COMP09092 RESEARCH METHODS IN COMPUTING

Effect of BYOD (Bring Your Own Device) and use of mobile technologies on data security.

Table of Contents

Research Topic and Abstract

Research Topic: Effect of BYOD (Bring Your Own Device) and use of mobile technologies on data security.

The purpose of this research is to raise awareness of BYOD practice, identify its major security threats and risks associated with using mobile devises and other technology remotely for business purposes, focusing on term BYOD (Bring Your Own Device). This research will also focus on analysis of methods and techniques to help UK businesses to reduce those risks. 'The number of mobile phone users in the world is expected to pass the five billion mark by 2019. In 2016, an estimated 62.9 percent of the population worldwide already owned a mobile phone. The mobile phone penetration is forecasted to continue to grow, rounding up to 67 percent by 2019.' *(Statista.com, 2013-15)* With numbers constantly rising it became more cost-effective, convenient and less time consuming to use employees own mobile phones and other devices for business purposes. With more companies moving to remote use cell phones, tablets and laptops, security issues arise which will be researched within this project. Methods of research will include primary and secondary research with quantitative and qualitative data.

Aims and Objectives

1. Investigate and produce an evaluation of use of mobile phones and BYOD within businesses and the importance of mobile security within organisations.
2. Investigate and identify main security threats and risks associated with BYOD practice.
3. Current advisory methods and standards used to promote mobile security including BYOD and its effectiveness.
4. Insight on current mobile device usage for work including BYOD and its procedures and standards on mobile security within UK and its effectiveness.
5. Comparison and contrast on advisory methods and standards with those existing within organisations (Comparison of findings from Aim 3 and 4).
6. Produce guidelines that give clear insight on what ways UK business can adapt BYOD securely or improve their existing BYOD security practice.

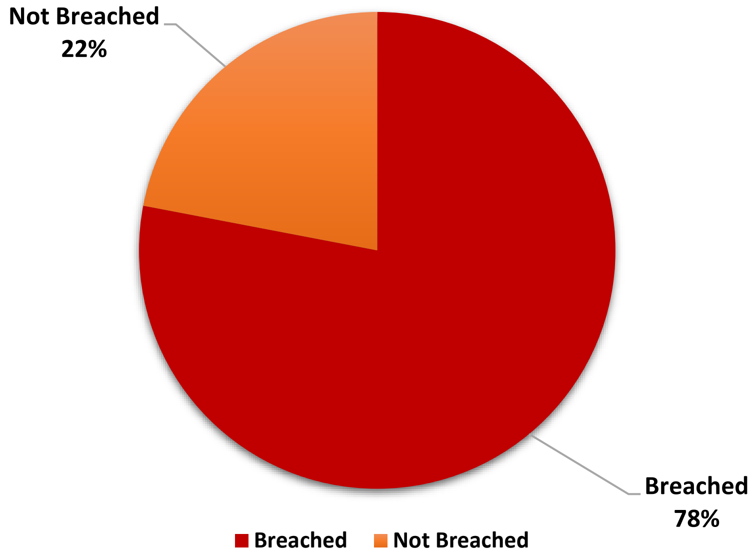
Justification

Just under half (46%) of all UK businesses identified at least one cyber security breach or attack in the last 12 months. This rises to two-thirds among medium firms (66%) and large firms (68%). *(Gov.uk, 2014)*

Most common breaches include receival of fraudulent e-mails, password attacks, viruses, malware and people impersonating the organisation or its employees to gain benefits from it. All those breaches and not only limited to, happen using mobile devices and other technology with remote access.

According to BT *(2014)* 95% of employees are allowed to use their devices for business purposes with full remote access to the organisation’s network ‘and yet 68 % per cent of respondents admit that their organisation has suffered a mobile security breach in the last 12 months.’ Such attacks result in loss of money averaging in hundreds of thousands, often more than the businesses are worth meaning many organisations will not be able to handle the consequences of such data breaches.

Figure 1. Data Breaches in 2015 (UK)



(Source: Experian, 2013)

According to data shown in Figure 1 it is believed that more than ¾ of businesses in the UK suffered an IT data attack in 2015. Furthermore 'almost a third of those surveyed don't have a data breach response plan in place'. *(Experian, 2013)*

As per survey, 53 % of the corporate world officially approved and accept BYOD concept and its practice. In that total 53 %, 20% of subsidy to employees who already start using their own smart-phones, PCs or laptops in the organization for work purposes. *(Experian, 2013)*

It is perceived that in many cases, businesses do not recognise remote security as an aspect worth investigating and consideration when using mobile devices for business purposes. Amongst many other goals mentioned earlier, this research is aimed to fill or at least contribute to further investigation of the gap of lack of alertness and understanding of BYOD security.

Ethical issues

Ethical Issues in Research Subject, Purpose and Questions		
Area/Issue	**Consideration**	**Adjustment**
Subject matter	Is the subject controversial, sensitive or it could be upsetting for someone?	Subject was chosen taking intro consideration other public matters and it is believed as not upsetting and not controversial for the majority of the potential readers
Subject matter and purpose	Is the subject matter and its purpose meaningful to others besides the researcher?	It is intended that the subject and its purpose will be beneficial to various groups of readers including private and public organisation and it will

		be written in an informative way
Ethical Issues in Data Collection		
Issue	**Consideration**	**Adjustment**
Confidentiality	Will the data be protected and stored along with Data Protection Act 1998?	Data collection will only be limited to the information necessary and with omitting personal details.
Consent	Will the data be collected with the consent of the participants?	Participants will be gathered voluntarily, and they will be reminded that they can withdraw their consent at any point of the research. When collecting primary data (interviews, questionnaires)
Ethical Issues in Data Analysis and Interpretation		
Issue	**Consideration**	**Adjustment**
Confidentiality	Will the study protect the anonymity if the individuals participated?	Data will be shown with no personal information unless agreed and pseudonyms of individuals or places will be used in necessary to ensure confidentiality.
Holding data	How long the data will be stored?	Primary data is intended to be stored for a year after research being conducted.
Interpretation	How the data will be presented? Will it show biased opinions?	Data will be presented with no prejudice and with no influence of third parties.
Ethical Issues in Writing and Disseminating the Research		
Issue	**Consideration**	**Adjustment**
Content	Will the content cause offence or distress to the reader?	Content will be written by taking into consideration various groups and will not intentionally offend any readers.

Literature Review

Key terms

Key terms: BYOD, Bring Your Own Device, mobile security, remote access security

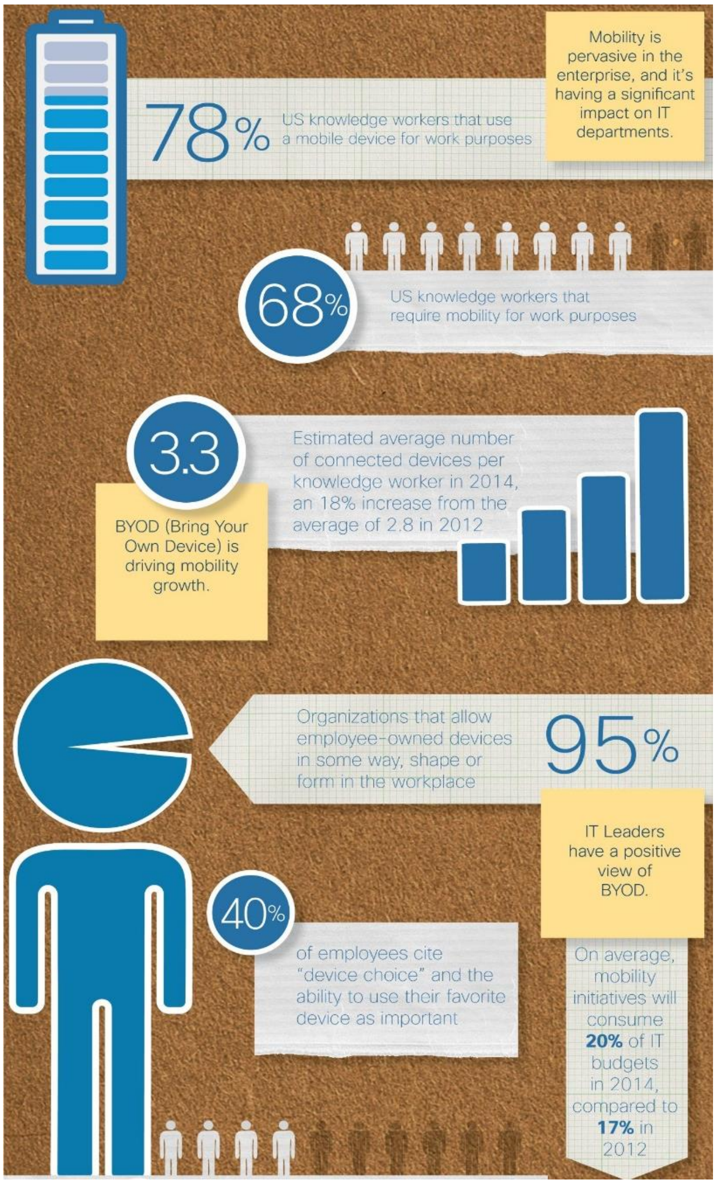
Term BOYD

Term Bring Your Own Device refers to using various devices for business purposes which can be detailed: s

- Devices: Universally BYOD covers (mainly) mobile devices, tables and computers (laptops)
- Connectivity: It can range from connection to organisational internet, network, use of e-mail or any other applications for business purposes as well as organisational systems and applications.

- Usage: It can be categorised into BYOD:
- BYOD as a Complement: allowing individual employees to use personal devices alongside enterprise devices
- BYOD as a Replacement: replacing individual’s enterprise devices with employee-owned devices.
- BYOD as an Addition: permitting the use of employee-owned devices who would not/ did not have access to an enterprise device. *(Detoitte, 2013)*

Term BOYD in 2003 but started rapidly grow in 2011. As employers struggle with keeping up with the latest technology due to its constant development, BYOD was introduced to enable employees use their own devices for work purposes. According to Cisco Survey *(2012)* BYOD is 'a getaway to greater business benefits'. It not only saves a significant amount of money on software and hardware but also promotes productivity and connectivity within the organisations. Moreover, 'Over three-fourths (76%) of IT leaders surveyed categorized BYOD as somewhat or extremely positive for their companies, while seeing significant challenges for IT'.


Mobility is pervasive in the enterprise, and it's having a significant impact on IT departments.

78% US knowledge workers that use a mobile device for work purposes

68% US knowledge workers that require mobility for work purposes

3.3 Estimated average number of connected devices per knowledge worker in 2014, an 18% increase from the average of 2.8 in 2012

BYOD (Bring Your Own Device) is driving mobility growth.

Organizations that allow employee-owned devices in some way, shape or form in the workplace 95%

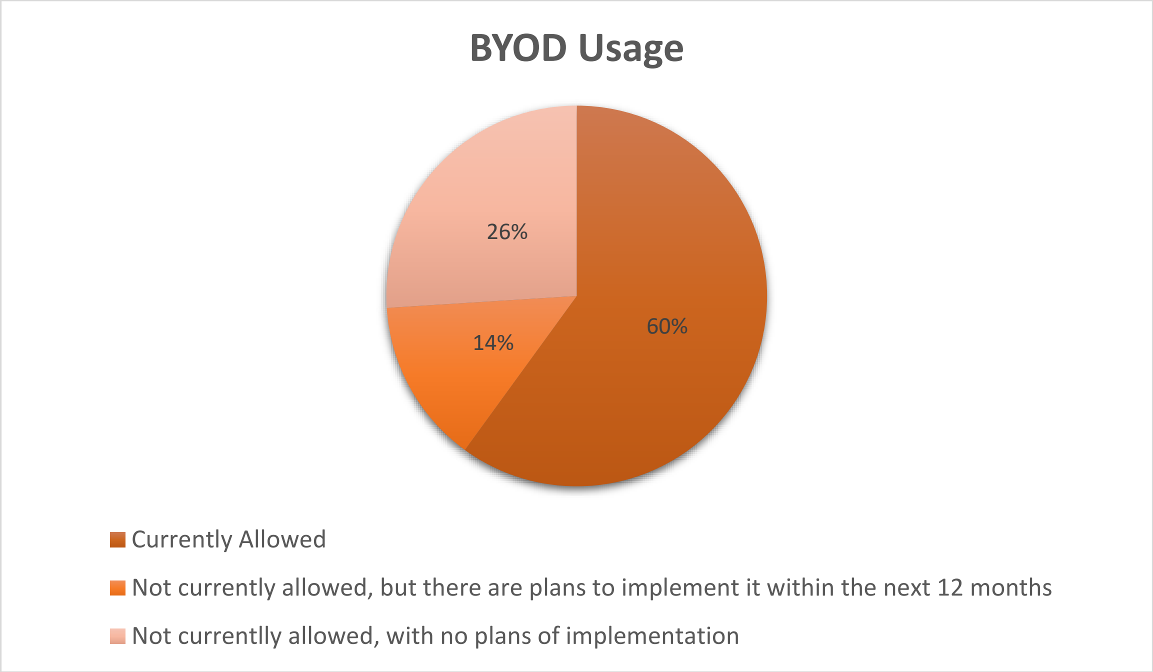
IT Leaders have a positive view of BYOD.

40% of employees cite "device choice" and the ability to use their favorite device as important

On average, mobility initiatives will consume **20%** of IT budgets in 2014, compared to **17%** in 2012

Source: Cisco (2012)

Status of BYOD



Source: Cisco (2012)

According to Tech Dar Pro Research from 2013, 74% of respondents are using or planning on using BYOD practice within their workplace, however only 30% of their IT departments were supporting this practice and 61% of respondents agreed that they see their BYOD devices as less secure compared to standard employee owned devices.

Despite the concerns, major companies such as Apple, Cisco, IBM, Citrix, HP or Kaspersky are in favour of BYOD practice, and recent survey conducted by Vanson Bourne revealed that only 44% of UK Businesses believe that BYOD gives them a competitive advantage, compared to 74% in the USA. This draws a conclusion that although BYOD is being widely used, many organisations do not realise its full potential or might not use BYOD effectively.

Benefits of BYOD

BYOD is believed to save costs from buying devices and upkeep of them however, 67% of IBM survey believe respondents that BYOD will increase total costs. Research conducted by Cisco *(2013)* shown that costs for device security, mobile management or back-end integration costs were reported as higher after implementing BYOD practice. However, the same research resulted in 46% participants reporting their device costs decreased and 82% agreeing that worker productivity has increased as well as their bottom line revenue.

Productivity gains

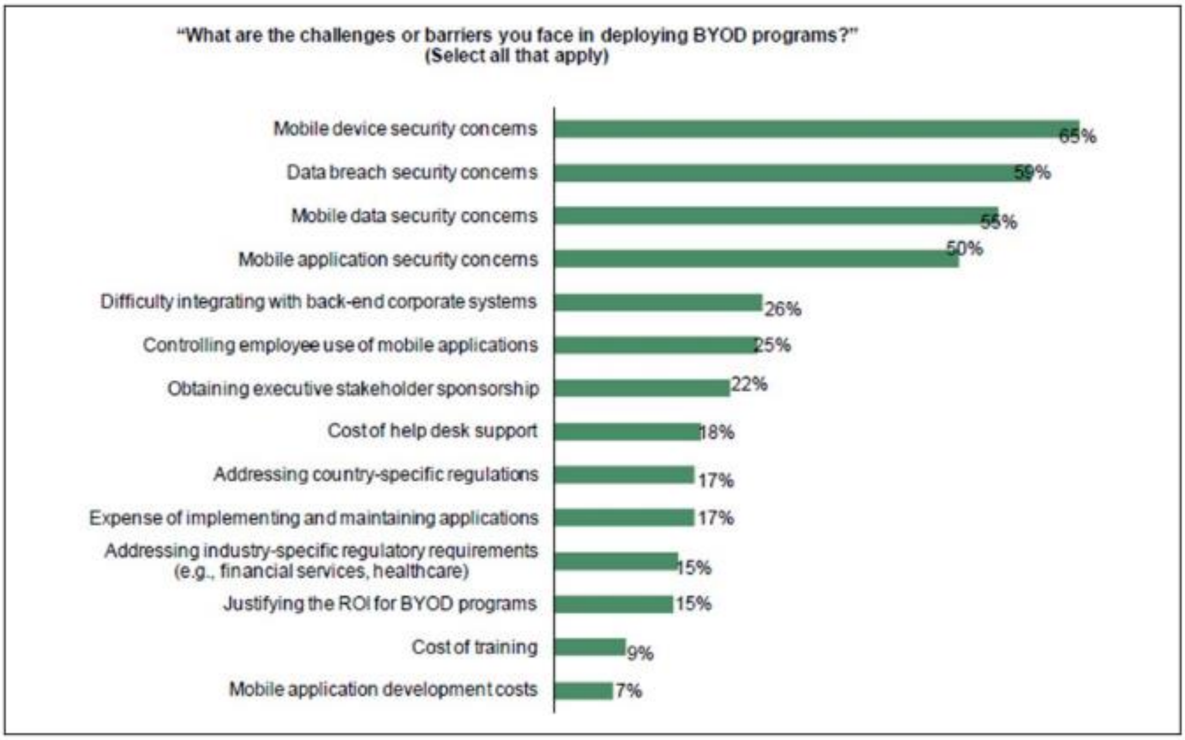
The last suggestion mentioned earlier from the Cisco (2013) leads to another perceived advantage such as productivity gains. “Productivity can be gained through BYOD in three ways: increasing the number of working hours, improving employee efficiency in working hours and putting technology into hands that would not usually be eligible.” *(Deloitte, 2013)*

It is believed that an employee who have greater access to communications and its business systems, is more likely to use it outside their working hours. While it benefits the business itself, an ethical issue arises as it can imbalance work-life separation and employee’s work satisfaction.

Employee Satisfaction and Flexibility

It is believed that employees who use their devices for work purposes have increased satisfaction of their work and its environment as they use equipment they are familiar with. BYOD also grants flexibility as employees can work remotely wherever and whenever they prefer to.

Main Security Concerns when using BOYD



Source: Forrester (2012)

Survery conducted by *Forrester (2012)* revealed that the main challenges for business to implement BYOD is security of their devices and data. Furthermore, focusing on the security of devices and its data, *Morrow (2012)* shows that data loss/leakage, DDos (Distributed denial of service) and malware are the main security threats when using BYOD practice.

TYPE OF THREAT	CAUSES	IMPLICATIONS
DATA LOSS/LEAKAGE	-Physical loss of the device -Malicious user of mobile device -Unauthorised access of the device	-Confidential data being compromised -Violation of General Data Protection Regulation
DDOS	-Malicious attacks on the server -Jamming -Blocking -FLooding	-Negative impact on the server -Possibility of the server being exposed to the attacker -Loss of service for the customers
MALWARE	-Spam -Phishing -Smishing -Third-party apps/programs with imbedded viruses	-Malfunction of the operational system -Confidential data being compromised

"The Business and personal data coexist on same device then it's very difficult to find a balance between a strict security control of enterprise and privacy of personal data, specifically when the device is no longer a corporate issued asset. Incident detection such as lost devices versus breached devise or actual versus suspected breach is also a problem. Confidential information is being sent or received over an unsecure channel. Many mobile devices are always on and connected, so the vulnerability to malicious attacks increases through different communication channels. Connecting rouge devices and access points with the help of device can also be problematic. Some human factors like a disgruntled employee may store confidential business data on his personal removable media and give this information to its competitor which may cause loss to the organization."
(Naventta, 2012)

Other work undertaken within the area of BYOD

Author	**Research**	**Summary**
Yong Wang, Jinpeng Wei, Karthik Vangury	BYOD Security Issues and Challenges	Research focuses on identifying main security issues such as theft, malware, data leakage and possible solutions to tackle those issues
Hormazd Romer	BYOD Security Recommendations	Research focuses on security recommendations for businesses using or planning on implementing BYOD
Jessica Keynes	Bring Your Own Devices (BYOD) Survival Guide	Research covers variety of areas of BYOD, from security to implementation, benefits and recommendations particularly focused on SME's.
Richard Oliver	Why the BYOD boom is changing how we think about business it	Research focuses on how BYOD changes attitudes about remote access working within business and how technology affect current business processes

Research Questions

Following literature review allow to draw conclusions. Use of smartphone and other technology became a norm within variety range of organisations. As technology advances and constant demand for being up to date with the latest software and hardware allowed Bring Your Own Device practice to become popular more than ever. Whilst in theory it can save costs, some studies show whilst using BYOD purchasing hardware is no longer necessary, security and training can potentially cost businesses more. As literature review shown BYOD has many benefits, however its major drawback is security concerns which makes businesses questioning this method. This leads to following questions which this research project will focus on:

- What are the businesses within UK opinions in relation to BYOD?
- What is the reality of BYOD security within business who practice BYOD?
- Is security of BYOD uncertain due to human approaches or defective business set up?

- How BYOD can be used to maximise security of data?

Research Methodology

The following research methods have been chosen within the project:

Quantitative Research

Definition

"Quantitative methods emphasize objective measurements and the statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys. Quantitative research focuses on gathering numerical data." (Babbie, 2010)

Questionnaires

Questionnaires will be issued to the organisations who raised interest in BYOD methodology. Method of delivery will be via online as well as paper based. If needed, questionnaire can be also conducted via telephone call or in person.

Protocol of the questionnaire will include the following components:

- Participants will be explained the purpose of the questionnaire, how the data will be gathered, used and presented within the project. They will be also remained of the protection of their personal details and information gathered, and of the possibility of withdrawal at any point of studies.
- Length of the questionnaire, overview and acknowledgement of how the interview will be recorded will also be provided.
- Participants will be thanked for the involvement and informed of further steps being taken with data.

This type of research will be used to meet Aim 1, 3 and 4 of the project.

Qualitative Research

Definition

"The word qualitative implies an emphasis on the qualities of entities and on processes and meanings that are not experimentally examined or measured [if measured at all] in terms of quantity, amount, intensity, or frequency." *(Norman,2000)*

Interviews

Interviews will be conducted with participants:

- SME's and large-sized companies: Business Owners whom allow BYOD (or plan to allow) and its employees
- SME's and large-sized companies: Business Owners whom do not allow BYOD (and have no plans of allowing) and its employees

Interviews will be conducted in a form of face-to-face, telephone or focus group interviews with six to eight interviewees in each group. The meeting will involve unstructured, open-ended questions as well as closed questions to have elicit views and opinions from the participants. This type of research will be used to meet Aim 3 and 4 of the project.

Protocol of the interview will include the following components:

- Participants will be explained the purpose of the interview, how the data will be gathered, used and presented within the project. They will be also remained of the protection of their personal details and information gathered, and of the possibility of withdrawal at any point of studies.
- Length of the interview, overview and acknowledgement of how the interview will be recorded will also be provided.
- Participants will be thanked for the involvement and informed of further steps being taken with data collected.

Documents

Research will focus on collecting public qualitative documents such as newspapers, website articles, official reports and private documents such as e-mails, private journals (with ethical assessment conducted and sensitive data being protected).

Observations

Observations are not planned to be conducted within the scope of the project due to being exposed to sensitive, organisational data and due to ethical issues arising it might not be possible to do so. If, however agreement could be drawn between the researcher and the organisation to conduct them, they would be protocoled as followed:

- Participants will be explained the purpose of the observation, how the data will be gathered, used and presented within the project. They will be also remained of the protection of their personal details and information gathered, and of the possibility of withdrawal at any point of studies.
- Length of the observation, overview and acknowledgement of how the observation will be recorded will also be provided.
- Participants will be thanked for the involvement and informed of further steps being taken with data collected.

This type of research will be used to meet Aim 3 and 4 of the project.

Bibliography

Cisco Study: IT Saying Yes To BYOD | The Network | The Network. 2018. Cisco Study: IT Saying Yes To BYOD | The Network | The Network. [ONLINE] Available at: https://newsroom.cisco.com/press-release-content?articleId=854754. [Accessed 13 March 2018].

Eddy, N, 2013. BYOD. Businesses must adapt to permanent BYOD presence, [Online]. 1, 15. Available at: http://www.eweek.com/small-business/businesses-must-adapt-to-permanent-byod-presence-ovum [Accessed 6 March 2018].

Forrester. (2012). Key strategies to capture and measure the value of consumerization of IT. Cambridge, MA: Forrester Consulting

French, A, 2014. Current Status, Issues, and Future of Bring Your Own Device (BYOD). Current Status, Issues, and Future of Bring Your Own Device (BYOD), [Online]. 35, 9. Available at: file:///C:/Users/eweli/OneDrive/Uni/Research/BYOD_CAISpaper.pdf [Accessed 7 March 2018].

Keyes, K., 2013. Bring Your Own Devices (BYOD) Survival Guide. Taylor & Francis.

Leavitt, N. (2013). Today's mobile security requires a new approach. IEEE Computer Society

Matthew Creamer. 2018. How Much Can You Save?: A BYOD Cost Analysis. [ONLINE] Available at: https://www.repsly.com/blog/field-team-management/save-money-byod-cost-analysis. [Accessed 16 March 2018].

Miller, K, 2012. BYOD: Security and Privacy Considerations. BYOD: Security and Privacy Considerations, [Online]. 1, 3. Available at: file:///C:/Users/eweli/OneDrive/Uni/Research/BYOD_Security_and_Privacy_Considerations.pdf[Accessed 7 March 2018].

Oliver, R, 2012. Why the BYOD boom is changing how we think about business it. Why the BYOD boom is changing how we think about business it, 7/10, 28.

Romer, H, 2014. Best practices for BYOD security. Best practices for BYOD security, 1, 3.

Rose, C, 2013. BYOD: An Examination Of Bring Your Own Device In Business. BYOD: An Examination Of Bring Your Own Device In Business, [Online]. 17, 6. Available at: file:///C:/Users/eweli/OneDrive/Uni/Research/7846-Article%20Text-31296-1-10-20130507.pdf [Accessed 7 March 2018].

Vanson, Bourne, 2015. Research Insight:. Blurred lines: Is BYOD changing the way we work?, [Online]. 1, 4. Available at: https://www.vansonbourne.com/ResearchReports/PDFs/BYOD/VB-BYOD-Brochure.pdf[Accessed 6 March 2018].

Wang, Wei, Vangury, Y, (2014). Bring Your Own Device Security Issues and Challenges. In The 11th Annual IEEE CCNC- Mobile Device, Platform and Communication. Nevada, January 2014. January 2014: Dakota State University. 6.

References

Babbie, Earl R. The Practice of Social Research. 12th ed. Belmont, CA: Wadsworth Cengage, 2010; Muijs, Daniel. Doing Quantitative Research in Education with SPSS. 2nd edition. London: SAGE Publications, 2010.

Deloitte, 2013. Understanding the Bring-Your-Own-Device landscape. Understanding the Bring-Your-Own-Device landscape a Deloitte Research report, [Online]. 1, 28. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-understanding-the-bring-your-own-device%20landscape.pdf [Accessed 12 March 2018].

Denzin, Norman. K. and Yvonna S. Lincoln. Handbook of Qualitative Research. 2nd edition. Thousand Oaks, CA: Sage, 2000.

Experian, 2016. SMEs Under Threat. SMEs Under Threat The crippling consequences for unprepared small to medium-sized businesses, [Online]. 1, 14. Available at: http://www.thepowerofwords.co.uk/images/pdf/Experian_whitepaper_FINAL2016.pdf [Accessed 6 March 2018].

Forrester. (2012). Key strategies to capture and measure the value of consumerization of IT. Cambridge, MA: Forrester Consulting

Naventta, D, 2012. Legal Implications of BYOD. Legal Implications of BYOD, 1, 15.

Statista. 2018. • Number of mobile phone users worldwide 2013-2019 | Statista. [ONLINE] Available at: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/. [Accessed 16 March 2018].

Technavio. 2018. Top 21 Companies in the BYOD Market - Technavio. [ONLINE] Available at: https://www.technavio.com/blog/top-21-companies-in-the-byod-market. [Accessed 16 March 2018].