

Synthesize a solution to a potential real life scenario

Author: Patrick Frank Atkinson (1811357)

ACCA4018 – Academic & Employability Skills

Faculty of Architecture, Computing and Engineering

Date of submission: 10th January 2019 at 15:00

Abstract

This report outlines a proposed implementation of a network infrastructure suitable for a Bring Your Own Device (BYOD) policy. It considers Unified Endpoint Management (UEM) solutions, wireless network authentication protocols and Bring Your Own Device (BYOD) policies, and suggests strategies based on this research. It also proposes a network layout and how to secure it from a physical and configuration standpoint.

Contents

1. Introduction.....	1
2. Related work	1
2.1. Bring Your Own Device (BYOD)	1
2.2. Unified Endpoint Management (UEM).....	2
2.2.1. Background of UEM.....	2
2.2.2. UEM functionality	3
2.2.2.1. OS support	3
2.2.2.2. Policy and app deployment.....	3
2.2.2.3. Containment features (walled garden).....	4
2.2.2.4. Device/user monitoring	4
2.2.2.5. Revocation	4
2.3. Wireless network authentication	4
3. Problem formulation	6
3.1. Network infrastructure	6
3.2. UEM.....	6
3.3. Policy.....	7
4. Implementation	7
4.1. Physical security.....	7
4.2. Configuration security.....	7
4.3. Redundancy.....	8
4.4. Segregation and security	8
4.5. Monitoring.....	10
5. Discussions and findings.....	11
5.1. UEM discussion	11
5.1.1. Comparison of UEM solutions	11
5.1.2. UEM selection	12

5.2.	BYOD discussion.....	12
5.2.1.	Potential benefits.....	12
5.2.2.	Areas of caution	13
6.	Conclusion and future work.....	14
6.1.	Conclusion.....	14
6.2.	Future work	14
7.	Glossary	15
8.	Bibliography	16
9.	Further reading.....	19
10.	Appendices.....	20
10.1.	Appendix A – example app services	20
10.2.	Appendix B – sample Wireless Access Policy	23
10.3.	Appendix C – Packet Tracer screenshot.....	25
10.4.	Appendix D – flowchart of staff user connecting to network	26

1. Introduction

Hyper-fort is a company that offer consultancy in the energy sector, with a large worldwide presence. It has a large user base made up of both staff and customers. The overwhelming feedback from the users is that they want to be able to use their personal devices to access Hyper-fort's network and resources. Protection of data and information is of utmost importance to Hyper-fort, particularly the personal data of staff and clients, and the company's own intellectual property which is worth billions. A large percentage (estimated at almost 95%) of the company's network is wireless-based, and the IT services provided to the users are cloud-based. A glossary of acronyms is included at the end of this report should the reader require it.

2. Related work

To account for users wanting to use their personal devices to access Hyper-fort's network and resources, a Bring Your Own Device (BYOD) policy could be adopted. This section will give an overview of BYOD policies, Unified Endpoint Management (UEM) and wireless network authentication. UEM is required as part of comprehensive BYOD policies to ensure the security of company data through management and monitoring of the devices being used to access company data. Wireless network authentication is another area that is discussed due to Hyper-fort's reliance on wireless devices.

2.1. Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) policies are a growing trend in a number of sectors. These policies encourage or require employees to use their personal devices to access corporate resources. This typically applies to mobile devices, such as smartphones, tablets and laptops, but can include desktops and other equipment as well. The implementation of the policy may differ depending on the organisation's needs. In the report *Understanding the Bring-Your-Own-Device landscape* [1], it's suggested that there are three 'flavours' of implementation; using personal devices as a replacement for enterprise devices, using personal devices to complement enterprise devices, and using personal devices where the user would not ordinarily be given an enterprise device. In the same report, it is suggested that the first of these options is the most controversial as significantly changes the contract between the employer and employee.

There are numerous advantages to an organisation implementing a BYOD strategy, but there are factors that need to be considered to ensure data security. In section 5.2 of this report, the potential benefits and areas of caution are discussed.

2.2. Unified Endpoint Management (UEM)

2.2.1. Background of UEM

Cloud services and platforms have become ubiquitous in workflows in recent years. In McKendrick's article *The Other MDM: Why 'My Device Matters'* [2], Tad Johnson suggests that this, alongside 'highly functional mobile apps', has made the possibility of running an organisation's operations via mobile devices realistic. Whilst the flexibility inherent with mobile devices provides the opportunity for enhanced workflows, the security implications need to be considered. In the same article, Jeff Holleran recommends that organisations adopt a UEM solution to maintain data security 'across different operating systems, form factors, ownership models, and security postures'. The term UEM is used to describe an approach of managing 'endpoints' (e.g. desktops, laptops, smartphones, tablets and Internet of Things (IoT) devices) from a single application or application suite [2]. UEM is an evolution of Enterprise Mobility Management (EMM), which is itself was developed from Mobile Device Management (MDM). MDM was considered to be suited to environments where every device was owned and managed by the organisation. This approach was thought to be 'heavy-handed' and inflexible due to its rigid security controls. The industry adoption of BYOD led to MDM evolving into EMM, which accounted for devices owned by employees by managing them in a less strict way. The change in workflows mentioned earlier caused a shift in focus from device visibility and control to increasing employee productivity without compromising data security. As such, EMM was developed to include mobile app and content management. UEM is the latest incarnation, intended to manage all endpoints [2]. Whilst modern operating systems such as Windows 10 S and Chrome OS favour UEM-based management, older operating systems may require some form of Client Management Tool (CMT) (e.g. Microsoft's System Center Configuration Manager) to get the most complete management functionality for that operating system. Silva, et al [4] suggest that most organisations have not yet implemented UEM as their primary management method, and therefore vendors have a strong selling point if they provide a 'bridge' between the UEM and CMT. They state that they see 'the majority of organizations facing nontrivial obstacles to fully embrace UEM, but the number of organizations making the switch to UEM management will grow in the coming three years'.

2.2.2. UEM functionality

2.2.2.1. OS support

Due to the evolution of UEM from MDM, all the major UEM solutions have strong support for mobile operating systems, such as Android and iOS. This is not the case for desktop operating systems. Despite three of the major desktop operating systems currently on the market (Windows 10, macOS and Chrome OS) supporting MDM, some UEM solutions offer no, or limited, support for them, particularly in the case of Chrome OS. Some solutions provide support for legacy platforms, such as Windows 7, but these often require the use of a CMT in addition to the UEM. This has cost implications, and the feature-set of CMT may not mirror that of the UEM.

2.2.2.2. Policy and app deployment

When a device is ‘enrolled’ into a UEM solution, a profile will be deployed to the device. This will have numerous policies defined by the organisation. These can include, but are not limited to [5]:

- The ability for the organisation to silently install and remove apps and certificates;
- The ability for the organisation to create, access and delete data in the work profile;
- Forcing the user to have a password on the device;
- Preventing screen capture within the work profile;
- Monitoring of network activity and location.

The profile will also require that a companion app be installed on the device. This app will be used by the UEM solution for device management and monitoring. The level of control over the device afforded to the organisation by the profile is dependent on the device itself as well as the UEM solution. Older versions of operating systems may not allow management of certain features. For example, apps couldn’t be silently installed on iOS devices until iOS 7 was released [6], and numerous changes have been made to Windows 10’s MDM capabilities since its release [7]). Organisations may choose to license software for their employees and deploy it to their devices. The software can then be revoked if necessary and re-issued to another device or user.

2.2.2.3. Containment features (walled garden)

Many UEMs offer containment features that isolate the user's personal data from the business data on the device. Apps can be 'containerised' and password protected to secure sensitive data, with access levels being tied to the identity of the user. Some UEMs can be configured to require that the apps are encrypted, and certain functions (such as copy-paste, save-as and screenshots) can be disabled to prevent data leakage. Apps that access the organisation's network can be configured to require a secure VPN. This can be done on a per-app basis. As highlighted in [4], many of the providers offering the functionality outlined above are using Microsoft's Intune APIs that are available through Microsoft Graph, although some providers (such as VMWare [8]) have their own ecosystems.

2.2.2.4. Device/user monitoring

The companion app mentioned previously will request access to various data and permissions on the device, such as location and connection data (Appendix A shows the permissions requested by one such app). The app will use this access to monitor the device's activity and report back to the UEM solution. The UEM solution will have some form of dashboard for monitoring and reporting.

2.2.2.5. Revocation

Through the dashboard, the organisation will be able to revoke access of company data from devices. This can either be done manually (for example when a staff member leaves employment), or if the device fails to meet the criteria of the organisation's policy. As well as revoking access to company data and services, any software installed on the device through the UEM solution can be removed as required.

2.3. Wireless network authentication

The increase in the availability of wireless infrastructure and the consequent ubiquity of its use has resulted in increased scrutiny of the security standards used for wireless communications. IEEE 802.11, commonly referred to as Wi-Fi, has been a particular target for cyber-criminals due to its heavy adoption. IEEE 802.11 is set of standards for implementing a Wireless Local Area Network (WLAN). The specifications pertain to the media access control (MAC) sub-layer and physical (PHY) layer within the OSI model, where the main differences between wired and wireless networks lie [9]. Since its introduction, the protocols used for devices to connect and authenticate with Wi-Fi networks have evolved to improve security. The initial

protocol was the Wired-Equivalent Privacy (WEP) key. As the name implies, it was intended to offer a level of security equivalent to wired networks through an RC4 encryption algorithm [10]. It is applied to all layers above the data-link layer in the OSI model. Several security vulnerabilities with WEP have been identified and it is consequently considered to be a weak security protocol [10]. For example, with WEP, a common key is shared between the radio stations and is used in the RC4 encryption of the packets. Once this key has been discovered, data security is compromised. In 2007, Tews et al claimed to be able to ‘crack’ a 104 bit WEP key in under 60 seconds [11].

WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, quickly followed by WPA2 in 2004. WPA uses TKIP encryption, whereas WPA2 uses AES encryption, although it can use TKIP to provide backward compatibility [12]. WPA2 will be the focus for the remainder of this section. There are two main variants of WPA2; WPA2-PSK (often referred to as WPA2 Personal) and WPA2-Enterprise. The difference between the variants is in how the authentication works.

WPA2 Personal – uses a pre-shared key. The user selects the network on their client device and enters the pre-shared key. The access point uses the Service Set Identifier (SSID) name and the pre-shared key to generate a pairwise master key (PMK) which is used to encrypt the traffic (typically using AES) between the access point and device. The PMK will always be the same for that client. If it is compromised, all past and future traffic encrypted using it can be decrypted.

WPA2-Enterprise – WPA2-Enterprise does not use a pre-shared key with the client. There are several possible authentication methods; password-based, token-based and certificate-based. Whichever method is used, the credentials will be user-specific. Once the credentials have been passed to the access point, it then passes them to a RADIUS server. The RADIUS server checks the credentials. If they are satisfactory, it passes the access point a randomly generated PMK to be used for the current session only [13]. This means that if the key was to be compromised, only the traffic for that session could be decrypted. Another benefit is that an individual user’s access can be revoked without affecting other users, whereas if the pre-shared key for WPA2 Personal is changed, all users are affected [13].

Due to WPA2-Enterprise’s requirement of a RADIUS server to carry out authentication, it is typically only used in larger organisations, with WPA2 Personal being the usual solution in home settings or smaller organisations. Some companies also provide ‘guest networks’ for the

general public to use. These are often ‘open’ and require no authentication to connect. They do, however, often direct the user to a landing page where the user has to enter various information about themselves before they are given internet access. Due to the lack of authentication, the traffic between the client device and the access point is unencrypted, making it vulnerable to sniffing attacks [14].

3. Problem formulation

3.1. Network infrastructure

When considering the network infrastructure, it is important to first analyse the groups of users. Staff and clients will both be accessing the network. It is assumed that the staff users will need access to the network both internally and externally (e.g. from home). The assumption for clients is that if they are accessing the network they will be doing so internally. In both cases, the data needs to be secure in transit. Staff and client traffic will need to be segregated on the network to safeguard the confidentiality of any information being transferred.

Measures need to be taken to ensure the availability of the network. To this end, redundancy should be employed to provide failovers should there be issues with the infrastructure. Moreover, the network should be physically and cryptographically protected to guard against network intrusions. There should be controls in place stipulating levels of access to information and resources within the network. It is assumed that Hyper-fort already has a Unified Threat Management (UTM) system configured that manages the firewalls and content-filtering. A further assumption is that Hyper-fort uses cloud services in its business and therefore these services do not need to be replicated on-premises. These services include email, document storage, business applications and web hosting.

3.2. UEM

A UEM solution should be identified and implemented. It will need to manage the various operating systems and manufacturer devices that are commonly in use, as well as being able to deploy applications to these devices. It will need to be able to manage different groups of devices and assign the appropriate policies and software. In addition, monitoring and tracking should be available to monitor inappropriate use and track missing devices. It will need to be able to safeguard the company’s data and, where necessary, revoke access to data and software.

3.3. Policy

The Wireless Access Policy should be revised to take into account the revisions made to the implementation of the network to ensure users are aware of the expectations on them if they use the wireless network. A sample policy is shown in Appendix B.

4. Implementation

To illustrate some of the concepts outlined in this section of the document, a proposed network topography has been created using Packet Tracer. A sample of the layout can be found in Appendix C. Reference will be made to the layout throughout this section.

4.1. Physical security

The core infrastructure of the network should be physically secure within the building. The room should be devoid of windows, with access only possible through a secured door. This door should be secured with both a mechanical and an electronic lock. Access to the room should require the use of an RFID card and key assigned to the staff member. Use of the RFID cards should be monitored to identify suspicious behaviour (e.g. the room being accessed out of working hours). This should be combined with CCTV cameras recording people entering the room and cameras within the room itself to log people's movements. The equipment in the room should be in lockable cabinets, and these cabinets should be adequately fixed in place to reduce the likelihood of tampering and relocation. Access to the cabinet keys should be logged for monitoring and auditing purposes. Wireless access points that are deployed in the company's premises should be wall or ceiling mounted and, ideally, high up enough that they can't be reached without a ladder to increase the difficulty of tampering. Other infrastructure supporting the network, such as power sources and environmental control systems, should also be secured to prevent tampering.

4.2. Configuration security

The infrastructure devices on the network should be configured to prevent unauthorised access to their configuration. This should be the case for physical and remote connections to the devices. To this end, unused ports on the devices should be disabled. Access to the Command Line Interface (CLI), either through console ports or remotely via Telnet or SSH, should be password protected. These passwords should be encrypted within the devices' configurations. The same should be true for access to privileged EXEC mode on Cisco devices. Copies of the

device configuration files should be made to ensure devices can be quickly returned to a state that is known to be good (e.g. after a faulty device is replaced).

4.3. Redundancy

The core equipment of the network should be powered off of Uninterruptable Power Supplies (UPSs). These should be adequately specified to give sufficient runtime in the event of a power outage. Eaton [15] recommend this should be calculated after consideration of the business needs, system shutdown time and desired safety margin. Certain types of UPS can also provide a ‘cleaner’ power supply [16]. The UPSs should be supported with a compatible generator that starts up if the main supply has been down for a set period of time [17]. Power redundancy should extend to the security protecting the server room. The RFID reader should have an internal battery to ensure the reader remains active in the event of a power cut. Should the battery fail to work and the reader become inoperable, the mechanical lock remains as a final layer of security.

To reduce the impact of device or connection failures in the network, there should be redundant devices and connections to act as failovers. Examples of this sort of redundancy are shown in the Packet Tracer example. In addition, devices selected for use in the network should have some form of internal redundancy. For example, many enterprise networking devices have a secondary power supply that is always running, ready to take over if the primary power supply fails or loses power. The multiple Network Interface Cards (NICs) used on servers are another example of internal redundancy. In both cases, the redundant component should be connected to a different location to the primary component (e.g. a different power source or switch).

4.4. Segregation and security

Multiple Virtual LANs (VLANs) should be setup to segregate the traffic from each group of users. Table 1 outlines the proposed VLANs for the Hyper-fort network.

VLAN number	VLAN Name
1	Admin
10	Staff
20	Client
30	RemoteStaff

Table 1: Proposed VLANs for the Hyper-fort network

VLANs 1, 10 and 20 are for devices connected to the internal network. VLAN 30 is for remote working staff. Devices on the Client VLAN should be considered ‘untrusted’ and as such their access to resources on the network will be limited. Devices on the Staff VLAN should be considered ‘untrusted’ until the device has been enrolled into the UEM solution and the relevant policies applied. ‘Trusted’ devices should have a different set of firewall rules in the UTM system to the ‘untrusted’ devices. This differentiation should also extend to the content-filtering. The same considerations will be made for staff working remotely. The firewall and content-filtering rules for remote-workers (VLAN 30) should be initially set the same as for internal staff (VLAN 20), but the rules and filters should be kept separate should differentiation be required in the future.

There should be multiple SSIDs on the network, each intended for different users. The SSIDs should be associated with different VLANs. In the Packet Tracer example, there is a basic managed wireless system. This allows each Access Point (AP) to be configured with multiple Service Set Identifiers (SSIDs). Each SSID is VLAN tagged with the VLAN appropriate for the type of user. SSIDs and AP groups can all be configured centrally.

The SSIDs used, and their basic setup, is outlined in Table 2.

SSID name	Broadcasting	Connection security	VLAN
Hyper-fort Staff	Disabled	WPA2-Enterprise	10 (Staff)
Hyper-fort Clients	Enabled	WPA2-PSK	20 (Client)

Table 2: Basic SSID configuration details

The staff SSID is configured with security in mind. Broadcasting is disabled to reduce the visibility of the network. WPA2-Enterprise is used as the authentication method to ensure only users with appropriate authentication can connect to the network. The authentication uses RADIUS and is managed by the AAA server. Using this authentication method provides a link between a device and user which can be used for managing access and for monitoring purposes. An example flowchart of a staff user connecting to the network is shown in Appendix D.

The client SSID is configured with ease of use in mind. Broadcasting is enabled to enable clients to easily identify the network on their devices. The connection security uses WPA2-PSK as this only requires a passphrase to connect but still uses AES encryption as mentioned earlier in this report.

Remote workers will use a Virtual Private Network (VPN) to connect to the Hyper-fort network. This will use tunnel mode in IPsec. Tunnel mode protects each IP packet in its entirety

(both the IP header and payload), as opposed to transport mode which only protects the payload [18]. All data being transferred between the remote worker and the Hyper-fort network will be encrypted and protected against eavesdropping.

4.5. Monitoring

Monitoring will be set up on the network with two objectives; maintaining an audit trail of activity on the network, and for providing alerts of suspicious activity or network issues to the system administrators.

Monitoring should be employed to provide an overview of the health of the network. This can indicate whether a network device, such as a server or switch, is still operable. The logs can be used to identify trends of behaviour on the network (e.g. network usage at different times of day) and troubleshoot issues. It may also be used by devices on the network to manage traffic. For example, if a particular device is using a disproportionately large amount of the available internet bandwidth and affecting connection speed for other devices, Quality of Service (QoS) rules could be actively applied to that device to reduce the amount of bandwidth available and reduce the effect on other devices.

Alerts should be utilised to notify system administrators of events that need attention. They should be categorised based on the severity of the issue and the notification method adjusted accordingly. For example, if a client device uses incorrect credentials to authenticate but subsequently authenticates successfully, an alert wouldn't be required. If the same client were to have repeated failed attempts to authenticate in a short timeframe, the administrator could be notified via email and provided with the logs, allowing them to make an informed decision about how to proceed. For services supporting the network, such as power sources and environmental control systems, administrators should be informed of outages or readings that move outside of pre-defined parameters (e.g. excessive voltage fluctuations or excessive temperatures). Alerts should also be sent if a network device is no longer sending or receiving network traffic, which may indicate the device, or the connections to it, have failed. The UTM should notify administrators if Intrusion Detection System (IDS) detects a threat or if the Intrusion Prevention System (IPS) takes actions to thwart a detected threat. Within the UEM solution, the administrators may decide to enable alerting if an enrolled device no longer meets the requirements of the policy. Device location may also be used to alert if a device moves to an unexpected geographical region, which may indicate the device has been stolen.

5. Discussions and findings

5.1. UEM discussion

5.1.1. Comparison of UEM solutions

This section of the report with makes comparisons between UEM solutions offered by different vendors. Five vendors will be considered, and key points listed. These vendors were considered to be leaders in the Gartner report, *Magic Quadrant for Unified Endpoint Management Tools* [4]. This report was published on July 2018 and provides an independent and relatively up-to-date comparison of the UEM solutions on the market.

Vendor (UEM solution): BlackBerry (BlackBerry UEM)

Key points

- A containerised environment can be provided in place of a VPN [8]
- Support for wearable platforms (watchOS and Android Wear) [9] and the GNX IoT platform
- Supports direct management of Office 365 [9] and the ability to apply Microsoft Intune app protection policies and DRM to Office documents [10]
- MacOS MDM controls limited compared to Windows controls [3][11]
- Use of Intune APIs requires an additional license [3]

Vendor (UEM solution): IBM (MaaS360)

Key points

- CMT for supporting legacy operating systems and devices via BigFix [12]
- Support for containerised apps [13]
- Identity Access Management (IAM) available but requires additional product (IBM Cloud Identity) [14]

Vendor (UEM solution): Microsoft (Enterprise Mobility + Security)

Key points

- Integration of System Center Configuration Manager (SCCM) CMT if desired [3]
- Tight integration with Office 365 [15]
- Simple pricing structure with only two tiers of product [16]

Vendor (UEM solution): MobileIron (MobileIron (UEM))

Key points

- Validated against multiple security standards and certifications [17]
- Support for containerised apps and per-app VPN [18]
- Use of Intune APIs requires an additional license [3]

Vendor (UEM solution): VMWare (Workspace ONE)

Key points

- Chrome OS management possible [3][19]
- Virtual Desktop Infrastructure (VDI) via VMware Horizon available on highest tier [20]
- Support for containerised apps and per-app VPN [20]
- Integration with SCCM through VMware AirLift [21]

5.1.2. UEM selection

Following assessment of the five UEM solutions discussed earlier in this document, the author believes VMware's Workspace ONE would be the preferred choice. VMware have acquired well-regarded companies (such as Airwatch [19] and Boxer [20]) and integrated their products to offer a comprehensive UEM solution. It appears to offer the most rounded operating system support of the five UEM solutions that were considered, including support of legacy and IoT devices, as well as Chrome OS. It has parity with other UEM solutions for security provisions, with per-app VPN and app containerisation available.

5.2. BYOD discussion

The following sections will outline some of the potential benefits of a BYOD implementation, as well as areas of caution.

5.2.1. Potential benefits

Reduced equipment costs – depending on the type of policy being adopted, devices being provided by the employees instead of the organisation may forgo the need for organisational expenditure on equipment. As well as reducing or negating the cost of equipment procurement, on-going overheads for support contracts would be similarly reduced as the onus would be on the employees to manage support for their devices. Whilst there would be a cost for a UEM

solution, a solution would likely be implemented in any case if the organisation chose to provide its staff with devices. This benefit would not be likely if a policy was adopted where personal devices replace enterprise devices, as this implementation usually incorporates an allowance for the employee to purchase equipment [1].

User familiarity and confidence with devices – as the employees would choose their preferred devices, they would be able to choose the devices they are most comfortable or familiar with, or that are most appropriate for the type of work they do. This has the potential for decreasing the amount of support and training needing to be disseminated to employees, and therefore reducing the amount of resources and funding required for support.

Increase in productivity – the aforementioned familiarity with their devices should make employees more efficient and therefore productive. Additionally, employees are afforded greater flexibility in terms of working hours and location, for example by making greater use of ‘fragmented’ time [16].

5.2.2. Areas of caution

Potential for data leakage – the portability of mobile devices when combined with insufficient security measures can greatly increase the potential for data leakage. Theft or loss in such a scenario would compromise the security of the data of the device, and inadequate security controls on devices could lead to data leakage through intentional or unintended misuse.

Device security may vary – device security can vary based on the device vendor and age. For example, Duo Labs’ research in 2016 showed that of the 68% of Android devices that could receive security patches, only 25% were running the most recent patch (as of 30th April 2016) [17]. Google’s own analysis in October 2018 of the split of Android versions across devices shows 29% of devices having a version of Android lower than Android 6.0 Marshmallow [18], itself a four-year-old operating system having been released on 5th October 2015 [19]. Additionally, some users may choose to gain privileged control over their device via rooting (Android) or jailbreaking (iOS) it. This could potentially allow malicious apps or code to execute with superuser permissions.

6. Conclusion and future work

6.1. Conclusion

The author's conclusion is that implementation of a BYOD policy will have a positive impact on the productivity and efficiency of Hyper-fort as an organisation. The author suggests the policy is aimed at users using their devices alongside their current enterprise devices (e.g. staff) or those who would not usually be provided with a device (e.g. clients). Whilst there are potential security dilemmas that need to be accounted for, the widespread adoption of BYOD policies in various sectors means solutions and strategies have already been found to counter-act them. From a network perspective, segregation of devices and their traffic on the network, and strong cryptography for establishing connections and data transmission can provide protection from data leakage. From a device perspective, a complete UEM solution with appropriate policies and access control can protect sensitive data from deliberate and unintentional data leakage. These counter-measures reduce the risks associated with BYOD sufficiently for the author to make their recommendation.

6.2. Future work

One potential area for future work would be to investigate the implications of the recently announced WPA3 security protocol. This incorporates several new features to improve security [21]. These include:

- Opportunistic Wireless Encryption (OWE) – provides data encryption to users on open wireless networks.
- Forward secrecy – protects previously transmitted data even if the password has been compromised after the transmission.
- Simultaneous Authentication of Equals (SAE) – replaces the PSK in WPA2-Personal and prevents attempts to retrieve the network password through the use of offline-dictionary attacks.
- Stronger encryption modes in WPA3-Enterprise – 192-bit minimum strength security protocols available as an optional mode.

Although WPA3 was announced in June 2018 [22], speculation suggests widespread adoption isn't expected until at least 2019 [23] [24] [25]. Similar to the transition from WEP to WPA, it is possible for some devices to be made WPA3 compliant through firmware updates [25][26].

7. Glossary

Acronym	Term
AAA	Authentication, Authorisation, Accounting
AP	Access point
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CLI	Command Line Interface
CMT	Client Management Tool
DRM	Digital Rights Management
EMM	Enterprise Mobility Management
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
LAN	Local Area Network
MDM	Mobile Device Management
NIC	Network Interface Card
PSK	Pre-Shared Key
QoS	Quality of Service
RFID	Radio Frequency Identification
SSID	Service Set Identifier
UEM	Unified Endpoint Management
UPS	Uninterruptable Power Supply
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired-Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

8. Bibliography

- [1] P. Lee and T. Struthers, “Understanding the Bring-Your-Own-Device landscape,” 2013.
- [2] J. McKendrick, “The Other MDM: Why ‘My Device Matters,’” *Database Trends Appl. Chatham*, vol. 31, no. 2, pp. 4–8, 2017.
- [3] K. Hess, *Unified Endpoint Management For Dummies, IBM Limited Edition These*. Hoboken: John Wiley & Sons, Inc., 2017.
- [4] C. Silva, R. Smith, M. Bhat, B. Taylor, and R. Doheny, “Magic Quadrant for Unified Endpoint Management Tools,” 2018.
- [5] Google, “What is a work profile? - Android Enterprise Help,” 2018. [Online]. Available: <https://support.google.com/work/android/answer/6191949?hl=en>. [Accessed: 02-Dec-2018].
- [6] Hexnode, “List of iOS Supervised mode features by version - Help Documentation | Knowledge Base | Hexnode MDM.” [Online]. Available: <https://www.hexnode.com/mobile-device-management/help/ios-supervised-mode-features/>. [Accessed: 02-Dec-2018].
- [7] “What’s new in MDM enrollment and management | Microsoft Docs,” *Windows IT Pro Center*. [Online]. Available: <https://docs.microsoft.com/en-us/windows/client-management/mdm/new-in-windows-mdm-enrollment-management>. [Accessed: 02-Dec-2018].
- [8] VMWare Inc., “Productivity Apps | VMware AirWatch,” 2018. [Online]. Available: <https://www.air-watch.com/capabilities/productivity-apps/>. [Accessed: 02-Dec-2018].
- [9] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.
- [10] K. Curran and E. Smyth, “Demonstrating the wired equivalent privacy (WEP) weaknesses inherent in wi-fi networks,” *Inf. Syst. Secur.*, vol. 15, no. 4, pp. 17–38, 2006.
- [11] E. Tews, R.-P. Weinmann, and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds,” in *Information Security Applications. WISA 2007. Lecture Notes in Computer Science*, 4867th ed., S. Kim, M. Yung, and H. Lee, Eds. Heidelberg: Springer, 2007, pp.

4–6.

- [12] B. Mitchell, “Understanding Wireless Protected Access 2 (WPA2),” *Lifewire*, 2018. [Online]. Available: <https://www.lifewire.com/what-is-wpa2-818352>. [Accessed: 07-Dec-2018].
- [13] E. Geier, “Moving to WPA/WPA2-Enterprise Wi-Fi Encryption & Two Modes of WPA/WPA2: Personal (PSK) versus Enterprise,” *Cisco Press*, 2010. [Online]. Available: <http://www.ciscopress.com/articles/article.asp?p=1576225>. [Accessed: 09-Dec-2018].
- [14] G. Sims, “How easy is it to capture data from open free Wi-Fi? - Gary explains,” *Android Authority*, 2018. [Online]. Available: <https://www.androidauthority.com/capture-data-open-wi-fi-726356/>. [Accessed: 26-Dec-2018].
- [15] Eaton, “IBM Eaton UPS - How Much Battery Runtime Do You Need?” [Online]. Available: <http://powerquality.eaton.com/ibm/EMEA/btyrun.asp>. [Accessed: 17-Nov-2018].
- [16] “How does an Uninterruptible Power Supply (UPS) work? | CyberPower Power Blog.” [Online]. Available: <https://www.cyberpowersystems.com/blog/how-does-a-ups-work/>. [Accessed: 24-Dec-2018].
- [17] A. Luscombe, “Powering Up,” *Facilities Management Journal*, 2016. [Online]. Available: <http://www.fmj.co.uk/powering-up/>. [Accessed: 17-Nov-2018].
- [18] W. Stallings, *Cryptography and Network Security; Principles and Practice (Global Edition)*, 7th ed. Pearson Education Limited, 2017.
- [19] “VMware and AirWatch | UK.” [Online]. Available: <https://www.vmware.com/uk/company/acquisitions/airwatch.html>. [Accessed: 16-Dec-2018].
- [20] “VMware acquires Boxer to enhance AirWatch Inbox Solution | UK.” [Online]. Available: <https://www.vmware.com/uk/company/acquisitions/boxer.html>. [Accessed: 16-Dec-2018].
- [21] “Security | Wi-Fi Alliance,” 2018. [Online]. Available: <https://www.wi-fi.org/discover-wi-fi/security>. [Accessed: 21-Dec-2018].

- [22] “Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security | Wi-Fi Alliance,” 2018. [Online]. Available: <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security>. [Accessed: 21-Dec-2018].
- [23] S. Mudrakola, “WPA3: Much-awaited WiFi security upgrade finally announced,” *TechGenix*, 2018. [Online]. Available: <http://techgenix.com/wpa3-wifi-upgrade/>. [Accessed: 21-Dec-2018].
- [24] R. Priday, “WPA3 explained: Wi-Fi is about to get one of its biggest ever security updates | WIRED UK,” *Wired*, 2018. [Online]. Available: <https://www.wired.co.uk/article/wpa3-wifi-standard-security>. [Accessed: 21-Dec-2018].
- [25] G. Dorai, “Greater Wi-Fi Adoption brings the need of higher security,” *Cisco Blog*, 2018. [Online]. Available: <https://blogs.cisco.com/wireless/greater-wi-fi-adoption-brings-the-need-of-higher-security>. [Accessed: 21-Dec-2018].
- [26] “RT2600ac Release Notes | Synology Inc.,” 2018. [Online]. Available: <https://www.synology.com/en-uk/releaseNote/RT2600ac>. [Accessed: 21-Dec-2018].

9. Further reading

Bennett, L., & Tucker, H. (2012). Bring Your Own Device. *ITNOW*, 54(1), 24–25.
<https://doi.org/10.1093/itnow/bws010>

Lee, P., & Struthers, T. (2013). *Understanding the Bring-Your-Own-Device landscape*.

Olalere, M., Abdullah, M. T., Mahmud, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 5(2).
<https://doi.org/10.1177/2158244015580372>

10. Appendices

10.1. Appendix A – example app services

Services required by the BlackBerry UEM Client on Android (version 12.34.0.155084 from 03/12/2018).

This app has access to:



Device & app history

- retrieve running apps



Identity

- find accounts on the device
- add or remove accounts



Contacts

- find accounts on the device



Location

- precise location (GPS and network-based)



SMS

- read your text messages (SMS or MMS)



Phone

- read call log
- read phone status and identity



Photos / Media / Files

- read the contents of your USB storage
- modify or delete the contents of your USB storage



Storage

- read the contents of your USB storage

- modify or delete the contents of your USB storage

Camera

- take pictures and videos

Wi-Fi connection information

- view Wi-Fi connections

Device ID & call information

- read phone status and identity

Other

- interact with a device admin
- delete apps
- download files without notification
- modify secure system settings
- receive data from Internet
- view network connections
- pair with Bluetooth devices
- access Bluetooth settings
- connect and disconnect from Wi-Fi
- measure app storage space
- full network access
- close other apps
- run at startup
- enable app debugging
- set wallpaper
- control vibration
- prevent device from sleeping
- modify system settings
- toggle sync on and off
- install shortcuts
- uninstall shortcuts

- read Google service configuration

10.2. Appendix B – sample Wireless Access Policy

Hyper-fort Wireless Access Policy

1. Overview

Wireless technology has provided new opportunities for mobile working and collaboration. Hyper-fort's recognition of these opportunities has led to them adopting a Bring Your Own Device (BYOD) policy for their staff and clients. Whilst wireless technologies can increase productivity, they present security risks that require mitigation and management.

2. Purpose

Hyper-fort offers a wireless network for staff and clients to use their devices on. The purpose of this policy is to define what Hyper-fort considers to be acceptable use of their wireless infrastructure.

3. Scope

This policy is applicable to all users of Hyper-fort's wireless network infrastructure. This includes staff and clients of Hyper-fort, and any devices they connect to the Hyper-fort wireless network.

4. Policy

4.1. Staff users

- Staff will connect their devices using only the individual credentials they have been provided.
- Staff users will not access inappropriate or criminal content whilst on Hyper-fort's network.
- Staff users will not disseminate credentials to other users (staff or otherwise).
- Staff users will apply applicable security updates to any devices they connect to the Hyper-fort network.
- Staff users will not knowingly connect compromised devices (e.g. virus infected) to the Hyper-fort network.
- Staff users will report foul-play to the system administrators.
- Staff users will periodically change their password in line with Hyper-fort's password policy.

4.2. Clients users

- Client users will not access inappropriate or criminal content whilst on Hyper-fort's network.
- Client users will report foul-play to the system administrators.
- Client users will apply applicable security updates to any devices they connect to the Hyper-fort network.
- Client users will not knowingly connect compromised devices (e.g. virus infected) to the Hyper-fort network.

5. Violations of policy

Violation of the policy by staff of Hyper-fort may result in disciplinary action and possibly termination. Violation of the policy by a client may result in termination of their access to the Hyper-fort network and the matter being reported to the client's employer. Illegal activity of any users will be reported to the relevant authorities.

6. Distribution

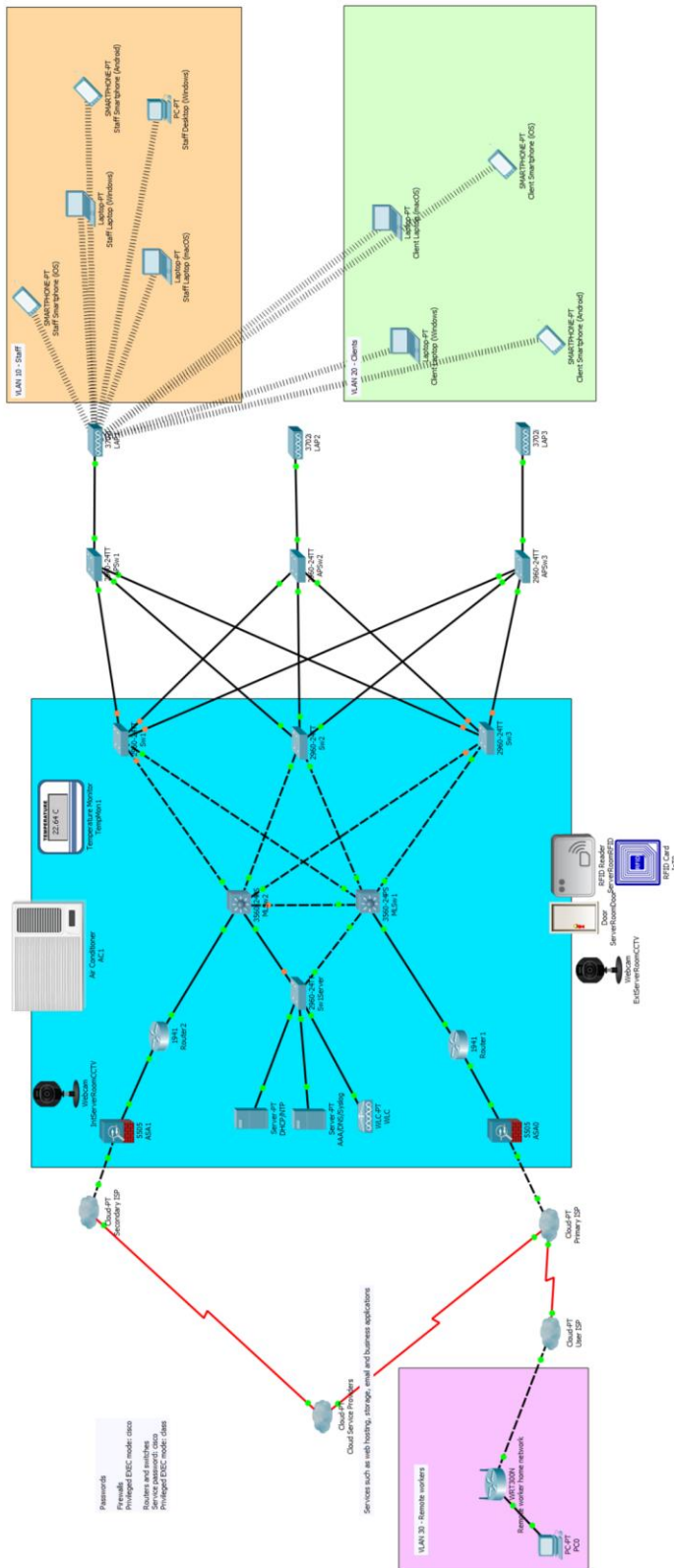
This policy will be disseminated to all Hyper-fort staff and clients.

7. Policy review and modification

The policy should be reviewed annually or if changes are made to working practices or infrastructure that may have an impact on this policy. This should be carried out by system administrator in collaboration with the appropriate parties in the organisation.

10.3. Appendix C – Packet Tracer screenshot

Screenshot of Packet Tracer example.



10.4. Appendix D – flowchart of staff user connecting to network

An example flowchart of a staff user connecting to the network.

