

Synthesize a solution to a potential real-life scenario



PRIFYSGOL CYMRU

Y Drindod Dewi Sant

UNIVERSITY OF WALES

Trinity Saint David

Siobhan Kelly Stephens

3267 Words

January 2018

Internet Technology and Security

School of Applied Computing
University of Wales Trinity Saint David

Abstract

This report outlines a comprehensive Bring Your Own Device framework that covers all aspects of internal and external security of an organisation's corporate network. The policies outlined focus on the CIA triad, of confidentiality, integrity and availability, key principles of data security.

The threats to personal devices, corporate data and the corporate network, are discussed, and policies and protocols to mitigate against them are suggested. Technologies such as Mobile Device Management Software are recommended, and an MDM software, VMWare Workspace One, is selected and discussed.

An implementation of the corporate network has been created using Cisco Packet Tracer and its key features and assumptions are outlined. The challenges and advantages of BYOD are also debated.

Finally, the author summarises on the framework and suggests future improvements.

Table of Contents

1. Introduction	3
2. Related Work	3
2.1. Principles of Security	3
3. Implementation	4
3.1. Permitted Devices and Users	4
3.2. Authentication Process	5
3.3. Segregation of Personal and Corporate data	8
3.4. Physical Security	8
3.5. Protection of Data at Rest, in Use and in Transit	9
3.5.1. Data at Rest	9
3.5.2. Data in Use	9
3.5.3. Data in Transit	10
3.6. Device and User Monitoring	11
3.7. Incident Response	11
3.8. Redundancy and Resilience	12
3.9. Guest Network	13
3.10. Cisco Packet Tracer Implementation	14
3.11. Mobile Device Management Software Selection	15
4. Discussion	15
4.1. Advantages and Challenges of BYOT	15
5. Conclusion	16
6. Appendices	17
Appendix A	17
Appendix B	22
Appendix C	22
Appendix D	23
Appendix E	23
Appendix F	23

Appendix G

24

7. Bibliography

24

1. Introduction

The aim of the report is to develop a comprehensive Bring Your Own Device framework that covers all aspects of internal and external security of an organisation's corporate network.

A recent survey showed that 97% of organisations thought that incorporating BYOD schemes into their overall security policy is important, 37% believing that it is critical, and 40% believing it is extremely important, however 38% of these organisations don't have a formal policy around BYOD [1]. Also, according to this survey, only 25% of organisations forbid the use of personal devices [1].

It is therefore of high importance that robust policies, measures and protocols are put in place in order to protect invaluable intellectual and sensitive personal data [2].

2. Related Work

2.1. Principles of Security

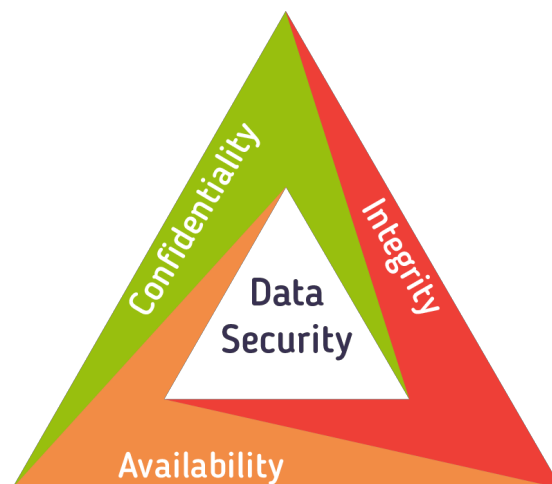


Figure 1. Data security principles [3].

The CIA triad, as pictured above in figure 1, is a model used to influence policies in IT security, and covers three areas, confidentiality, integrity and availability. It is “regarded as the pillars of security for any information system” [4].

Confidentiality “preserves authorized restrictions on information access and disclosure” [5] and aims to protect data privacy by implementing access control and authentication, often through the use of AAA (Authentication, Authorisation and Accounting).

Integrity ensures that data is accurate, consistent, and trustworthy, and is certified through the use of checks such as checksums. Digital signatures can be used to verify that a message was sent by the signer and that it has not been altered [6]. Data integrity can also be maintained through the use of hashing algorithms, such as SHA 256, and by applying a salt.

Maintaining availability means that users must be able to access data, services and resources. The five-nines (99.999%) of availability is a standard many large organisations aim to achieve, resulting in a downtime of less than 5.26 minutes a year [7]. High availability is achieved through proper maintenance of hardware, eliminating single points of failure, devising risk management and planning for disasters, and ensuring resiliency of a network through redundant hardware [4].

Another principle, not stated on the CIA triad, is accounting, which is defined as the traceability of user and device actions on a network or system, which can be used in the case of a litigation [8].

The principles outlined above must be considered to create a balanced and comprehensive security framework.

3. Implementation

3.1. Permitted Devices and Users

Appendix A.1 states that employees must have authorisation to join Hyper-fort’s BYOD scheme, A.2 states that devices must be inspected before acceptance onto such a scheme, and will be subjected to random spot checks, and A.3 outlines the permitted device list. By only allowing a controlled group of device types and versions, and ensuring them and their contents are up-to-date, the risks that occur from security loop-holes such as malware infections and zero-day attacks will be minimised. The acceptance of only genuine chargers is to reduce the risk of electrical failure that can arise from the use of unregulated electronic devices. Jailbroken

or rooted devices are not permitted as they may be able to bypass the Mobile Device Management Software (MDMS) and therefore compromise security.

A record of all employees and their registered devices will allow accounting of a device and its activity on the network, which is necessary for legal and moral culpability, and is the reason for the policy implemented in Appendix A.4, stating that devices will not be granted access to the network until authorised and that an up-to-date list of devices must be maintained.

The policy outlined in Appendix A.5 states that users must agree to the installation of MDM and anti-virus software onto their device. MDM software is critical to the proposed framework, as it allows monitoring, management and security of BYO devices, and will be covered in more detail later in this report. Up-to-date anti-virus software will aid in the detection and prevention of malware.

3.2. Authentication Process

The process of joining Hyper-fort's BYOD scheme is shown below in figure two.

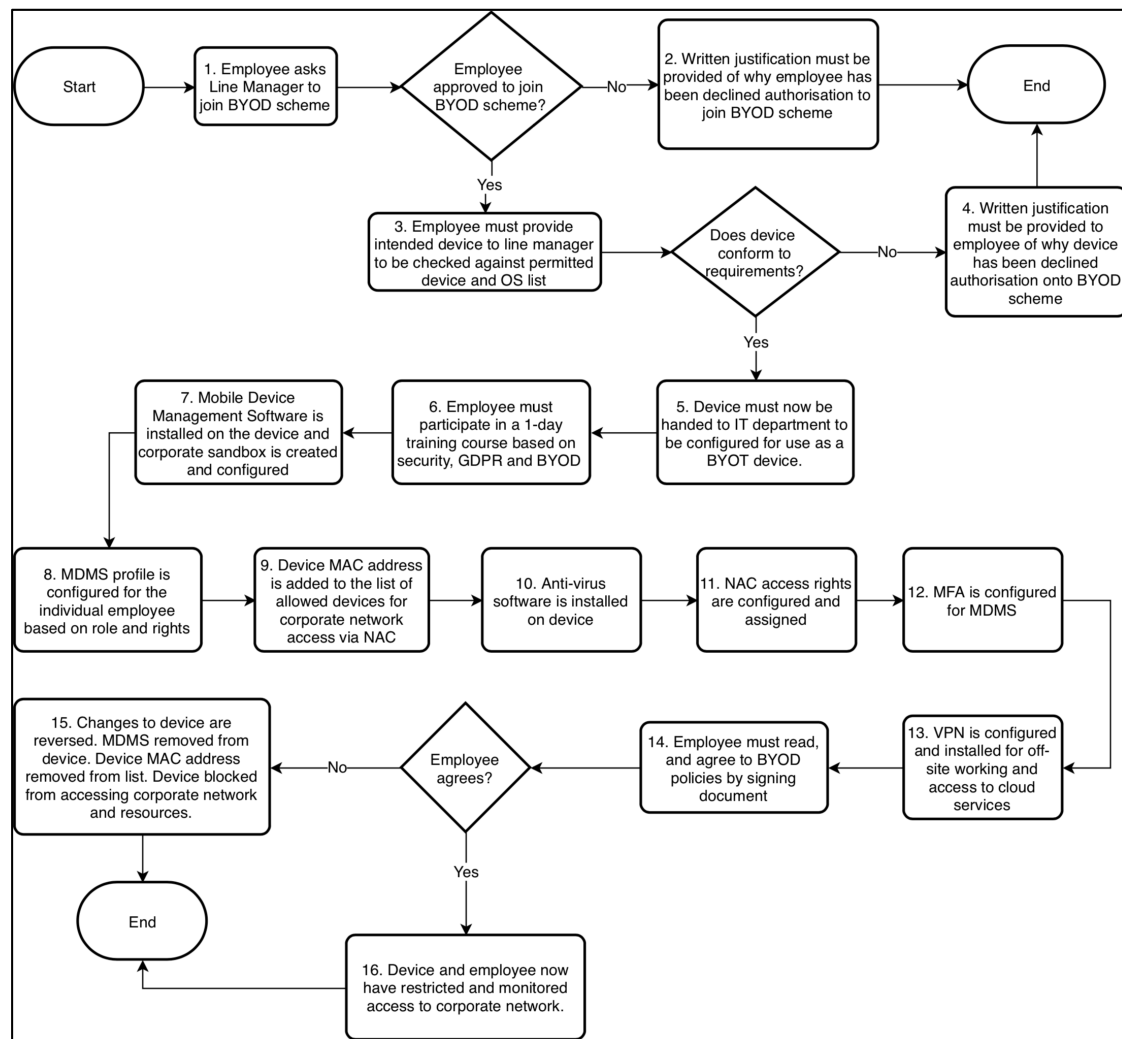


Figure 2. Flowchart demonstrating how an employee joins the BYOD scheme

Employees must be made aware of basic security principles in order to protect corporate data and intellectual property, hence the need for Appendix A.6. According to Cyan Solutions, the biggest risk of data breaches is from neglect and human error by employees [9], such as opening an email attachment containing malware. Inadequate staff training around security and legislation, such as the 2018 GDPR may leave an organisation open to attack and data breach, resulting in ceased operation or data loss and fines of up to €20 million, or 4% annual global turnover [10].

The policy in Appendix A.7 states that employees must agree to the BYOD policies. This is required to make them aware of what they can and cannot do, their responsibility if an incident is to occur, and how to proceed. The policies should be covered in the staff training so that they can be better explained. Employees may opt out of the BYOD scheme or decline policies as

per Appendix A.8, and in this circumstance all corporate data and applications will be removed from the device along with being removed from the network.

Appendix A.9 states that when attempting to connect to the corporate network, the device will be tested by Network Access Control, where the MAC address of the device will be compared against the database, and the presence of anti-virus and MDM software, along with the device OS version, and the use of a VPN (if offsite) will be checked. A Media Access Control (MAC) address is used to identify a device, and is a unique address for a Network Interface Card that is assigned during manufacturing [11]. Restricting access to the network through the use of NACs ensures that only registered devices that meet the criteria can connect. Appendix D provides more information on NAC. NAC will check the OS version to ensure it is permitted and is up-to-date, along with the presence of anti-virus and MDM software on the device, mitigating against the risks outlined above in Section 4.1.

The data flow diagram below in figure three outlines the process of connecting to the corporate network and accessing resources.

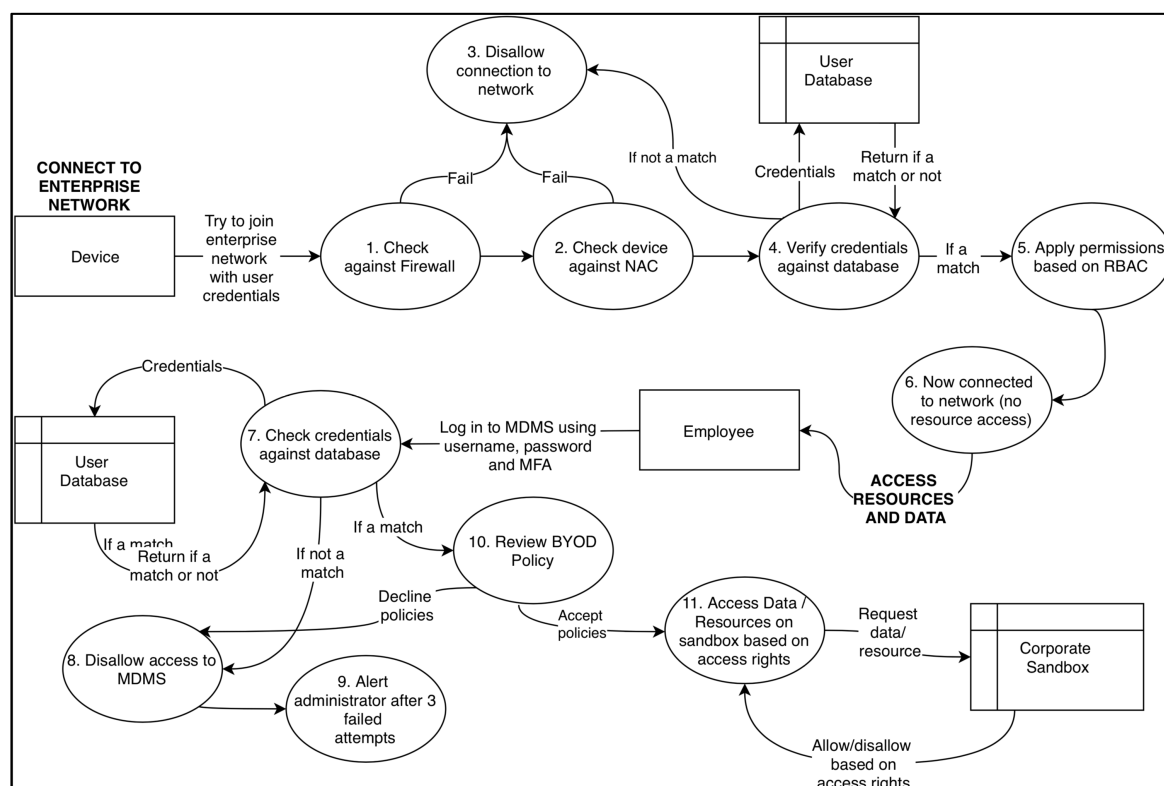


Figure 3. DFD outlining connection to network and access to data.

3.3.Segregation of Personal and Corporate data

Corporate and personal data must remain separated for many reasons, such as to ensure that only authorised individuals can access data and applications to maintain confidentiality. Authorisation is an important factor of data security to conform to Government legislation. The blending of personal and corporate data can become an issue where the corporate data is left unsecured (unencrypted), meaning it can be read by anyone with access to the device, and may be accidentally or deliberately shared to unauthorised and unsecured individuals or devices. Appendix A.10 states that MDM software will be used to isolate corporate data and applications on the device using a sandbox, ensuring that the organisation can remain in control of their data and resources, and who has access to them.

Appendix A.11, along with Section 4.7 outlines the organisation's right to maintain in control of their data if a device is to be lost, stolen, damaged or compromised, or if an employee is to leave.

3.4. Physical Security

Access to the Hyper-fort main building, along with internal rooms is restricted as stated in Appendix A.12. Server room access is further restricted to authorised personnel only, as stated in Appendix A.13. RFID cards provide access information and only employees with permitted access may gain entry to rooms. The use of a four-digit numeric code aims to mitigate against access by unauthorised individuals who may acquire possession of an employee's RFID card. Server rooms must be protected from manipulation to ensure only those with necessary rights can make changes to the network, in order to maintain network security and availability, and to reduce the likelihood of network downtime.

Security cameras and entry and exit logging will be used as stated in Appendix A.14, which allows for the traceability of an individual's actions if a security breach is to occur, along with legal and moral culpability.

3.5. Protection of Data at Rest, in Use and in Transit

3.5.1. Data at Rest

To ensure that corporate data remains contained and secured, the corporate sandbox is to be encrypted, as per Appendix A.15. In the event of device loss, theft or infection from malware, the contents of the sandbox cannot be read due to the AES 256-bit encryption, which is currently the highest security symmetric encryption [12].

3.5.2. Data in Use

In order to authenticate users accessing the sandbox, access is restricted using credentials and two-factor authentication, along with the device's location as stated in Appendix A.16. Secure passwords are to be used, along with the logging of login attempts and blocked access after three failed attempts, as stated in Appendix A.17 and A.18 respectively. Secure passwords are less risk for brute force attacks, and also makes shoulder snooping more difficult than with a shorter, simpler password. Logging failed login attempts can help to identify a system attack and alert an administrator before an attack causes harm to the system.

The framework implements strict access rights using Role Based Access Control (RBAC) and NAC as outlined in Appendix A.19. NAC is used to check for the presence of certain applications and device status, as outlined in section 4.2. Allowing only the lowest amount of access to data prevents the disclosure of information to unauthorized individuals, maintaining data privacy, and lowering access rights further outside of normal working hours aims to protect against suspicious activity on the network.

DDoS protection software is to be used in order to defend against Distributed Denial of Service attacks. Appendix C explains DDoS attacks and the risks they pose to a network. DDoS software identifies potential DDoS threats and blocks them before they are able to cause harm to a network, and therefore reduces or eliminates the network downtime they may produce.

Appendix A.20 states that network devices must have all unused ports disabled. This mitigates against the risk of an unauthorised individual connecting their device to the network, as they would be unable to do so without making changes to the network's physical configuration.

Network defences including IPS, NAC and firewall will be used, as stated in Appendix A.21. Appendix B, D and E provide information on IPS, NAC and Firewalls respectively. The use of these defences protects against and detects attacks from DoS and DDoS attacks, along with malware infiltration such as viruses, before they are able to harm the network.

Malware can be introduced through the use external media, hence the need to protect against it as in Appendix A.22. Data cannot be contained and safeguarded by the organization if it is allowed to be transferred without adequate protection. Along with this, corporate data held on an unsecured device poses other risks, such as a data breach, where unauthorised individuals are accessing sensitive or personal data. As mentioned earlier in this report, organizations can face hefty fines if such a breach should occur. A.23 also aims to mitigate against these risks.

As part of the user policy, employees should not be allowed to access certain websites during work hours, as outlined in Appendix A.24. This aims to defend against risks to the network posed by some websites, such as inadvertently downloading malware, but also aims to encourage staff to conduct themselves in a more professional manner.

Appendix A.25 mitigates against the risk of man-in-the-middle attacks where data is sent over an unsecured network, by using a corporate VPN, discussed below in Section 4.5.3.

Applications produced by questionable developers may include malware which could harm device data and endanger network security, hence Appendix A.26. Applications must be from certified developers and tested for malware before being added to a whitelist.

3.5.3. Data in Transit

Appendix A.27 states that network access will be denied without the use of the VPN, IPSec and L2TP. These protocols are described in Appendix F. This has been implemented to defend against man-in-the-middle attacks when using public internet connections, such as those in coffee shops. Appendix A.28 also mitigates this and ensures that data cannot be read if intercepted due to encryption.

3.6. Device and User Monitoring

Employees must be aware of acceptable use of personal devices during working hours, as per Appendix A.29. Alongside this, Appendix A.30 states that employees must consent to device monitoring. Devices will be monitored for prohibited applications that pose security risks to the device and corporate network, and to ensure they are not jailbroken or rooted. Devices can be tracked to identify suspicious activity such as a lost or stolen device, in order to be recovered. Administrators can be alerted if a device leaves a predefined geo-fence and if not accounted for, can be blocked from accessing the corporate network to maintain security.

3.7. Incident Response

Appendix A.31 outlines incidents that must be reported. In the case of an incident the device may be remotely locked, or the corporate sandbox remotely wiped. The device's location will be tracked in order to be recovered and will be blocked from the network by its MAC address. If a device is to be sold, the corporate sandbox must be wiped, and the device removed from the network. The above scenarios mitigate against the access of corporate data by unauthorised individuals and maintains the privacy of data.

The data flow diagrams below in figures four and five visualise the incident response process.

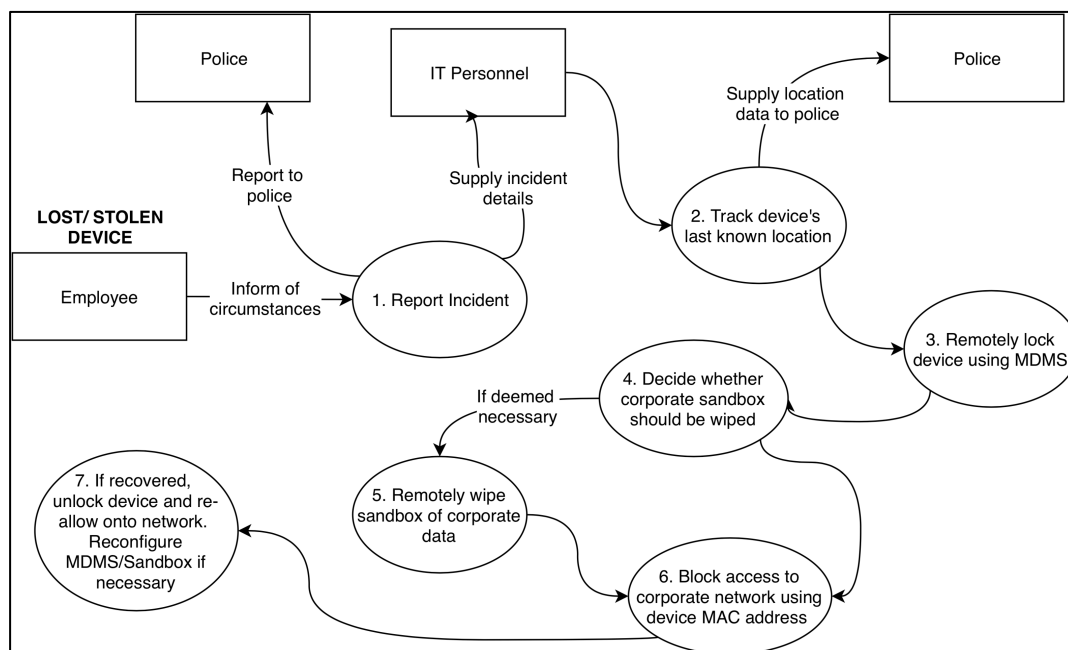


Figure 4. DFD outlining incident response to a lost/ stolen device.

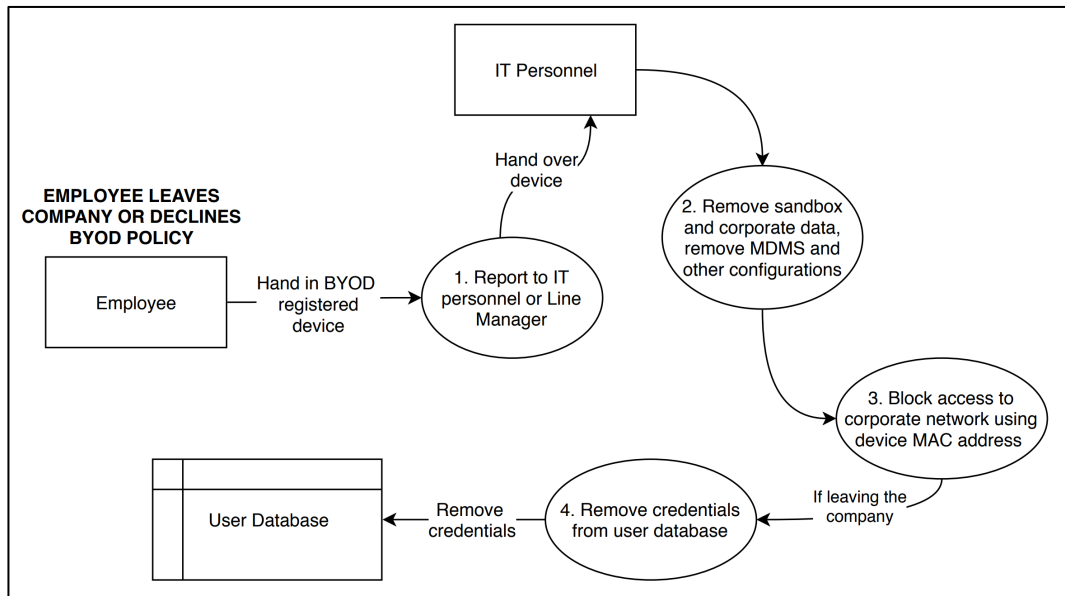


Figure 5. DFD outlining incident response to an employee leaving the company, or declining BYOD policy.

3.8. Redundancy and Resilience

Network redundancy is the processes of deploying network operations to redundant infrastructure in the case of a device failure or outage, and is used to mitigate against a single point of failure and network or system outages [13]. Network resilience is “the ability of a network to defend against and maintain an acceptable level of service in the presence of such challenges” [14]. Figure 3 below shows an example design of network redundancy.

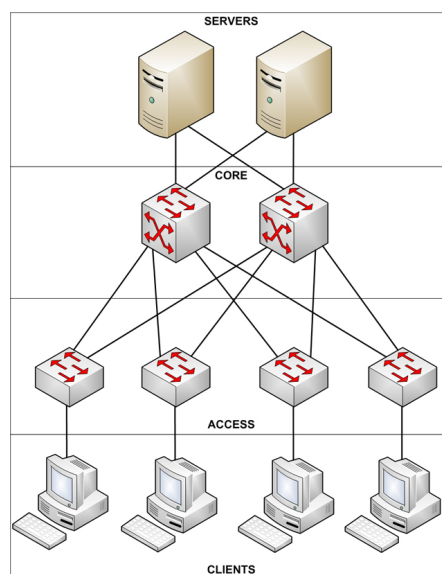


Figure 6. Design for Network Redundancy. Image source: [15].

The Spanning Tree Protocol (STP) is used for redundancy. The primary function of the STP is to eliminate loops caused by redundant links in a network, which are deadly as they consume all of the network bandwidth [16].

It is assumed that Hyper-fort has an off-site backup along with a hot-site, containing core services and hardware, which are available to be used in case of a disaster to ensure rapid recovery of services and to minimize down-time and potential business loss.

The network implemented on Cisco Packet Tracer has been created to ensure network resilience and redundancy. It has no single points of failure and has redundant hardware in case of failure, as recommended. The implementation can be seen in section 3.10.

3.9. Guest Network

As required, Hyper-fort will allow access to a limited, separate guest network, as stated in Appendix A.32. This network will make use of AAA, through the use of a database containing credentials and minimal user access levels. Customers will be allowed to set their own password, provided it meets the requirements, as they are less likely to write it down and leave it unsecured. The network has been separated to mitigate against risks discussed in this report, such as the introduction of malware and unauthorised access to confidential information held on the corporate network.

Device authorization is not required for the guest network, as customers will only be able to access the separate network containing limited and non-sensitive data.

3.10. Cisco Packet Tracer Implementation

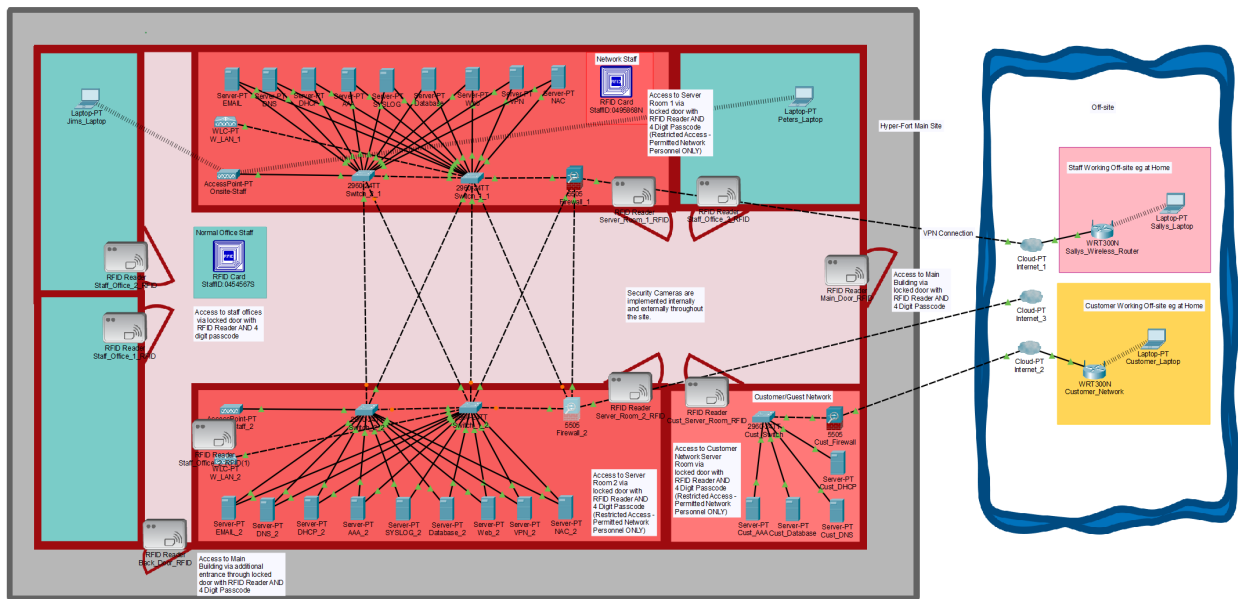


Figure 7. Logical Cisco Packet Tracer View

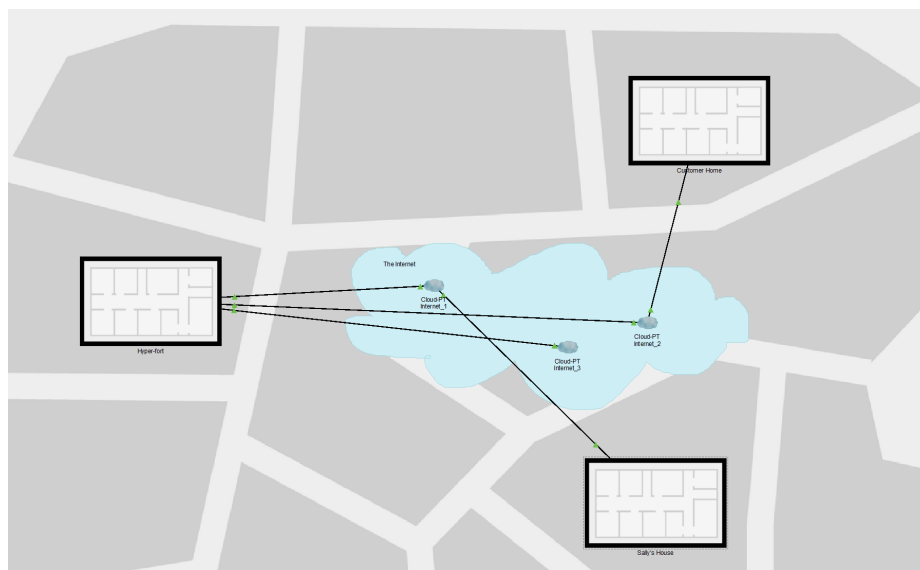


Figure 8. Physical Cisco Packet Tracer View

Figure seven and eight above show logical and physical network design. Assumptions for the implementation are listed below.

It is assumed that the following have been configured for both the corporate and customer network:

- a. User Access Rights
- b. NAC

- c. IP addresses
- d. Email
- e. Web
- f. DHCP and DNS
- g. AAA
- h. VPN
- i. Firewalls
- j. SYSLog
- k. Spanning Tree Protocol

3.11. Mobile Device Management Software Selection

Appendix G outlines the primary functions of a MDMS. Based on research of current MDMS, the author has chosen VMWare Workspace One for the following reasons. Firstly, it aids in the productivity of new users by providing embedded training videos, links and a wizard-like approach [17]. Within a single platform, organisations are able to manage both BYO and corporate-owned devices [18], simplifying the process for IT staff. It allows for full device management and the containerisation of enterprise applications and enables MFA, conditional access based on device location, and the revocation of user access, all of which is a requirement of the proposed framework. Also, it allows for new devices to be added easily, policies to be created and deployed, and connections to both enterprise email and VPN [19].

4. Discussion

4.1. Advantages and Challenges of BYOT

BYOD can bring many positives for a business, including enhanced efficiency, productivity and morale, which is why approximately 70% of businesses already utilise BYOD, according to recent reports [20]. In 2015, on average 81% of adults own or have a laptop in their household [21], therefore organisations are able to reduce hardware costs by insisting employees use their own [2].

Many employees agree that they prefer using their own device in the workplace, as they are already familiar with it, and as a result less IT training is required by a company [2]. It has

also been reported that employees may accept lower paid jobs if the organization allows the flexibility of BYOD [22].

However, if not managed correctly and without suitable staff training, BYOT can result in hefty fines and prosecution. The blending of personal and corporate data can result in sensitive data being left unsecured and at risk of breaching GDPR legislation. Personal devices may not have adequate anti-virus protection, leaving devices open to malware attacks and posing risks to corporate data. Another disadvantage to organisations who do not currently, but wish to allow BYOD, is that updated infrastructure, policies and procedures must be provisioned, which is both a costly and timely task.

The framework outlined in this report aims to minimise the challenges of BYOD and instead to focus on the positives.

5. Conclusion

The policies discussed in this report aim mitigate against external and internal threats to corporate data through the use of hardware and software-based technologies, including firewalls and MDMS to ensure integrity, availability and confidentiality of data, which as highlighted in section 2.1, is the key to data security. It also outlines acceptable use and user policies, because as stated in this report, employees are often the largest risk to data security.

Future improvements to the framework would be to include a more comprehensive customer network, to allow them to access more resources, such cloud services, and to include more software-based networking technologies. Cloud services should also form a larger part of the network in order to stay up to date with current trends.

Further improvements include improving the network implementation on Packet Tracer, as, due to lack of knowledge of the software and time constraints, the author was only able to create a simple network which was not fully configured, it did however include basic security such as disabling ports, adding passwords to the CLI, and disabling Telnet.

It is felt that a balanced framework has been implemented with suitable measures to safeguard data and to protect the corporate network, it's data and resources.

6. Appendices

Appendix A

Hyper-fort Policies, Guidelines and Procedures

- A.1. Employees must request authorisation from their line manager in order to join the BYOD scheme. Employee acceptance is approved on a case-by-case basis as deemed appropriate by the relevant managers. Only after approval will the device authorisation process begin.
- A.2. Devices must be inspected by the relevant line manager, who have participated in suitable training and are therefore deemed competent. Devices are inspected individually and will be audited by random spot checks.
- A.3. Permitted devices are those that conform to the following standards:

1. Devices must be of the following type, operating system and OS version:

Type of Device	Operating System	Version
Laptop	Microsoft Windows	8.1 or later
Laptop	Apple MacOS	10.10 or later
Smart phone / Tablet	Android	7.0 or later
Smart phone / Tablet	Apple iOS	9.0 or later

2. Devices must NOT be jailbroken or rooted.
3. Devices must be of the most up-to-date Operating System version and must have all necessary firmware, application, software and security patch updated also.
4. Devices must be used in conjunction with genuine or original chargers, provided or sold by the corresponding manufacturer.
5. Manufacturer and brand of device has not been specifically stated, and so any device that meets the above requirements will be permitted.
6. The device must have a passcode or password set of a suitable standard. Biometrics in addition to device passwords are permitted.

7. The personal device must not contain any illegitimate data or be used in relation with any unlawful activity.

- A.4. Devices will not be granted access to corporate network or resources until they have been authorised. An up-to-date list of registered BYOD users and devices will be maintained.
- A.5. Users must agree to the installation of corporate supplied Mobile Device Management software and anti-virus software.
- A.6. Employees must participate on a one-day basic training course which will cover data security, user responsibilities, procedures, legislation and incident protocols relating to this framework before being permitted to join the BYOD scheme.
- A.7. Employees must agree to the outlined BYOD policies and must sign a written agreement before being permitted to use a personal device on the corporate network.
- A.8. An Employee is able to opt-out of a BYOD scheme, or decline the BYOD policies at any time, in which case they will be removed from the corporate network, have their corporate data wiped from their device and will be required to use on-site corporate PCs.
- A.9. Devices connecting to the personal network will be tested against Network Access Control. NAC will check the MAC address of the device attempting to join the network, which must exist in the system. NAC will also check for the status of OS version and for the presence of anti-virus software and MDM software, and if not satisfactory, connection will fail. If working offsite, the corporate VPN must be used to gain access to the network and resources.
- A.10. Mobile Device Management Software, referred to as MDM software or MDMS, will be used on BYOT devices in order to isolate corporate data and applications from personal data and applications.

- A.11. In the case that a device is lost or stolen, the organisation has the right to remotely wipe the corporate data and applications held on the MDM software. Device tracking using GPS location may be used along with remotely locking the entire device until recovered.
- A.12. Access to the Hyper-Fort building, internal rooms and offices is controlled. Only authorised personnel may gain entry, through the use of a corporate supplied RFID card and four-digit numerical code. An RFID card must be scanned in order to exit the building and internal rooms. The four-digit numerical code will vary for each employee and will be updated every six weeks. A different four-digit code will be required for the internal rooms and external doors.
- A.13. Access to internal server rooms containing network infrastructure is strictly forbidden for unauthorised personnel. An RFID card and four-digit numerical code is required to gain entry, which will only be granted if the individual has the necessary access rights. An RFID card must be scanned in order to exit the rooms. The four-digit numerical code will be individual to each employee, will differ from the one required for external building entry, and will be updated every two weeks.
- A.14. Security cameras are used internally and externally throughout the Hyper-Fort premises in order to monitor Employee access and behaviour. Entry and exit logging information will be kept for each Employee's access to the building and its containing rooms.
- A.15. The corporate sandbox and e-mails will be fully encrypted using AES 256-bit encryption.
- A.16. Access to the corporate sandbox requires both a username and password, along with the use of two-factor authentication using a one-time short-lived code, sent to a separate device. Device location will be considered when trying to gain access to the sandbox, and if the location is outside of the pre-defined geo-fence, access will be denied.

- A.17. Passwords used as a form of authentication must be of a minimum of eight characters consisting of uppercase, lowercase, numeric and special characters.
- A.18. Login attempts will be logged for each account. After three failed login attempts, the user account will be blocked for twenty-four hours, or until assistance is requested from the relevant IT personnel.
- A.19. Employees will be assigned individual access rights based on their job role and normal day-to-day operations. The assigned access rights will be of the lowest level deemed necessary, and if additional rights are required these must be requested in writing along with justification to the relevant line manager. Access rights will be further reduced outside of normal working hours, between the hours of six-PM and seven-AM.
- A.20. Network devices stored in secured server rooms must have all unused ports disabled by network personnel.
- A.21. Network security defences including but not limited to: Intrusion Prevention Systems, Firewalls and Network Access Control will be employed on the Network.
- A.22. The transfer of corporate data stored on personal devices to external storage media shall not be permitted in any circumstance.
- A.23. The transfer of corporate data between personal and corporate emails shall not be permitted in any circumstance.
- A.24. Employee access to websites and applications of the following nature through the corporate network or during working hours is not permitted:
1. Social Media, including but not limited to: Twitter, Facebook, Instagram;
 2. Dating, including but not limited to: Tinder, Plenty of Fish, e-Harmony;
 3. Gambling, including but not limited to: Bet Way, Jackpot Joy, Paddy Power;
 4. Online Shopping, including but not limited to: Amazon, E-bay, Depop;
 5. Pornographic;

6. Illegitimate;

- A.25. Personal devices should have Bluetooth, WIFI and wireless mobile networks turned off as default when not in use. Devices should be set to prompt users before connecting to Networks. Connecting to public networks is not recommended, however if absolutely necessary, connection should be through the corporate VPN.
- A.26. The Mobile Device Management software will not allow any external applications to be installed unless they have been pre-approved or are part of the application whitelist. If a further application is required, it must be requested in writing along with justification to the relevant line manager and access will be approved on a case-by-case basis.
- A.27. Access to the corporate network when offsite will be denied without the use of the corporate VPN using both IPSec and L2TP.
- A.28. Access to corporate e-mails must be through the encrypted application held in the corporate sandbox and over the corporate network, or VPN if offsite.
- A.29. Users must use personal devices only for activities directly relating to the organisation during business hours. Very limited personal use is permitted, such as keeping in contact with family. During breaks, limited personal use is permitted on authorised websites and applications only.
- A.30. Employees must consent to device monitoring. Monitoring may include checking device version, applications, browsing history and retained data in the context of a litigation involving an organisation. Device location may be monitored during working hours or if the device is to leave the pre-defined geo-fence without prior notification. Monitoring is solely for the purpose of tracking suspicious and illegitimate activity.
- A.31. A reportable incident may include but not limited to:
 - Physical device loss, theft or damage;

Data breach;
Accidental loss or damage to data;
Suspected malware on device;

Incidents must be reported immediately to the relevant line manager or IT personnel. If stolen, a police report will be required. The device will be locked immediately following an incident being reported and the corporate data on the device may be remotely wiped. In any circumstance, the device's location will be tracked, and the device will be temporarily blocked from access the corporate network and resources.

- A.32. Customers will be allowed access to the segregated guest network, containing limited data and resources. This network may be accessed via the use of username and password credentials supplied by Hyper-fort, which will be checked against a user database.

Appendix B

Intrusion Prevention System (IPS)

Intrusion Prevention Systems (IPS) are used to investigate network traffic to detect and protect against the manipulation of network vulnerabilities. In order to eliminate threats and ensure legitimate packets are not misidentified as threats, along with maintaining network security, the IPS must decipher between them accurately, and must perform actions on incoming traffic flows, such as alarming the administrator, dropping malicious data packets, blocking incoming traffic and resetting a connection. IPS can implemented as part of unified endpoint management (UEM), or high tech firewalls [23].

Appendix C

Distributed Denial of Service (DDoS) and Denial of Service (DoS)

A DoS attack typically uses one machine, whereas DDoS attacks uses a number of coordinated computers, both with the aim of crashing a website or network by sending huge volumes of packets to flood the network. (D)DoS attacks consume resources and bandwidth, so that victims are unable to provide services to legitimate users. (D)DoS attacks are also used to identify security holes or flaws. These attacks often cause financial loss due to the ceasing of

business operations. Large organizations including eBay, Amazon and CNN have fallen victim to DDoS attacks [12].

Appendix D

Network Access Control (NAC)

Network Access Control, also referred to as Network Admission Control (NAC) is used to consolidate endpoint security, such as anti-virus and firewalls, along with user authentication and network security enforcement. NAC consists of a set of rules and protocols which describe what is required of a device in order for it to be permitted access to a network. NAC can be used to check for the presence of anti-virus, or for the current OS version. It is used to mitigate against risks such as zero-day-attacks, which are vulnerabilities in software, along with the introduction of malware and unauthorised users and devices [24]. NAC gives network administrators greater control of the network and those who access it, improving overall network security.

Appendix E

Firewall

Firewalls are used to allow or disallow traffic flow through a network, such as from the internet. They can be used to restrict access to certain websites, and individual IP addresses. There are different types of firewall, such as packet filtering, which operate at layer 3 of the OSI model and are used to block packets based on their address and port number and can be used to protect against DoS and DDoS attacks. Application proxy firewalls can also be used, which analyse entire network packets and block traffic at the application layer. These are often considered the most secure firewall but create single points of failure on a network [24].

Appendix F

IPSec and L2TP Protocols

IPSec, or Internet Protocol Security is a suite of protocols that defines and uses cryptographic algorithms to encrypt, decrypt and authenticate packets over IP (Internet Protocol) networks. IPSec authenticates a session, and then encrypts each packet sent during that session. It also defines the necessary protocols for key management and exchange.

Layer two tunneling protocol (L2TP) is used to create a ‘tunnel’ between two connection points and is used with IPSec [25]. The combination uses a 256-bit key, that is considered “complex enough for top-secret communications” [26].

Appendix G

Mobile Device Management Software (MDMS)

Mobile Device Management Software (MDMS) allows IT administrators to control, secure and enforce policies on smartphones, tablets and other devices across multiple device operating systems and versions [27]. Key features of MDMS include [17]:

- The ability to track software in order to record licences and prevent unauthorised access to applications
- Added security for access to corporate applications and resources, such as email and data
- Creating a secured, encrypted container with authentication for corporate data and applications (sandbox)
- The ability to remotely lock a device in case of loss or theft
- The ability to remotely wipe sandboxed data in case of loss, left or damage
- End-to-end encryption to eliminate the risks of man-in-the middle attacks
- Jailbreak or root detection, to prevent malware and possible override of MDMS security
- The ability to enforce user policies by disabling certain applications
- Device tracking, to remotely track the device’s last known location which can be used to recover a device if lost or stolen, or to monitor for suspicious activity

7. Bibliography

- [1] K. Johnson, T. Delagrange Advisor, and B. Filkins, “SANS Survey on Mobility/BYOD Security Policies and Practices A SANS Whitepaper Sponsored by RSA,” 2012.
- [2] B. Alotaibi and H. Almagwashi, “A Review of BYOD Security Challenges, Solutions and Policy Best Practices,” in *2018 1st International Conference on Computer*

- Applications & Information Security (ICCAIS)*, 2018, pp. 1–6.
- [3] “The Importance of Database Security and Integrity.” [Online]. Available: <https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity/>. [Accessed: 15-Dec-2018].
 - [4] T. Andre, “Cybersecurity an Enterprise Risk Issue,” 2017.
 - [5] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges R,” *Comput. Electr. Eng.*, vol. 67, pp. 469–482, 2018.
 - [6] “Digital signatures and certificates.” [Online]. Available: <https://support.office.com/en-us/article/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96>. [Accessed: 30-Dec-2018].
 - [7] “Uptime calculator.” [Online]. Available: <https://uptime.is/99.999>. [Accessed: 30-Dec-2018].
 - [8] M. Rouse, “What is authentication, authorization, and accounting (AAA).” [Online]. Available: <https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting>. [Accessed: 28-Dec-2018].
 - [9] CYAN SOLUTIONS, “The biggest risk for data breaches is your employees - Cyan Solutions.” [Online]. Available: <https://cyansolutions.co.uk/the-biggest-risk-for-data-breaches-is-your-employees/>. [Accessed: 13-Dec-2018].
 - [10] IT Governance, “GDPR Penalties and Fines | IT Governance UK.” [Online]. Available: <https://www.itgovernance.co.uk/dpa-and-gdpr-penalties>. [Accessed: 13-Dec-2018].
 - [11] “What is a MAC Address?” [Online]. Available: <https://whatismyipaddress.com/mac-address>. [Accessed: 13-Dec-2018].
 - [12] A. K. Azad and M. Y. Mollah, *Advances in Science, Technology and Engineering Systems Journal (ASTESJ)*, vol. 3, no. 3. [publisher not identified], 2018.
 - [13] “What is Network Redundancy? - Definition from Techopedia.” [Online]. Available: <https://www.techopedia.com/definition/29305/network-redundancy>. [Accessed: 30-Dec-2018].
 - [14] P. Smith *et al.*, “Network resilience: a systematic approach,” *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 88–97, Jul. 2011.
 - [15] Brian Hill, “Designing a highly reliable small & medium business network | Ars Technica.” [Online]. Available: <https://arstechnica.com/information-technology/2010/02/designing-a-highly-reliable-small-medium-business-network/>. [Accessed: 29-Dec-2018].

- [16] “Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches - Cisco.” [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html>. [Accessed: 30-Dec-2018].
- [17] D. Tse, L. Wang, and Y. Li, “Mobility Management for Enterprises in BYOD Deployment,” in *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 638–645.
- [18] C. Preimesberger, “VMware AirWatch Launches Unified Endpoint Management,” p. 1, Oct-2016.
- [19] “Mobile Device Management | MDM | VMware AirWatch.” [Online]. Available: <https://www.air-watch.com/capabilities/mobile-device-management>. [Accessed: 30-Dec-2018].
- [20] K. Downer and M. Bhattacharya, “BYOD Security: A New Business Challenge,” in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015, pp. 1128–1133.
- [21] “• Laptop ownership in UK households 2015 | Survey.” [Online]. Available: <https://www.statista.com/statistics/488892/laptop-ownership-in-households-by-age-united-kingdom-uk/>. [Accessed: 29-Dec-2018].
- [22] A. Bello Garba, J. Armarego, D. Murray, and W. Kenworthy, “Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments,” *J. Inf. Priv. Secur.*, vol. 11, pp. 38–54, 2015.
- [23] “What is an Intrusion Prevention System? - Palo Alto Networks.” [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>. [Accessed: 13-Dec-2018].
- [24] J. M. Stewart, *Network security, firewalls, and VPNs, second edition*. Jones & Bartlett Learning, 2014.
- [25] M. Boulter, “Remote Network Access: Which VPN Protocol Should I Use?,” Philadelphia, 2015.
- [26] J. DeMuro, “VPN protocols,” 2017. [Online]. Available: <https://www.techradar.com/uk/news/whats-the-best-vpn-protocol-to-use>. [Accessed: 02-Jan-2019].
- [27] “What is mobile device management (MDM)? - Definition from WhatIs.com.” [Online]. Available: <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>. [Accessed: 28-Dec-2018].