



Internet Technology and Security

Synthesized solutions to potential real life scenarios

Shaun Holborow

Course: Computer Networks and Cyber Security

Faculty name: SOAC

Student Number: 1704229

Introduction:

In recent years, the increase in mobile internet capable devices (laptops, tablets, smart phones etc.) has become difficult for companies to handle them commercially the way they used to not long ago as they are now much more commonly used for basic or important tasks (social interaction, banking, shopping, research etc.), the result of this has spurred the public into further pressuring of these businesses associated with the sale of said devices into opening them up to being capable of performing more important tasks and one of the most demanded functions of said devices is the ability for employees to use these devices to access various corporate networks and the suggestion has been coined the name “Bring Your Own Device” or (BYOT) for short.

For Shaun’s assignment, he was placed in a scenario where he works for company named “Hyper-fort” which is a consultancy company specializing in the energy sector and has a large presence globally. The company uses a form of cloud services to provide IT services to its own staff and clients, according to the company it’s been estimated that 95% of the company’s network is utilised via wireless means.

The company also has a large online and social media presence to advertise its activities efficiently. However because of the size of its staff and customer base, the company has recently been faced with massive pressure to enable staff and clients the ability to utilise their mobile internet devices to access the company’s network/resources but the concerns from the company regarding this are staff/client personal data as well as intellectual properties which is valued in the billions.

Thus hired under the job position as an IT Security Consultant for Hyper-fort, he was tasked with providing a list of recommended guidelines with a comprehensive security policy that covers all areas of the enterprise network which includes online and offline resources.

Shaun Holborow was tasked with creating a report that describes the results of his work effort involved with a scenario that had him as an IT Security Consultant hired by Hyper-fort to provide recommended guidelines on a well thought-out security policy that covers all aspects of the enterprise network which includes online and offline resources.

Thus he created the three types of policies required for this network to function correctly and as preferred by the company.

User Policy (framework):

- I will only access my own email or sites which are authorised using my own username and password
- Only use the devices to support my work in the company
-

Device Management Policy (framework):

-

Security Policy (framework):

-

After these policies were created and chosen to represent the recommended guidelines, a data flow diagram was created to present the overall implementation of the BYOT management architecture that he had decided to utilise for this task as shown below:

Data flow diagram:

Once the data flow diagram was finished and implemented, he then created a virtual configuration of the network using the software “Packet Tracer” in order to demonstrate the overall effectiveness of the design as a Hyper-fort Ltd enterprise network.

Proposed network configuration:

In order for the network plan to function, a type of mobile device management software had to be used and the chosen type was software known as "IBM MaaS360" which was chosen for a variety of reasons which were listed below as the following bullet points [9]:

- Platform compatibility - Works on practically all types of operating systems.
- Remote Lock - Can be remotely locked from almost any location outside the company.
- Remote Wipe - Can be remotely wiped of all data
- Geofencing/Location services - Used to protect said devices with important data from the company.
- User Self Registration.
- Granular Selective Wipe - Only wipes data related to the company without requiring a factory reset.

Upon choosing the proposed software for use of BYOT, an explanation was asked by the company in regards to the rationale behind the choice which was...

Finally he was asked about the advantages and disadvantages behind the utilisation of BYOT which he listed for each as the following below using the information provided from Optimus Learning [8]:

Advantages:

Lower costs –

One of the more well-known advantages of using BYOD, any purchases, repairs etc. required are pushed as the sole responsibility of the owner of said devices thus any costs to the company they work for are immediately mitigated entirely.

Technological Familiarity –

When familiarity is present with the user and his chosen device of use, the typical benefits of this result are things like increases in work efficiency due to his/her knowledge of the tools available with said device that are required for said work to be completed correctly and on time.

This also results in a significant decrease in training costs that would otherwise be required if the employee could only work with the machines provided by said company.

Flexibility –

One of the known problems of using only company devices to work is that it reduces flexibility for the employee considerably since in order to complete his/her work they would most likely have to work with several types of devices and if they wanted to use these outside the company then they would most likely have to either buy or ask the company for use of said devices outside the company itself.

With BYOD however this is mitigated almost entirely as all necessary equipment/tools would be available for use on the one portable device the owner possesses and also don't need to obey any rules involving company owned devices as the device being used not owned by the company, thus efficiency as well as flexibility is increased considerably.

Disadvantages:

Costs for the employee –

One of the more obvious problems mentioned, Due to the costs of owning said device as well the potential repairs required after prolonged usage, not all employees would be able to benefit from it even if they wanted to.

Device disparities –

Devices provided by the said companies for their employees are typically catered for the specific tasks required them which means providing them with tools that work and look as intended by the company however due to the nature of BYOD, these requirements can be significantly more difficult to achieve as devices not specified by the company can vary greatly with things like compatibility and clarity of graphics thus adaptation has to be considered by the company if they wish to utilise this part of the policy with the rest.

Security –

Considerable funding in this area with various companies is still present for a reason, with the ever shifting dynamic that is security of devices and data. Companies continue to change or update their policies and system to counter act such threats and thus spending is put into various hardware and software to insure all devices and data is secure however this is considerably more complicated with the BYOD policy as employees are prudent to having sufficient security on even their own systems whether due to laziness or lack of knowledge to implement said defences, as such this adds even more risks for the company and its employees unless strict measures in the form of policies are put into effect to insure no devices or data is compromised.

With regards to the design, it was required for the following issues to be assessed and handled with solutions to mitigating threats that would result from them as shown below:

Q:What type of data is retained by the mobile devices connecting to Hyper-fort network?

A:

Q:What is the potential for data leakage when the participating devices leaves the office environment?

A:

Q:How to address the blending of personal and business usage when devices are in office.

A:

Q:What strategy to deploy to deal with different brands of devices.

A:

Q:What strategy to deploy to deal with different Operating System platforms.

A:

Q:What strategy to deploy to deal with different application on user devices.

A:

Q:What mitigating strategy will be deployed when the owner of a participating device leaves their employment or the device is lost, stolen, or fails.

A:

Bibliography/References

- [1] William Stallings, *Cryptography and network security, principles and practice*, 6th ed.: Upper Saddle River, NJ. : Prentice Hall, 2014.
- [2] Charles A. Snyder, Bliss N. Bailey Houston H. Carr, *The Management of Network Security: Technology, Design, and Management Control*, Illustrated, Revised ed.: Pearson, 2010, 2010.
- [3] Mark Ciampa, *Security + Guide to Network security fundamentals*, 4th ed.: Cengage Learning, 2012, 2012.
- [4] Michael Gregg, *Certified Ethical Hacker (CEH) cert guide*. Indianapolis, Indiana: Pearson, 2014.
- [5] Michael Solomon David Kim, *Fundamentals of information systems security*. Sudbury, Massachusetts: Jones & Bartlett Learning, 2012.
- [6] James Michael Stewart, *Network security, firewalls, and VPNs*. Sudbury, Massachusetts: Jones & Bartlett Learning, 2011.
- [7] Michael E Whitman and Herbert J Mattord, *Principles of information security*, 4th ed. Boston, Massachusetts: Course Technology, 2012.
- [8] (2013, September) Optimus Learning. [Online]. <https://www.optimuslearningservices.com/practical-ld/advantages-disadvantages-byod-in-learning/>
- [9] Paul Ferrill. (2018, January) PC Mag. [Online]. <https://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software>

