company.

[6] Quartz, 2019

2.

BYOD POLICY

2. BYOD Policy

As we have seen, humanity had quite a journey before being able to do what maybe today we take for granted: call a friend who lives abroad, communicate with a business partner within seconds through instant messages or immediately access the Internet on our mobile phones to find out whatever we need. We can also use our mobile devices for work purposes - this implies some serious risks and should not be treated lightly.

2.1. Definition

Bring Your Own Device (BYOD) is a policy that allows employees to access work-related networks and systems using personal devices like laptops, smartphones, tablets, even IoT gadgets: smartwatches, fitness trackers, e-readers, game consoles or even printers.

The use of BYOD policy is "expected to surpass USD 350 billion by 2024. [...] It has been observed that employees prefer using one device only, for their professional and personal use. This prevents inconvenience caused by separate devices and reduces thefts. Furthermore, the need to switch between personal and work devices also gets eliminated. Such a trend lowers the hardware & device costs for a company. Since devices are personally owned, employees are better acquainted with them. This boosts their productivity at work and also increases employee satisfaction." [7]

2.2. Benefits & Disadvantages

As it probably happens with everything in this world, BYOD policy also has advantages and disadvantages. Here are its implications for a business:

Benefits

- Reduced costs

As probably many people already own a smartphone, companies which apply the BYOD policy will save the money that would normally be used for phones and laptops.

[7] Hexa Research, 2016

Moreover, people also tend to take more care of personal devices than of the ones that their company provides and it might be convenient to carry and take care of a single device instead of two.

- Employee productivity

BYOD policy can reduce the time of employees learning new technologies or operating systems: one, for example, can be familiar with Android, another one with iOS. By reducing the learning curve, they can immediately start accomplishing their tasks in a productive manner. Moreover, although it might not be recommended for the work-personal life balance, having all the tools they need already in their pockets allows employees to handle emergencies faster, wherever they are.

- Staff satisfaction

A BYOD policy encourages work flexibility, which is related to how satisfying employees find their job. BYOD policy gives people a chance to decide how they work, to use better devices than the ones that their company would provide them and it also makes it easier for them to work remotely, which in 2020 has become a necessity.

Disadvantages

- High (or even higher) security risks

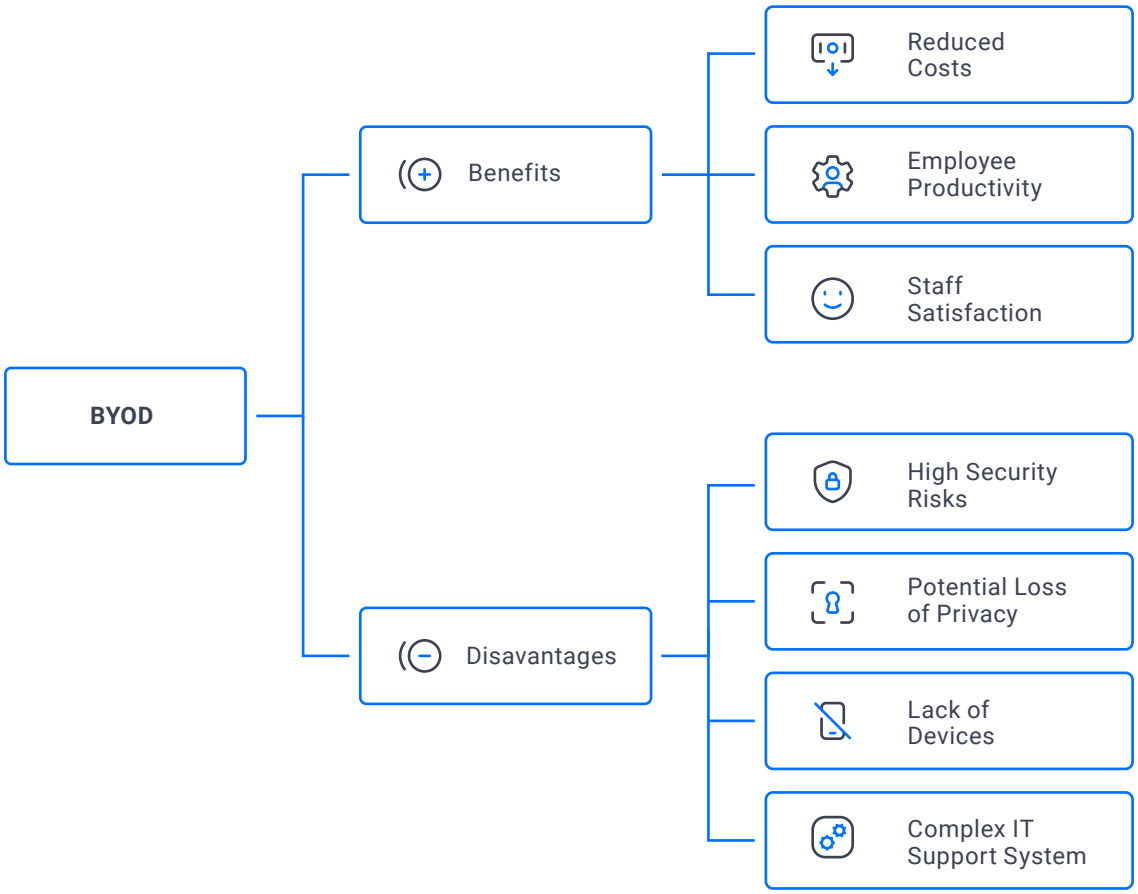
Handling the cybersecurity of a company is no easy task - you must have the proper solutions installed, an antivirus, a powerful firewall, an email protection solution. Despite this fact, it's quite easy to make them mandatory on company devices, but how do you make sure that your employees keep their personal devices (and your company's data) safe?

- Potential loss of privacy

It's easy for a company to write guidelines regarding the use of company devices in order to protect its sensitive data and information, but doing the same for personal devices it's not, since so many aspects (that we would further discuss) should be taken into consideration. Moreover, it's also important how you handle confidentiality when employees who have used their own devices leave the company and what should be done in case their devices get lost or stolen. For avoiding any problems, the matter of data privacy should be discussed before employees start to use their own devices for work purposes.

- Lack of devices and the need of a more complex IT support system

Although it's true that some people may have better devices than the ones that a company would provide, it's also true that some may not. How will a company deal with this possibility? Also, how should it deal with device issues - will the IT support team offer their help over the phone, should the employees go to the office? These questions are particularly important especially in this pandemic context.



2.3. BYOD Threats

Hereinafter, let us have a closer look at the threats that a BYOD policy implies:

- Cross-contamination of data

If the employees, by applying the BYOD model, store private and company data in the same place, data cross-contamination might happen: sensitive and important business data can get accidentally deleted or exposed, and private data can accidentally be shared in the company's system.

- Lack of management and outsourced security

With any private mobile device used, companies risk loss of management and control - it's difficult to control whether the employees connect to a secure network, for example, or whether their devices get lost or stolen.

Letting aside these unfortunate, but plausible scenarios, there is also the problem of outsourced security - how do you control if the employees update their devices in time and from the correct source? Mobile devices can get attacked in various ways (that we'll be discussed in the next chapter of this paper), and the IT support teams might not be able to do anything to prevent or remediate the damages.

- Insecure use and device infection

As mentioned above, employees might connect to an insecure public Wi-Fi network or skip reading applications' terms of service and allow external parties to use their devices, thus providing access to confidential business data. Smartphones and tablets can get infected without their owners even realizing it until it's too late.

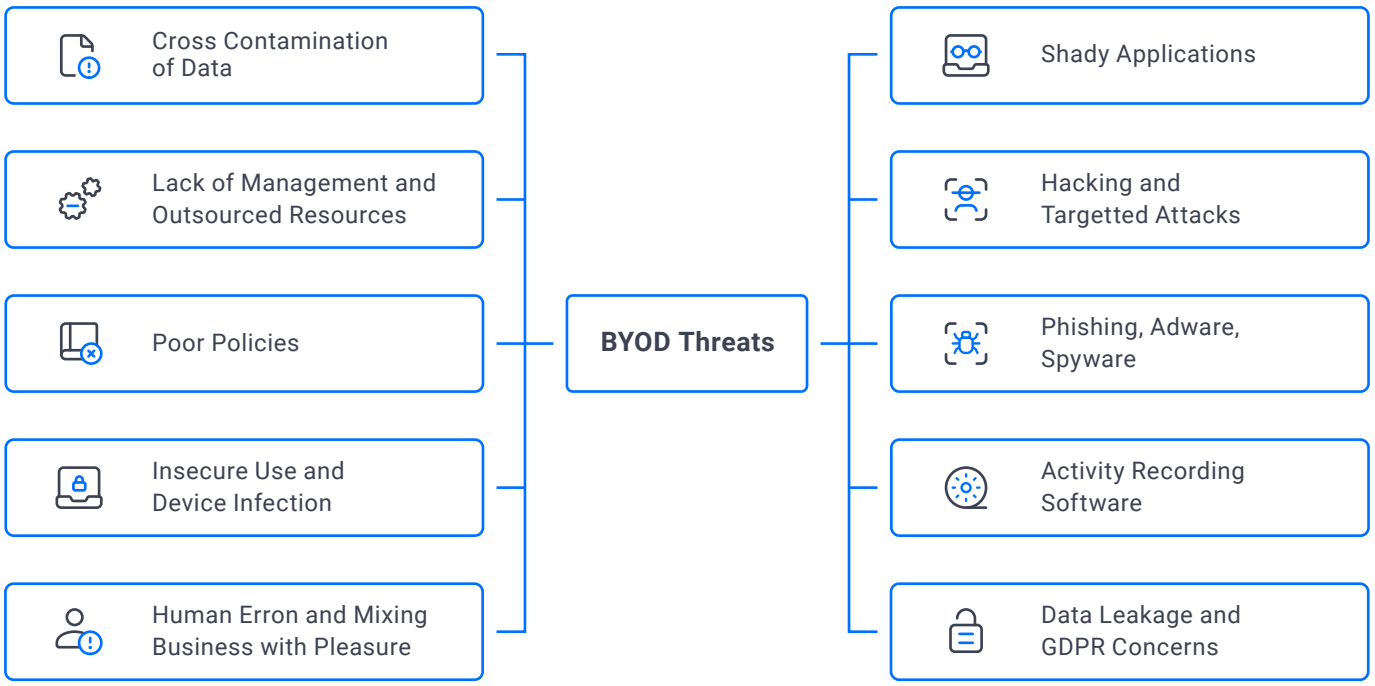
- Human error and mixing business with pleasure

When it comes to BYOD, human error can take many forms and company managers should not be mistaken - all the forms have great chances to materialize. Employees could lose their devices or leave them unlocked in public places. They could shop online from compromised websites or loan their devices to friends.

- Data leakage and GDPR concerns

Within the BYOD policy, employees might have access to sensitive customer data - and in this GDPR era, it is of

paramount importance to protect them. Customer's data can be lost or exposed, and this has massive moral and legal implications. As DataPrivacyManager writes, "GDPR represents the most groundbreaking and wholesome data protection regulation and imposes huge fines in order to protect the privacy of an individual." [8]



- Shady applications

Not all mobile device applications are as harmless as they are perceived - shady applications can get complete control over a device, thus opening the path for surveillance, unexpected charges or loss of personal and work information.

- Hacking and targeted attacks

Hackers will always find ways to take advantage of poor security measures to get into the enterprise network, where they will try to carry on with their malicious plans: scanning for other vulnerable devices, look for sensitive data, steal stored information, access systems and servers and so on. All this can happen by chance, but targeted attacks are not uncommon either.

[8] Data Privacy Manager, 2020

- Phishing, adware, spyware

As defined in the Heimdal™ Security's Cyber Security Glossary, these terms refer to:

Phishing:

" Phishing is a malicious technique used by cyber criminals to gather sensitive information (credit card data, usernames and passwords, etc.) from users. The attackers pretend to be a trustworthy entity to bait the victims into trusting them and revealing their confidential data. The data gathered through phishing can be used for financial theft, identity theft, to gain unauthorized access to the victim's accounts or to accounts they have access to, to blackmail the victim and more."

Adware:

" Adware is a type of software that delivers ads on your system. Usually, these pop-up ads appear while visiting sites, like annoying pop-up ads or banners. They come in "bundle" versions with other applications. Most types of adware are not dangerous, maybe a bit annoying since they deliver pop-up ads while visiting a website, but there is another dangerous form of adware that delivers spyware, which can track down your activity and retrieve sensitive information."

Spyware:

" Spyware is a type of malware designed to collect and steal the victim's sensitive information, without the victim's knowledge. Trojans, adware and system monitors and are different types of spyware. Spyware monitors and stores the victim's Internet activity (keystrokes, browser history, etc.) and can also harvest usernames, passwords, financial information and more. It can also send this confidential data to servers operated by cyber criminals, so it can be used in consequent cyber attacks." [9]

- Activity recording software

Although there is no clear evidence of devices being able to listen to the users' conversations, it has been discovered that apps can send "screenshots and screen recordings of user activity to unrecognized destinations. Among the data collected were zip codes and user login credentials. In many cases, users had no idea that apps were recording their behavior. The researchers determined that most recordings were benign. They simply tracked user behavior and preferences to optimize the performance of the app. Nonetheless, these findings

[9] Heimdal Security

highlight the ease with which a malicious body could potentially collect information from a mobile device. A seemingly innocent app could capture and distribute personal information, passwords or private messages without the knowledge of the user." [10]

- Poor policies

As probably everyone can imagine so far, implementing a BYOD program without effective security policies is certainly risky. In order to be compliant and avoid any issues, good security policies should take into account: passwords and lock screens, authentication, network connectivity, use of a VPN, location tracking, updates and patching, mobile device management. More about this in the following lines.

2.4. BYOD Best practices

As we have seen, BYOD implies various and multiple risks. For this reason, any management team who wants to use BYOD in their company should be acquainted with the best BYOD practices. A few examples:

- Pro's and Con's

The first step when talking about the implementation of a BYOD policy is to decide whether BYOD is right for your organization in the first place. Although BYOD does save a company money and gives employees a greater flexibility, it might not be the best idea if you have above-average risks concerns. Take your times to think of BYOD's benefits and disadvantages.

- Policy on paper

If you decide that BYOD might be a fit for your company, make a plan and put it on paper before implementing it. This plan should include: goals, acceptable use, governance and practices monitoring. Everything should be noted in only 1-2 pages - because you do want your employees to read it thoroughly.

- Acceptable devices

It would be useful to make a list of what devices would be acceptable for BYOD - which Android smartphones and what specific iPhone models. When creating the list you should consider what devices do employees already own and what devices you can effectively monitor.

[10] Corrata, 2018

- Company and personal data division

Company and personal data division is essential if you want to prevent a data breach. You should make it clear that a BYOD policy implies risks of information loss and that employees have a role in preventing it, but also provide specialized apps that can separately contain the company data. It is recommended to use apps that can be remotely deleted in case a device is stolen or lost.

- Personal data protection plan

BYOD also means you have to make sure that you do not violate your employees' private data. Your device management software should never interact, copy or store an employee's personal data and apps.

- Data usage monitoring process

If your employees travel often, they might exceed their personal data plan, so setting up a data usage monitoring process is an important step of implementing BYOD policy. Make sure you design a reimbursement process so you can cover higher-than-usual data charges.

- Zero-Trust model

The Zero-Trust model is "a concept based on the notion that organizations should not trust anyone or any device by default and thus, they must verify every single connection before allowing access to their network. This model came as a response to former security approaches founded on the assumption that insider threat was nonexistent and that were only focusing on defending organizations from external threats." [11]

Multi-factor authentication, encryption and privileged access management are some of the Zero-Trust model's pylons. According to them, resources must be accessed in a secure manner disregarding the location and all traffic must be inspected and logged.

- MFA & RBAC

Multi-factor authentication (MFA) and role-based access control (RBAC) are essential for the cybersecurity of your company. Every individual should pass multiple levels of identity verification to access corporate resources and every individual should only access the tools and information required by their specific role.

[11] Bianca Soare, 2019

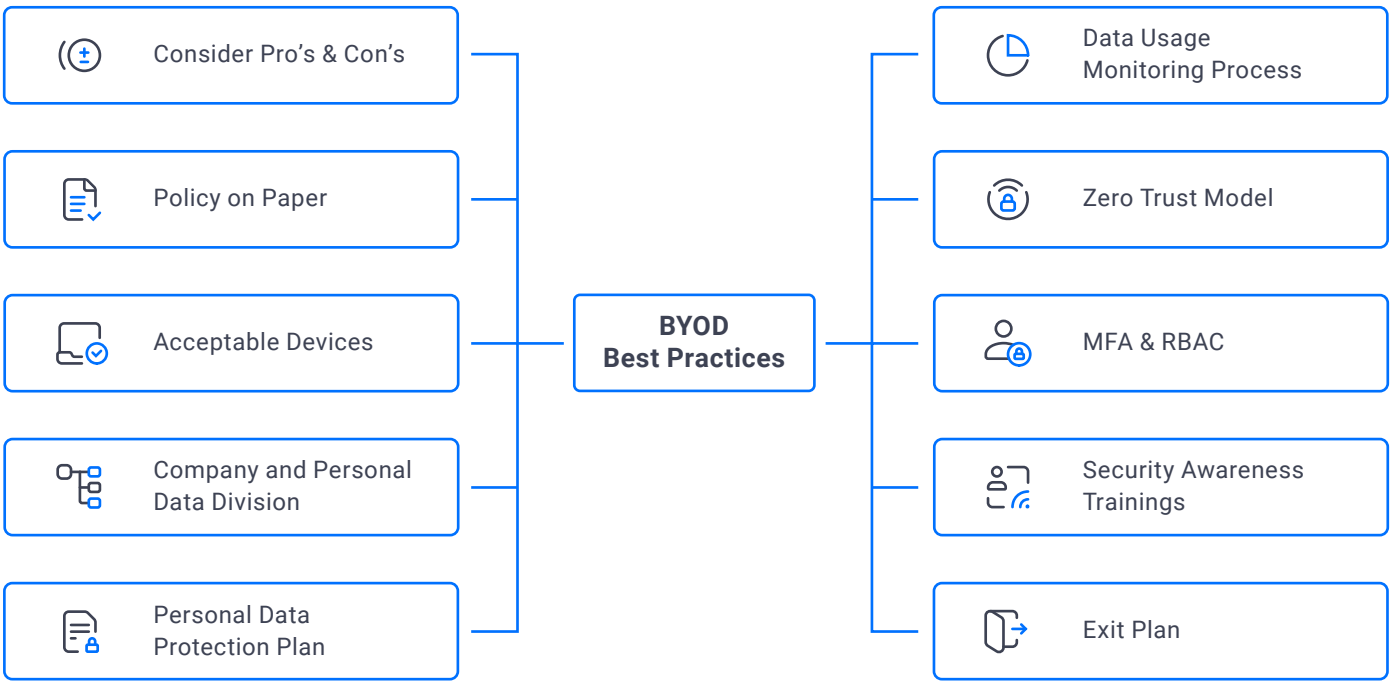
Besides downsizing insider threat risks and increasing overall visibility over authentication protocols, the implementation of the RBAC model will also help you to achieve complete compliance with various rules and regulations, including GDPR.

- Security awareness trainings

Regular awareness training is essential not only because they educate employees on cybersecurity matters - it also places corporate responsibility on their shoulders. These sessions should require full participation and attention and should include information on how to reduce risks, but also what to do in case of a data breach.

- Exit plan

Employees might lose their devices. Employees' devices might get stolen. Employees might leave your company. You must have a plan for all these possible situations, you need to have protocols in place to make sure no company data is lost, including the ability to remotely delete corporate data from the devices.



2.5. BYOD and the Times We Live In

2020, the year in which this paper has been written, has brought humanity a new challenge: the COVID-19 pandemic. The new coronavirus was first known to wreak havoc in China, and afterwards it spread to all the corners of the Earth, reshaping the way we live and work by forcing us to practice social distancing, move various real-life events online and work from home - if possible -, speeding up the digital transformation by 5.3 years. [12]

While remote work was, before COVID-19, a procedure that only a few companies allowed or encouraged, in the past few months it has become a necessity - wherever the nature of the activity allows it, people move their work remote and learn to deal with all the challenges that come with such a shift.

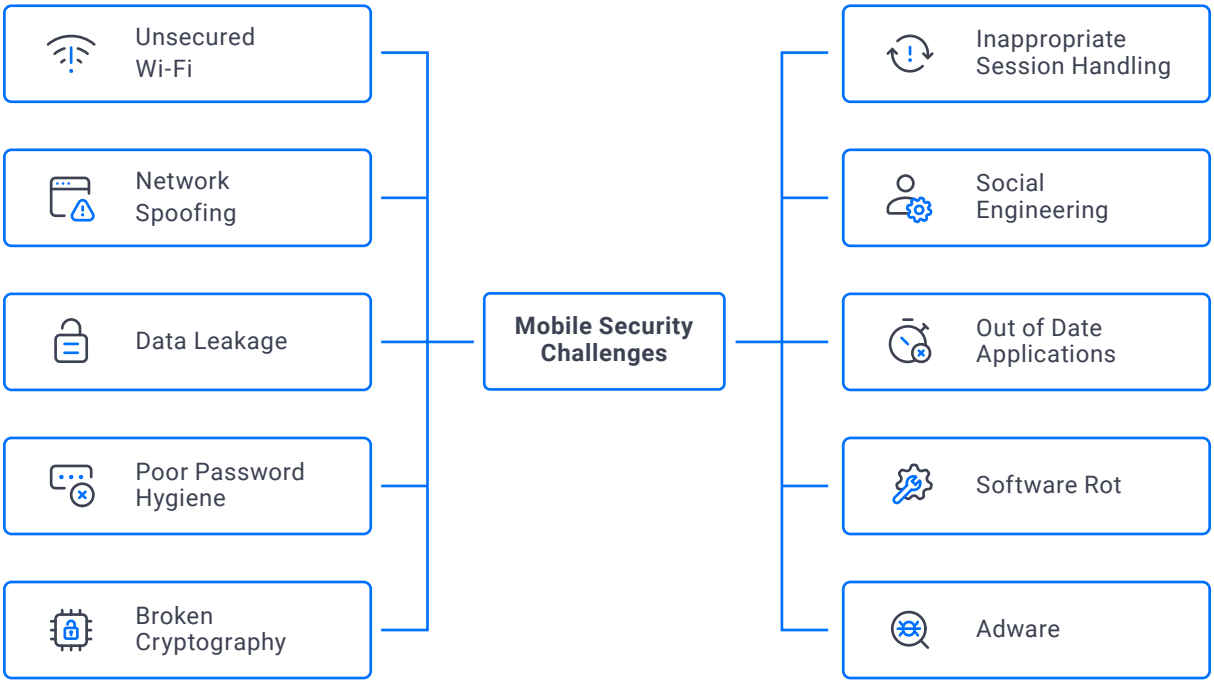
Although WFH policy reduces long commutes, pollution and overcrowding, when it is combined with BYOD it presents multiple cybersecurity threats. The task to reduce these threats falls both on the employer's and the employees' shoulders. For this reason, it's important to choose the best practices for BYOD and to know the risks that mobile devices impose.

[12] Anasia D'mello, 2020

3.

MOBILE SECURITY CHALLENGES

3. Mobile Security Challenges



Whether your mobile devices work on Android or iOS, there are a few aspects that threaten their security. You'll find them mentioned here before diving into more specific details according to the most common operating systems.

- Unsecured Wi-Fi

Free Wi-Fi networks are dangerous because they are usually unsecured. They should be used with caution, and never for accessing confidential information or personal services, like banking or credit card operations.

- Network spoofing

Network spoofing is related to the free Wi-Fi threat, because it consists of hackers creating fake access points that seem to be Wi-Fi networks in high-traffic public locations. Users might be required to create an account for accessing them, which is dangerous because, unfortunately, the password they would set might be used for other accounts too - and these accounts would thus be at the hackers' disposal.

- Data leakage

Data leakage can occur due to riskware (a general concept referring to legitimate programs that are potentially risky because of software incompatibility, security vulnerability or legal violations) applications that are granted or ask for more permissions than needed, but also as a result of user error. Company files could get uploaded into a public cloud storage service, confidential information can be pasted in the wrong place and emails can be forwarded to unintended recipients.

- Broken cryptography

Cryptography is a crucial element for many cybersecurity models: it "applies algorithms to shuffle the bits that represent data in such a way that only authorized users can unshuffle them to obtain the original data. Cryptographic algorithms use mathematics to achieve effective shuffling. Most common cryptographic standards are open where the algorithms are known and published, but the clever mathematics make it impractical to decode the shuffled bits. Open standards help ensure cryptography is secure."[13] Broken cryptography can appear if developers use encryption algorithms with known vulnerabilities or leave flaws in other parts of the code that can be discovered and exploited by hackers.

- Inappropriate session handling

Many times, applications use tokens for mobile device transactions in order to allow users to perform multiple actions without having to re-authenticate. Secure applications should generate new tokens with every access attempt / session and these tokens should be confidential. However, session tokens might be unintentionally shared with malicious actors.

- Social engineering

Many people always have their phones nearby and use it much more than they use a laptop, for example, in their free time. They browse on the internet, talk to friends and colleagues, read emails on the phone - and hackers dealing with social engineering (a cyberthreat that relies on human nature and the errors people are likely to commit) know this. For this reason, phishing is still a very effective cyber attack. The mobile devices offer phishing the perfect environment for avoiding detection: smaller screens, limited display of information (especially in the notifications), a sense of familiarity.

[13] The University of Rhode Island, 2016

- Out-of-date apps / software rot

Software rot, "also known as bit rot, code rot, software erosion, software decay, or software entropy is either a slow deterioration of software quality over time or its diminishing responsiveness that will eventually lead to software becoming faulty, unusable, or in need of an upgrade."[14] The concept is related to legacy software, which refers to "any piece of software that can't receive continued patching or support from its developer, or can't meet the compliance standards in use."[15] Out-of-date applications can present many vulnerabilities, so patches are essential for mobile devices cybersecurity.

- Poor password hygiene

Although advice on how to create a strong password can be found on every sign-up page, on probably every platform or application, many still use the same password for multiple accounts and choose incredibly easy to hack combinations, not to mention that they probably don't even know about the 2-factor authentication concept. In the context of BYOD, imagine how serious it is if the same password is used for a personal and a company account.

- Adware

Mobile advertising has brought cybercriminals millions of dollars in the past few years and it will continue to do so if users do not pay attention, because adware functions in a pretty simple way: it consists of malware that generates clicks on ads hiding in the background of legitimate apps. Although the mobile advertising industry is the one that loses the largest amounts of money due to adware, it can also affect the users - the mobile device's performance slows down, its battery gets drained, and higher data charges or overheating appear.

3.1 Android

As we have seen, there are certain cybersecurity threats that apply to all mobile devices. There are some, though, that are specific only to Android operating systems and iOS. In this section the Android vulnerabilities will be mentioned.

Although firstly released by Google in 2008, Android has soon become the most popular choice on the market, due to its intuitive interface and various connectivity options.

[14] Wikipedia
[15] Miriam Cihodariu, 2019

However, users should pay attention to certain aspects:

- Permissions

Android protects users data from exploitation by operating on the principle of permissions - applications can access hardware and data only if and when they are given permission, and the system maintains a list of permissions for each application installed on the device. Also, "the system resets the permissions of unused apps that target Android 11 or higher, and apps might need to update the permissions that they declare if they use the system alert window or read information related to phone numbers." [16]

Android permissions range from normal (e.g. ACCESS_WIFI_STATE, BLUETOOTH, BLUETOOTH_ADMIN, INTERNET etc.) to dangerous (READ_PHONE_NUMBERS, CALL_PHONE, ANSWER_PHONE_CALLS, SEND_SMS, RECEIVE_SMS, READ_SMS etc.) and can be abused in multiple ways.

- Banking Trojans

Banking Trojans are a type of malware designed to gain access to confidential information stored or processed by online banking systems. It can pose as a legitimate piece of software until it's installed, or it can get user credentials by spoofing a financial institution's login webpage. Banking Trojans can be used to harvest sensitive data, spy on the users' activity, delete files, download more malware etc.

- Component-Based Threats

Apart from applications, cybercriminals also target Android software and components, like Wi-Fi or Bluetooth. The biggest threats here are highly-customizable malware tool kits and phishing-type attacks.

- Third-Party App Stores

Third-Party applications are particularly dangerous to Android devices because they are not controlled or at least verified by Google, so they might produce serious infections.

- Keyloggers

Keystroke logging refers to the act of tracking and recording every keystroke entry made on a computer. A keystroke means any interaction users make with a button on the keyword.

[16] Android Developers

The keyloggers (the devices/programs used for keylogging) are interested in the name of the keys but also in the length, time and velocity of the keypress. According to the degree of knowledge that users have about keylogging and the purpose for which it is used, keylogging can be legally acceptable, morally questionable or a criminal activity.

3.2. iOS

iOS is the operating system that runs on iPhones and iPod. It was initially called iPhone OS and first appeared in 2007-2008. Although iOS soon enjoyed greater success than anyone imagined, the mobile devices that use it do share a list of most common attacks and threats.

- Applications vulnerabilities

It may happen that the information stored by applications on the device to be unencrypted or include poorly encrypted access codes. This information can easily be extracted over a Wi-Fi network through various methods.

- Images

Images (in formats like .JPEG, .BMP etc.) can also spread malicious code if the users click on them. For iOS users, this is particularly dangerous because malicious .exe files (Trojans, malware, spyware) can be inserted into images that appear in the Safari browser.

- iOS surveillance and Mobile Remote Access Trojans (mRAT)

Surveillance software and mRAT can be installed on iOS devices when the device is jailbroken - an operation that removes Apple's software restrictions. Jailbroken devices allow access to the root within the operating system and the installation of software that cannot be found on iOS App Store. To install malware on an iOS device, cybercriminals can jailbreak it by obtaining physical access or by propagating the code through a USB cable.

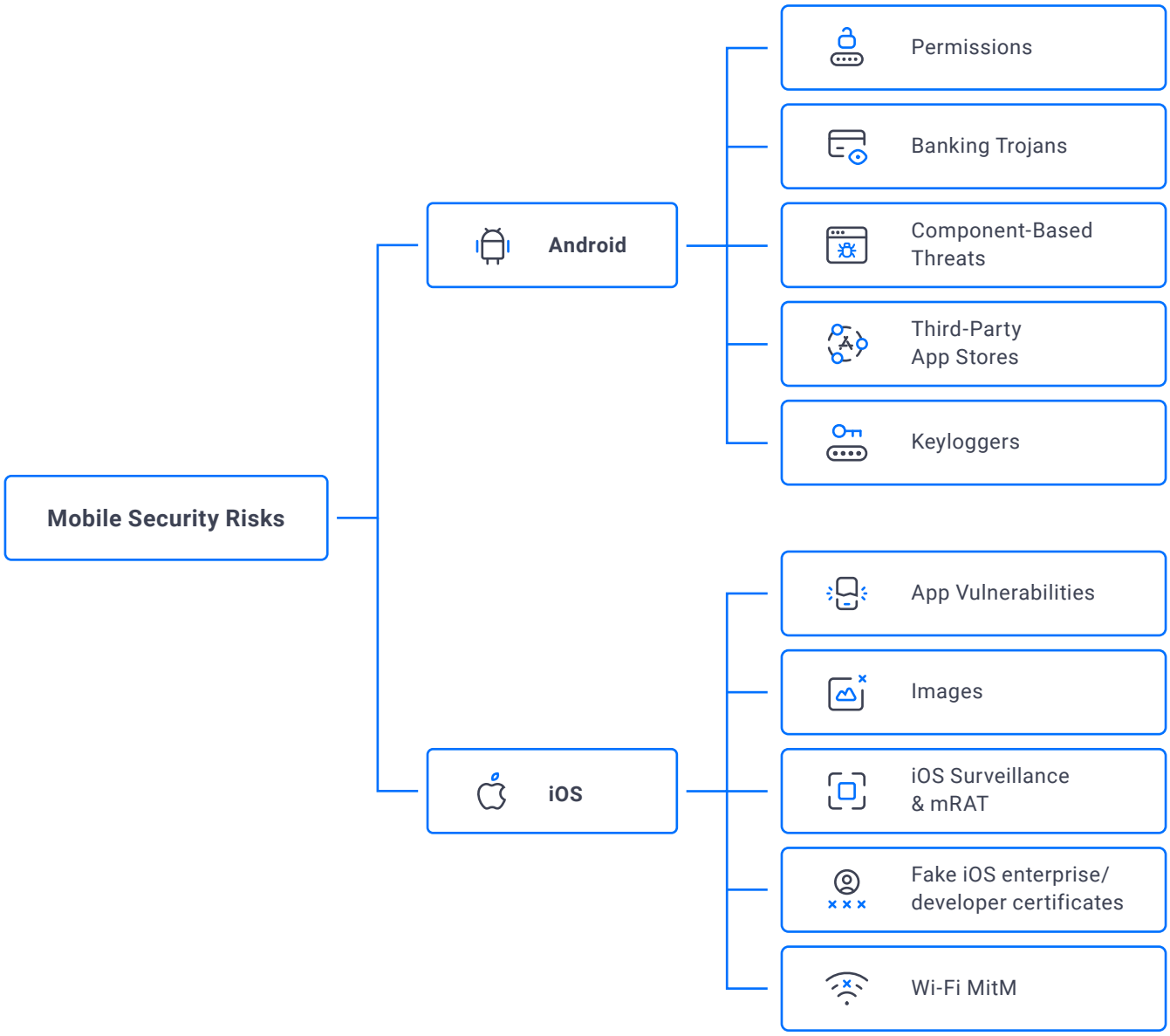
- Fake iOS enterprise or developer certificates

In theory, every iOS application should be signed by a trusted certificate before reaching the App Store. In practice, cybercriminals can steal or buy a certificate for their malware on the black market. If they succeed, a dangerous application can seem completely legitimate and be available for download.

- Wi-Fi Man-in-the-Middle (MitM)

Typically, in a man-in-the-middle attack a malicious player inserts him/herself into a conversation between two parties, impersonates both of them and gains access to the information that the two parties were trying to share. The malicious player intercepts, sends and receives data meant for someone else – or not meant to be sent at all, without either outside party knowing until it's already too late.

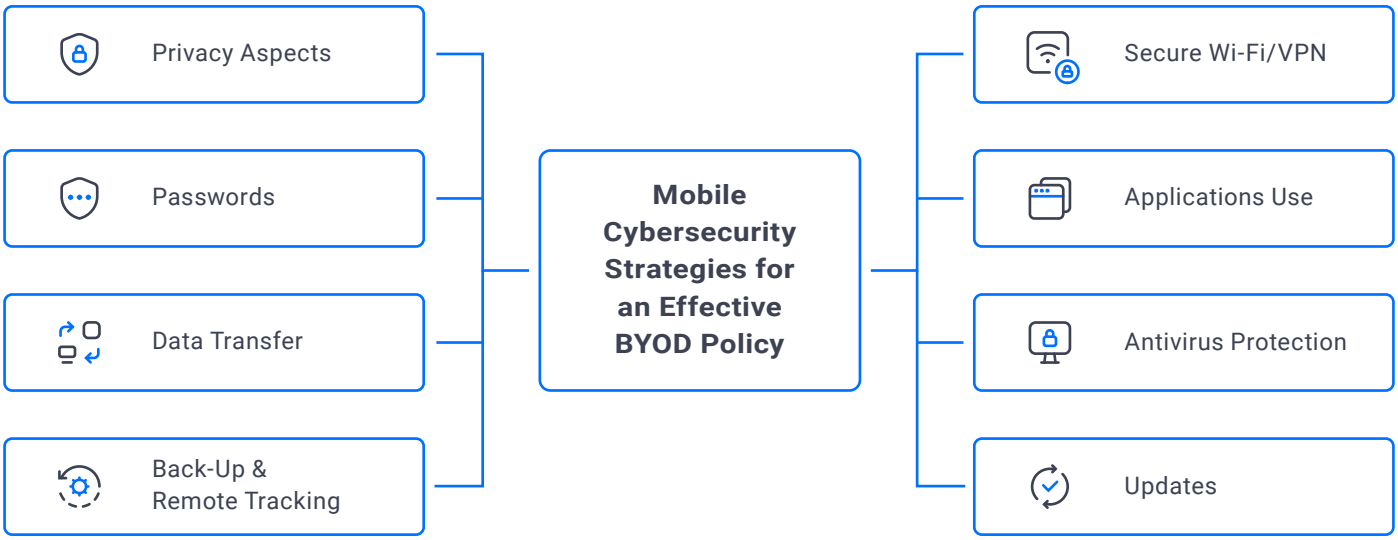
A mobile Wi-Fi MitM attack takes place when a device connects to a subversive Wi-Fi hotspot, which means that the cybercriminals can intercept and even alter the network's communication.



4.

MOBILE CYBERSECURITY STRATEGIES

4. Mobile Security Challenges



As we have seen, mobile devices are not safe from cyberthreats, and this is even more dangerous in the context of BYOD. Here are a few sugestions on how to keep your mobile safe in order to have a successful BYOD policy:

- Privacy aspects

Measures should be taken to ensure both the protection of company data and the privacy of the mobile device's owner. The two should remain separate and the employees should be given since the beginning the set of rules that govern their company's BYOD policy. Containerization could be a good option for keeping things separate: the term refers to a method in which a portion of the device is segregated into its own protected area, with a separated password and a separated set of rules. When users log into the containerized area, the personal applications and the other features not managed by the container will be inaccessible.

- Passwords

Passwords are an essential security procedure - anything related to company data should be password protected, but so should be the device itself, in order to avoid infelicitous incidents. Do not leave your mobile device without a lock screen and choose the shortest amount of time of how long can the phone be idle before locking. It would also be recommended to update your notification settings to only show previews when the device is unlocked.

- Data transfer

There could be serious legal ramifications if someone transfers data through an unapproved application and that application gets breached. Business data should be password protected, encrypted, and transferred only through company-approved applications.

- Updates

Mobile phone operating system updates are intended to improve performance but also to enhance security. It's important to install the updates as soon as they're available and not postpone them indefinitely.

- Secure Wi-Fi / use VPN

Both business data and private information would be safer if users would only connect to secure Wi-Fi networks. For the moments where there are only free (and probably shady) Wi-Fi networks available, the best option would be to use a VPN that can protect your location and device information.

- Applications use

Whether we talk about Android or iOS, applications represent one of the biggest cyberthreats for mobile devices. It's important to only download them from trusted sources, to read other users' reviews and to pay serious attention to the permissions they require. Delete all applications that you do not use and remove browser cookies often.

- Install an antivirus

Your mobile devices should benefit from antivirus protection too. Anti-phishing, privacy adviser, safe browsing mode or SIM lock up, that will lock down the device when the SIM card is removed would be very useful features to look for.

- Back-up & remote tracking

Unfortunately, accidents happen - mobile devices can get lost, stolen or destroyed. Consequently, the importance of (cloud) back-ups should not be neglected. It would also be useful to always enable the remote tracking setting, which also allows you to remotely wipe the smartphone's data if it's stolen and cannot be retrieved.

5.

CONCLUSION

5. Mobile Security Challenges

Mobile devices represent a revolutionary invention, one that has simplified and refined people's lives in various ways: they have made communication easier, have brought people closer and multiple services at our fingertips.

Moreover, mobile devices also allow us to stay close to our work tasks and calendar and to maintain a proper communication with our work colleagues, by having our business email and other enterprise applications directly on our phones and in our pockets.

As we can all imagine, BYOD policy is a great procedure to have in place particularly in the special context of a pandemic like the one we face today, when many companies have had to turn to remote work, but it does not come without cybersecurity risks. For that matter, proper planification and cybersecurity prevention strategies should be the best friends of any company that aims to make BYOD work for it, and not against it.

About Heimdal™ Security

Heimdal™ Security is an emerging cyber security provider with extensive experience in developing solutions that actively prevent, identify, and mitigate threats. We provide AI-driven DNS-protection at the endpoint and network-levels, automated vulnerability and patch management, email security, and Next-gen Antivirus, and our solutions can be scaled up and tailored to fit business's specific needs. Contact us for more information!

6.

BIBLIOGRAPHY

6. Bibliography

VoIPTech Solutions, "The Evolution of Telecommunication Technology", 2019.
https://voiptech.solutions/the-evolution-of-telecommunication-technology/

M-STAT, "The Evolution of Telecommunications" , 2015.
https://www.m-stat.gr/the-evolution-of-telecommunications/

How It Works, "How Bell's Telephone Worked", 2012
https://www.howitworksdaily.com/how-bells-telephone-worked/

Science Museum, "Ahoy! Alexander Graham Bell and the First Telephone Call", 2018
https://www.sciencemuseum.org.uk/objects-and-stories/ahoy-alexander-graham-bell-and-first-telephone-call

David E. Borth, "Mobile Telephone". Encyclopaedia Britannica, 2017
https://www.britannica.com/technology/mobile-telephone#ref1079062

Julie Bort, "The History of the Tablet, An Idea Steve Job Stole and Turned Into a Game-Changer". Business Insider, 2013
https://www.businessinsider.com/history-of-the-tablet-2013-5#apples-first-tablet-was-the-messagepad-in-1993-3

Matt Novak, "The First Internet Message Ever Sent Was <<LO>>" . Gizmodo, 2014
https://gizmodo.com/the-first-internet-message-ever-sent-was-lo-1597681715

Hexa Research, "BYOD (Bring Your Own Device) Market Analysis, Market Size, Application Analysis, Regional Outlook, Competitive Strategies and Forecasts, 2016 to 2024", 2016
https://www.hexaresearch.com/research-report/bring-your-own-device-byod-industry

Data Privacy Manager, "5 Things You Need to Know about Data Privacy", 2020
https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

Heimdal Security, "Glossary"
https://heimdalsecurity.com/glossary

Colm, "Spyware and Adware Attacks Threaten BYOD Policies". Corrata, 2018
https://corrata.com/spyware-attacks-threaten-byod-policies/

Bianca Soare, "What Is the Zero Trust Model?". Heimdal Security (Blog), 2019
https://heimdalsecurity.com/blog/what-is-the-zero-trust-model/

Anasia D'mello, "COVID-19 Has Sped Up Digital Transformation by 5.3 Years, Says Study". IoT Now, 2020
https://www.iot-now.com/2020/07/23/104031-covid-19-has-sped-up-digital-transformation-by-5-3-years-says-study/

The University of Rhode Island, "Cyber Security and Cryptography". Computing Concepts, 2016.
https://computing-concepts.cs.uri.edu/wiki/Cyber_Security_and_Cryptography

Wikipedia, "Software Rot", 2020.
https://en.wikipedia.org/wiki/Software_rot

Miriam Cihodariu, "What Is Legacy Software and a Legacy System in Business + The Risks". Heimdal Security (Blog), 2019
https://heimdalsecurity.com/blog/what-is-legacy-software-system-risks/