STUDY ON SECURITY AND PRIVACY RELATED ISSUES ASSOCIATED WITH BYOD POLICY IN ORGANIZATIONS IN NEPAL

Prabin Shrestha[1] and R. N. Thakur[2]
[1] PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2]Assistant Professor (IT), Lord Buddha Education Foundation, Kathmandu, Nepal

ABSTRACT

The purpose of this study was to find an appropriate security framework for protecting organizations in data privacy, preventing data loss and data availability, and controlling all the risks and threats that arise with BYOD policies. Today, the trend of Bring Your Own Device (BYOD) is unavoidable in organizations of all sizes and industries. BYOD policies help increase productivity, increase employee satisfaction, reduce operating costs, innovate faster, and maintain a competitive advantage. BYOD also shows the general trend of providing all devices for all workers who want to work in the corporate network anytime, anywhere (for example, on a laptop, commenting on a tablet and using their smartphone with team members). In addition, the BYOD strategy helps staff easily stream information and access applications and data across all devices, whether they are provided by an employer or by an individual. At the same time, BYOD trends have also created security challenges for IT to protect and manage more diverse mobile devices and applications. Without proper security management policies, BYOD can cause problems for organizations, which can lead to many security risks, data privacy and protection threats. When implementing the BYOD strategy as a security framework in an organization, a strong information security management system such as NIST, ENISA, COBIT 5, ISO / IEC 27001 must be used.

Keywords: BYOD, Security, Threats, Data protection, Security Framework

1. INTRODUCTION

Bring your own device (BYOD) means employees bring personal devices (such as laptops, tablets, smartphones, USB drives and external hard drives) into the workplace, allowing organizations to use them to access the company's network, data systems & the app.

BYOD (Bring Your Own Device) is an enterprise IT strategy that allows employees to access sensitive corporate data at work through their enterprise IT infrastructure using their own devices (Li, 2014).

BYOD (Bring Your Own Device) is the growing trend of employee-owned devices in an organization. Laptops are the mostly used device, but employees also want to bring their smartphones, tablets and USB storage devices into the workplace. BYOD has become a part of the IT consumerization, bringing consumer devices to the workplace (Wigmore, 2019).

According to Kalman Frank, in 2013, BYOD was an unstoppable trend and people liked to use their mobile devices. In a 2012 survey by consulting firm Accenture, nearly 60% of respondents said they would be satisfied if they can use personal devices and applications.

(Huffpost, 2016), said that an organization can save money by buying equipment such as laptops and mobile phones. BYOD enhances the w4rk environment, employees work confidently and comfortably, and they feel happy and satisfied, which increases the company's

productivity. It also provides employees with mobility from work outside the home and office (Huffpost, 2016).

While BYOD has some benefits, it can open the door to new threats in your organization. According to Tech Pro Research's 2014 report, 78% of organizations mentioned that they are hesitant to use BYOD's number one for security. Virus infection data from employee devices can be copied to internal organizations. When employees use their devices in the office, there may be data loss, data breaches, and data theft (Techpublic, 2016).

Although BYOD began to appear in 2003, it did start in 2011 (Leavitt, 2013). According to Security vendor Trustwave, 90% of the vulnerabilities commonly found in desktop computers also exist in mobile devices. Distributed denial of service (DDoS) and malware infection are the common threats, no matter how the operating system studies indicate data breaches and security.

IT consumerization emphasizes the need for BYOD policy development. Employees start using their laptops and smartphones to complete business tasks. BYOD strategies can help control their use and reduce security risks.

1.1 Problem Statement

BYOD policy brings lots of security issues like virus malware infection in organization network, risk of confidential data leaks, data loss & data manipulation and challenges to availability of resources like distributed denial of service (DDOS) attack plus there has to be extra effort for IT management for protecting organization data from all kinds of cyber threats (Penny, 2017).

1.2 Purpose of the Study

The purpose of the study is to find the appropriate Information Security Management system that can protect an organization from all kinds of cyber threats that comes up during the adoption of BYOD policy.

1.3 Objective of the study

- To investigate the types of devices that people can bring in an organization and risks that devices can pose against data security in organization.
- Study of Impact of cyber threats that organization has to face with adoption of BYOD policy.
- To suggest a Security Framework that can control risks and threats that BYOD brings and find appropriate Information Security Management complaint for an organization.

1.4 Research Questions

- Which type of employee devices can be allowed in an organization with BYOD policy?
- Which types of risk and vulnerabilities that employee devices can bring into an organization?
- Is there any association between perception of devices brought with employees and real risks?
- Is BYOD policy beneficial for an organization in terms of comfort, productivity and investment cost?
- Is a robust security frame a solution of problems that BYOD devices bring?

1.5 Significance of the Study

The study shows how organization data is prone to cyber threats, how personally owned devices exploit security risks and create threats to organization data security. As BYOD policy is growing popular and organization cannot stop employee using personal devices for doing official work, the study investigates the security management framework that can fulfil the requirement of protecting organization data complying confidentiality, Integrity and Availability.

1.6 Scope of the Study

The focus of the study is to find the robust Information Security Framework that helps organization to allow employee to work with own devices inside, analyse different types of cyber threats that employee devices can bring and implement security policies & compliances for protection of crucial data, network resources, critical data, preventing data loss, and protecting organization from cyber-attacks.

The limitation of the study is. it only convers IT security threats that BYOD brings like malware, denial of service (DOS), distribute denial of server (DDOS), data breaches, data loss to an organization but cannot say more about other kind of IT risks like social engineering, phishing, hacking, man in the middle (MIM).

2. LITERATURE REVIEW

2.1. Introduction

The objective of literature review is to write critical summary of the published related article, journal, research paper of the topic BYOD policy, risks and security framework. Articles about BYOD policy, threats & vulnerabilities, cyber security, security management, implementation strategy published by authors have to be studied and relevant information are phrased with citations.

2.2. BYOD & Threats

2.2.1. History of BYOD

First company that introduced BYOD concept in 2009 is Intel, when management began encouraging employees to bring their own devices and allow them to connect to the corporate network. Intel's example is accepted by other technology companies like Citrix, Unisys, and IBM Systems. This concept is widely implemented globally and has the highest adoption rate in developing countries (N.M, 2015).

At first, business owners like BYOD because it reduces investment costs, and secondly employees like to work on their own devices, which is more efficient when employees are free to work on their own computers. But today experts have discovered security risks and data ownership issues.

2.2.2. Threats

In BYOD policy employee can bring in laptops, smartphones, tablets and storage devices in an organization to work. The policy favors freedom, comfort, and confidence of employee such

that they can work with more comfort resulting creating and increase in productivity. Employee devices like Laptop, Smartphones, Tablets and other storages can bring lots of problems. Devices can be infected with virus and malwares. When such device accesses organizations network and data cyber threats like slowing down of laptops, smartphones and network can occur. Denial of service attack can trigger unavailability of resources, network congestion, and bottle necks. Unauthorized access to resources with employee device can create problems of data breaches and data loss.

2.3. Related Works

Literature review of related topic of research papers, journals, articles are presented for analysis of problem and meeting the objective of the research.

2.3.1. Analysis of Security Controls for BYOD

Rivera D & et al, 2014 explains the impact of bringing their own devices (BYOD) into organizational security in their research papers. It investigates the major risks and security measures published in research articles. This paper also finds important areas in which organizations apply security controls to minimise security risks associated with BYOD. It also analyses the major risks and shows how to apply existing security mechanisms. The search bases used are BYOD, Security Control, NAC, MDM, MAM, Virtualization, and Access Control (Rivera, 2014).

By downloading organizational data to user owned devices, BYOD extends the security risk of the organization. The fact that various devices lack sufficient security controls in these devices and when the devices share information also increases the strength of the problem. This has led to an impulse to assess the effectiveness of existing security audit, control and information management policies.

In BYOD personal mobile devices are easily attacked by malware from infected websites and illegal applications. Threats from BYOD are categorized as direct threats such as device loss/stolen and indirect threats like eavesdropping in insecure wireless networks, malware attacks and location tracking (Markelj and Bernik, 2014) (Markelj, 2014).

Given the increasing number of threats caused by BYOD, organizations have to re-evaluate the usefulness of the security framework in multiple factors, such as risk, control, policy, security culture, and in awareness & training. The follow-up part of this review highlights on security controls.

According to NIST, security controls are defined as “management, operational and technical protections or countermeasures for information systems to safeguard the confidentiality, integrity and availability of systems and their information” (NIST, 2013).

This analysis points out 5 different aspects of security control related to BYOD:

• **Control Data** - By restricting data that employees can copy to their devices by restricting data at the source and/or using an effective delivery mechanism.

• **Control Access** - Update existing access control mechanism to account for contextual factors such as risk and trust level.

• **Control Network** - Manage your network effectively by monitoring employee devices connected to its resources.

• **Manage devices** - Better manage user devices themselves with identity management, data processing and remote access.

• **Create support frameworks** - controls such as policies, user training and training.

2.3.2. Introducing BYOD in an organization: The risk and customer services viewpoints

According to Zoran.M et al., in 2014, with the latest advances in technology and the quick spread of smartphones and tablets, as employees to do various tasks in the workplace using their personal devices is very common. Allowing employees to use their own preferred devices in the workplace also presents risks that are often associated with loss of control over organizational data. The study aims to identify and assess the risk of introducing BYOD in ICT organizations (Zoran, 2014). The case study approach led to the introduction of hybrid measures for the adoption of BYOD: technologies (such as mobile device management - MDM) and non-technologies (IT management policies).

According to the article, the most important benefits of BYOD are: i) mobility, ii) mobile individuals, iii) mobile environments, iv) mobile technologies, v) mobile devices, vi) mobile computing and vii) IT consumerization.

The authors agree that the three most common BYOD risks are:

• Data leakage refers to confidential work-related data that is typically stored on employee-owned devices, and can result in the disclosure of large amounts of confidential data, such as customer information and business secrets (Morrow, 2012).

• The difficulty of equipment management refers to the "ownership" concern and is seen as the basis for this difficulty. There are fewer options to reducing the security of unmanaged devices - simply because of poor management and poor visibility (Morrow 2012).

• Portability and device loss are related to the fact that many mobile devices are very small and portable, but the size can cause the devices used by BYOD and the data stored on them to be lost (Morrow 2012).

The reviewed literature (Kautish et al, 2008, 2012, 2013, 2020) suggested at least five measures for achieving secure use of BYOD in an organization:

(i) Application security: Protection of employee device from malicious applications
(ii) Employee education: Aware employee about information security, risk of BYOD and protection of confidential data.
(iii) Security policies: Policies for securing organization resources.
(iv) Security culture: Practice of security habit in employee.
(v) Mobile Device Management (MDM): For configuration, management and monitoring of mobile devices, and remote wipe of data in case if device is lost.

According to Mikale (McCann, 2013) small business that wants to fulfill customer needs must be part of their daily lives through blogging, social media, local event, and this require agility and responsiveness. Anomah et al. (2013) state that BYOD is supporting businesses to reach objective such as high productivity, efficiency and customer value through rich media applications like voice integration, instant messaging, video and communication with customers by staff and employees on real time basis. Some researches emphasize that business needs to adapt to new ways of using technology and digital lifestyle driven by the "consumerization" of ICT and the usage of personal devices into normal service processes of the business (Faulkner, 2013).

Figure 1: BYOD Security (Faulkner, 2013).

2.3.3. Mitigating BYOD Information Security Risks

As technology becomes more prevalent, the use of personal mobile devices in organizational work is also increasing. Especially, the need for employees use own equipment to do organizational work in the workplace is the factor behind the organization's use of Bring Your Own Device (BYOD) approach. When BYOD is allowed, employees can have access to organizational data assets on employee devices (Astani et al., 2013).

Users can increase productivity and access organization resources from within and outside the office, and organizations can reduce the cost by not providing devices to employees (Donaldson, 2015). However, this easiness presents organizations with the challenge of implementing security practices on private devices (Zahadat, 2015).

The table summarizes the 13 BYOD risks in studies related to allowing BYOD to enter the organization. In addition, in order to know the most important risks, they are divided into three categories related to the use of BYOD: user activity risk, connectivity risk, and organizational practices. This section will discuss each risk in turn.

Table 1: Assessment of risks associated with allowing BYOD (Arregui & Maynard)

User Behaviour			
R1:	BYOD Device Choice	**R 5:**	Unauthorised Access
R 2:	BYOD Customize	**R6:**	Exposure of Data
R 3:	Infected Applications	**R7:**	Lost BYOD Devices
R4:	Insecure Operational Behaviour	**R8:**	Data tampering
Connectivity			
R9:	Public Netwoks	**R11:** Personal Networks	
R10:	Local Network		
BYOD Management Practices			
R12:	BYOD Remote Access	**R13:**	BYOD Awareness

In this study, the BYOD strategy was evaluated on the basis of a comprehensive list of security risks associated with allowing BYOD to enter the organization. The assessment aims to find statements in the BYOD strategy to control information security risks in the organization.

2.3.4. Bring Your Own Device (BYOD): A Survey of Threat and Security Management Models.

According to Zambrano and Rafael, BYOD has potential benefits for both employees and business owners (G., 2019). The "bring your own device" phenomenon means that employees, business partners and customers are increasingly using application access information on devices that are not owned or controlled by the organization, resulting in data breaches, data theft and compliance risks (Morrow, 2012).

Companies implementing BYOD face similar risks that occur on desktop computers, but have been improved to exploit the vulnerabilities and weakness of mobile devices; another threat affecting mobile devices is guided and persistent attacks. Not initiated by random or large crowds, on the contrary, for specific devices.

By studying the papers on BYOD, you can answer the following questions:

- Discovered the following threats: Advanced Persistent Threat (ATP), malware infection, operating system fragmentation, social engineering, theft or loss of device, app store, fake security certificate, policy and BYOD law.
- Twelve security models were discovered in the BYOD environment, 11 of which are based on technology management of mobile devices and their connections. Only the BYOD policy management model has a human-oriented feature.
- According to the reviewed literature, no model allows for full security management in a BYOD environment, as each security model is designed to manage some of the threats, but no complete model attempts to prevent the two mobile devices from being compromised i.e. technical and human factors.
- The basic controls that have to be included when designing a BYOD strategy are divided into organizational policy controls such as auditing equipment, features, security additions, employee profiles, acceptable usage policies, and control of mobile device user policies such as passwords, antivirus And anti-malware, sensitive data, lost or stolen devices, external memory card encryption, GPS lock. These controls are a starting point for designing a specific BYOD strategy for any organization.
- There are 15 security features that depicts a complete mismatch between BYOD compliance and the ease of use of enterprise-owned mobile devices. Enterprise-owned mobile devices are easier to meet 11 features than BYOD. Most of the research on mobile security takes into account the traditional enterprise-owned device environment.

2.3.5. Legal Issues in Secure Implementation of BYOD

According to Dhingra, M. In 2015, the use of smartphones, tablets and laptops today has become an important part of the work routine of most organizations and companies. The organization is adopting a new policy that allows employees to use their devices in the workplace. Despite the cost and use benefits of BYOD, the policy poses serious security risks and negative impacts based on employee ethics, and there are also lack of protections in implementing corporate regulations. This paper examines the legal issues that may arise when implementing the BYOD policy and proposes solutions to overcome these occasional problems (Dhingra, 2015).

According to the document, there are some legal issues in maintaining and storing data, BYOD security, employee privacy, data breach response, remote wipe and corporate data security destruction. When the organization wants to fully controls the device and it has to mention

legal terms in the consent document. Maintaining data integrity (Rani and Kautish, 2018) (Kaur and & Kautish, 2019) is also difficult, and there is a possibility of data leakage due to the use of a memory card.

Companies must implement system configurations, encrypt data or investigate devices, monitor data usage to detect abuse or hacking, and perform other security tasks without problems, but employees may be reluctant to implement security policies to improve security.

Therefore, appropriate BYOD strategies and policies must be developed and organized by the organization to train and notify employees to overcome the above.

The investigation of personal devices is also a problem that affects while adoption of BYOD strategies in organizations. If you need to conduct any investigation to detect a security breach, you will also need personal information about the device. If the organization only sets rights on capturing company data, the actual investigation cannot be performed effectively. All the issues guide organizations to protect their employee details while keeping their security policies.

There are some difficulties in the incident response and investigation that directly affect security and privacy issues. Since the organization does not have personal devices, access to the device becomes issue if any security breach occurs. In the event of a violation, the organization will notify the person and conduct a risk assessment to identify potential data loss.

The consequences of employee blockage must be notified in advance; the data caused by the application being installed on its own device is erased. All of these clauses must be mentioned in the documentation for the Personal Equipment Use Policy.

One such solution is to remotely wipe or reset employees' devices using remote mobile device tools. These tools can remotely delete data. The terms of employment document must include this clause so that the device can be reset without his or her permission when needed.

2.3.6. BYOD with Security

According to Neves & Mello, the company's concerns about protecting sensitive data from unauthorized usage and data leakage have increased a lot. The company's ongoing case of cyberattacks and data loss demonstrates the need for strict information security policies to improve data security and allow audit trails. With the development of technology, the use of personal mobile devices has increased in the organization allowing employees to use their mobile devices at work.

This article discusses the recent challenges IT companies are facing and in protection of access to confidential data, as well as strategies for mitigating, tracking, and reducing data misuse in organizations. With this in mind, a good information security practice framework based on ISO 27002:2005 and the actual control of the Internet Security Center (CIS) were proposed to link good practices to the needs of the BYOD culture. The framework presented in this paper emphasizes the need for standardization of information security rules in the adoption of BYOD.

ISO 27002:2005 defines a classification of information that is critical to ensuring information protection in an enterprise environment. According to ISO 27002:2005, it is recommended to use an information classification system in conjunction with a data classification strategy to determine the category to which the information belongs and to determine which strategy will be used to ensure the protection of this information (Zahadat, 2018).

According to ISO 27002:2005, the classification of this information must be updated regularly and the protection policy for this data must be revised according to the rules defined in the

organization (27002, 2013). CIS states that it is important for companies to understand the definition of sensitive information and the importance of access level classification. Based on this classification, when an unauthorized or leaked person accesses this information, the impact on the business is analysed. CIS reports that after information classification, companies must use logical and physical protection in information security. Network isolation, firewall access control, and network access are available as protection.

3. RESEARCH METHODOLOGY

3.1. Introduction

Research methodology is an important part of research and helps to find results from data analysis. Research methods are an important tool for identifying problems, need to be explored, and set goals in research (Mohamed Al Kilani, 2016). According to (Solms, n.d.), research methods play a crucial role in ensuring the quality of research and finding whether the results are reasonably integrated with each other.

The main objective of the research method is to clearly understand the method or process to be used and to discuss the research problem in order to solve it. It can define ways to collect and analyse data using tools to meet goals and achieve results.

3.2. Research Framework

The conceptual framework represents a combination of literature reviews. Through the observation of the research topic, it draws the actions, policy framework research and risk mitigation process required in the risk assessment research process.

According to McGaghie et al. (2001), the conceptual framework is a “set-up phase” that presents a set of research questions that pushes investigations on the basis of problem statements. The problem statement describes the background and problems of the researcher's research (Mcgaghie, 2001).

Based on this topic, a questionnaire was prepared covering the types of BYOD devices allowed in the organization, the risks and threats that the devices can bring, and the security measures to be followed when implementing BYOD policies in accordance with information security standards and guidelines. The research framework is based on a questionnaire survey.

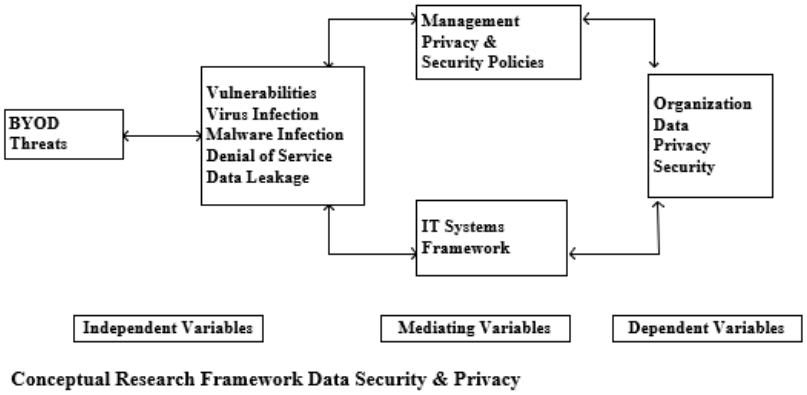

Figure 2: Conceptual Research Framework Data Security & Privacy

The data obtained from Questionnaire method of data collection is categorized into three variables:

3.2.1. Independent Variables

In this study of BYOD Independent Variables can be defined as employee devices and risks that is brought by this device like DDOS, malware virus infection, data leakage are security challenges. So, devices like laptops, smartphone, tablets, storage devices can bring lots of threats like virus malware infection, denial of service, data leakage, loss are independent variables.

3.2.2. Mediating Variables

Security frameworks like network access control, identity access management, mobile device management, mobile application management, data encryption, virtualization, and compliance with ISO/IEC 27000, NIST, COBIT and other information security management systems are being mediated to help the variables that protect organizational data come from all external threats from BYOD devices.

3.2.3. Depending Variables

Organizational data privacy and security i.e. prevention of data from theft, data tampering is depending variables, it depends on type of security framework and policy used while adopting BYOD.

Table 2: Description of Research Framework Construct

Construct Name	**Description**
BYOD Threats	Outside threats or risk that can enter Organization with employee devices e.g. laptops, smartphones, tablets, storages etc.
Vulnerabilities	Virus - Malware Infection, DoS attack. Data leakage
Management Policies	Development of management policies regarding issues.
Privacy Policies	Development of policy for privacy of data.
Security Policies	Development of policy for data loss and tamper.
IT Systems & Framework	IT infrastructures, technologies for Data protection
Data	Storage media infrastructure
Integrity	Assurance that data is not tampered or corrupted
Confidentiality	Ensuring data privacy from Unauthorized access, Identity access management

3.3. Research Design

According to Creswell, John W. (2014), research design is a set of methods and procedures used to collect and analyse metrics for variables specified in research problem statements. The design defines the type of research (descriptive, correlation, semi-experimental, experimental, review, meta-analysis, etc.) and subtypes (case studies, hypotheses, research questions, independent and dependent variables, experimental design), if possible, data collection

methods and statistical data analysis plans. Research design is a framework made for finding answers to research questions (Creswell, 2014).

3.3.1. Data Collection

The data collection is another important part of the study, as the proper data has to be obtained from proper group

A. **The primary data is** collected from questionnaire and online survey. The IT professionals and employee from other organizations are requested to fill up the form. IT professionals can give correct information in relation to the topic, types of risk of implementing BYOD and technologies for security framework and policies.
B. **The secondary data** is collected from studying literature, articles, journal relating to the research topic and analysis of various factors to check and verify the result with the result received from interpretation of primary data.

To achieve effective and efficient search, keywords were combined to form key phrases which were used to the search. Some of the keywords include: BYOD, BYOD policy, Information security framework, BYOD strategies, IT Consumerization, ISMS, ISO/IEC, MDM, MIM, BYOD Threats, Mobile device management. A number of databases were searched using the search terms in order to arrive at relevant journals, articles and publications on the various topics. Some of the databases include ResearchGate, IEEE, ScienceDirect, Google Scholar and the internet generally.

3.3.2. Sampling

Sampling is one of the most important factors which determines the accuracy of your research/survey result. It is the method adopted to collect data relating to the research topic.

In this study both types of sampling method are used Simple Random Sampling and Stratified Sampling.

In **Simple Random Sampling**, IT and non-IT professional are allowed to participate in online survey and questionnaire fill up. Non-IT person give data of usage of IT technology, for example, how good is BYOD in organizations, how it can contribute to productivity, etc.

In **Stratified Sampling**, only IT professional are targeted to get desired data for research. For example, IT professional according to their age and designation can give data of IT technology, how risky to implement BYOD, what security policy and security frameworks have to adopted?

The primary data is collected from group of people with designations like IT manager, Security Officer, Systems & Network Administrator, IT Officer, Support Officer, Accounts Manager, Marketing Manager, Sales Manager, etc. IT professionals can contribute more concerning BYOD risks and security framework.

3.3.3. Data validation

Data validation is the process of ensuring that datasets are cleaned up to ensure they have the correct and useful quality. It uses technology to check the correctness, significance and security of the data before entering the SPSS system.

Data cleansing is the method of finding and deleting empty or inaccurate records from a dataset. It is an incomplete or irrelevant part of the data by, modifying, or deleting the original data.

3.4. Proposed Method

The research method is proposed in related to the topic, is qualitative as the data collected is non-numerical and it gathers opinions, perception, & practices of targeted people. It can be

also said descriptive, as it only describes about BYOD, risks involve and IT security frameworks and relation between them.

According to Bhatt Adi, in 2019, qualitative research methods were designed to reveal the behaviour and perception of the target group, in reference to a specific topic (Bhatt A., 2019). There are many different kinds of qualitative research methods, for example in-depth interviews, focus groups, ethnographic studies, content analysis, questionnaires, and commonly used case studies. Questionnaire survey, journal paper research and literature review are qualitative research methods. The result of the qualitative method is descriptive and the conclusion can be easily derived from the obtained data.

The investigation is also exploratory because its purpose is to find a suitable analytical security framework, while analysing the risks and threats posed by the BYOD strategy and affecting its resources and data security.

4. PRESENTATION AND DATA ANALYSIS

4.1. Introduction

The data obtained from online survey and questionnaire is collected in spreadsheet excel format. The missing values are checked, cleansed and validated. The SPSS software is used for analysis of data to find the result. The data is categorized into variables like Background Information (Gender, Age, Designation, Organization Size), perception towards BYOD, practice for BYOD.

4.1.1. Background Information

- Age Group
- Gender
- What is the size of your organization?
- What is your designation?
- Does your company have BYOD policy? Are personal devices allowed in your company?

4.1.2. Perception Response of Bring Your Own Device

- The use of personal device and official device can mix up your personal life and working life.
- It is a growing trend that employees want to work in organizations with their own device.
- Employees feel more comfortable and creative to work with their own devices.
- Do you think BYOD policy increases productivity and creativity of workers, by allowing to work from personal devices?
- Do you agree that BYOD reduces organizational investment in devices?
- Without BYOD policy, there is security risk to your organization.
- To what extent does BYOD related applications potentially generate risks.
- Regular update and patching of operating system of devices should be done as a security precaution.
- BYOD gives mobility to work, you can work from home, office and anywhere.
- BYOD can reduce operating cost of an organization, due to mobility of employees.

- BYOD programs reduces pressure on IT support teams.
- Without BYOD policy your corporate data is on risk of disclosure, do you agree?
- The benefits of BYOD concept outweigh its security risks.

4.1.3. Practice response towards BYOD

- What types of personal devices should be allowed in your office under BYOD policy?
- BYOD devices are managed properly by IT department.
- For what business purposes BYOD devices, be used in organizations.
- Do you agree that Mobile devices should be regularly monitored and controlled by your IT department?
- Implementation of security BYOD framework can make your organizations data safe.
- To what extent security measures can be adopted with BYOD for security of data.
- If BYOD device is lost, the best remedial action for data protection are:
- To which extend can IT department control BYOD devices?
- Do your company monitor usage of BYOD devices?
- If your device is lost organization can wipe your personal data for security reasons. Do you agree?
- Appropriate BYOD device retirement policy of an organization:
- Proper IT security regulation for adopting BYOD policy in an organization.

4.2. Data analysis

Data Analysis Software used in this study is SPSS (Statistical Package for Social Sciences).It was produced by SPSS Inc., and it was acquired by IBM in 2009. Later it was named as **IBM SPSS Statistics** after 2015. SPSS is a mostly used program for statistical analysis in social science (Foley, 2018).

In this study SPSS is used for following type of data statistics.

- Descriptive statistics: Cross tabulation, Frequencies, Descriptive
- Bivariate Statistics: Means, ANOVA, Correlation

4.3. Frequency Analysis

It is a part of descriptive statistics. In statistics, frequency is the number of times an something happens. Frequency Analysis is an important area of statistics that deals with the number of occurrences (frequency) and analyzes measures of central tendency, dispersion, percentiles, etc.

4.3.1. Frequency distribution of Age Group

Table 3: Frequency of Age Group Variable

AgeGroup

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	18	14.4	14.4	14.4
	26-33	25	20.0	20.0	34.4
	33-41	58	46.4	46.4	80.8
	42-49	20	16.0	16.0	96.8
	>=50	4	3.2	3.2	100.0
	Total	125	100.0	100.0	

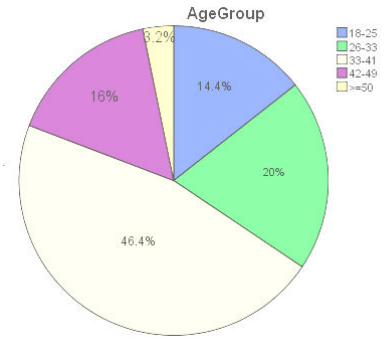

Figure 3: Pie Chart of Frequency of Age Group

Frequency Table and Pie Chart Diagram shows that 33-41 age group people are maximum respondents in Questionnaire i.e. 46.4% and 58 in numbers.
Age Group 33-41 people are experienced and well known in BYOD and Information Security.

4.3.2. Frequency distribution of Designation of Respondents

Table 4: Frequency of Designation

Designation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT Manager	30	24.0	24.0	24.0
	Security Officer	41	32.8	32.8	56.8
	Systems & Network Admin	27	21.6	21.6	78.4
	Support Officer	20	16.0	16.0	94.4
	Account Manager	2	1.6	1.6	96.0
	Sales Manager	2	1.6	1.6	97.6
	Marketing Manager	2	1.6	1.6	99.2
	Other	1	.8	.8	100.0
	Total	125	100.0	100.0	

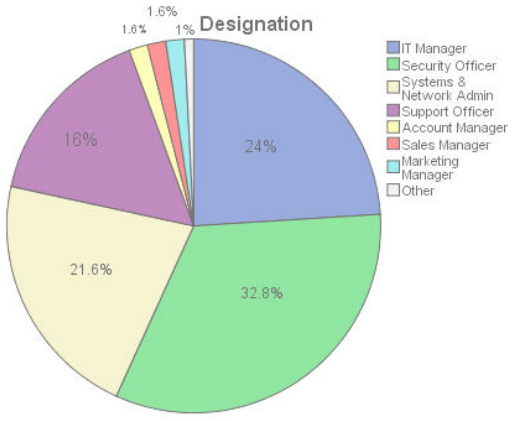

Figure 4: Pie chart of frequency of designation

Table and Pie Chart above shows that percentage of participants on the basis of designation is Security Officer i.e. 32.8%, secondly IT Manager i.e. 24%, thirdly Systems & Network Admin i.e. 21.6%. IT Manager and Security Officer is the most relevant designation regarding the topic of the study.

4.3.3. Trend of employee want to work with own device

Table 5: Frequency of respondent agreeing on growing trend of BYOD

A growing trend that employees want to work in organisations with their own device.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	81	64.8	64.8	64.8
	Agree	42	33.6	33.6	98.4
	Neutral	2	1.6	1.6	100.0
	Total	125	100.0	100.0	

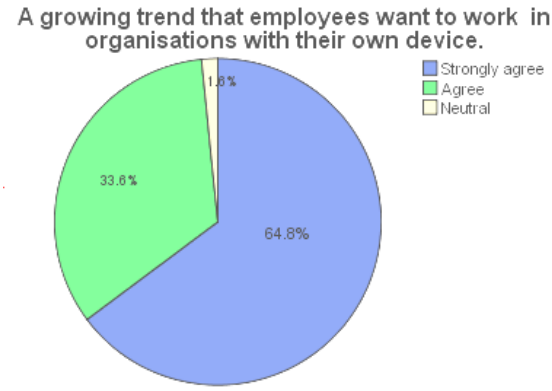

Figure 5: Pie chart of frequency of respondent agreeing trend of BYOD

Table and Pie chart above shows that respondents strongly agree 64.8% and agree 33.6% towards growing trend of BYOD in an organization. It means is a growing trend BYOD and it is unstoppable.

4.3.4. Employee's comfortability and creativity

Table 4.3.4: Frequency table showing employees feel comfortable with BYOD

Employees feel more comfortable and creative to work with their own devices.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	25	20.0	20.0	20.0
	Agree	97	77.6	77.6	97.6
	Neutral	2	1.6	1.6	99.2
	Disagree	1	.8	.8	100.0
	Total	125	100.0	100.0	

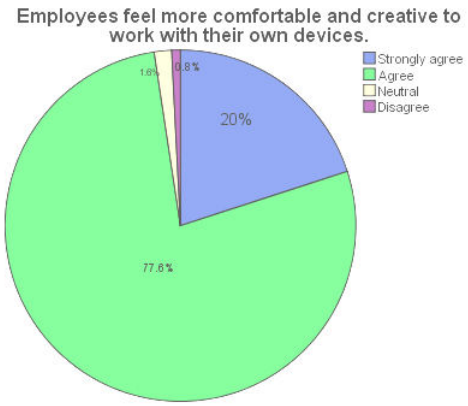

Figure 4.3.4: Pie chart showing respondent feel comfortable with BYOD

Table and Pie chart above shows 77.6% agree & 20% strongly agree that BYOD makes employee comfortable and creative in work.

5. CONCLUSION AND RECOMMENDATION

5.1. Introduction

The analysis of data shows that the robust security framework is needed while adoption of BYOD in Nepal. Without proper security framework it would be a hassle to manage issues and resources have to wasted managing them. There are standards of Information Security ISO/IEC 27000 services and NIST security guidelines for protection of assets of an organization. Security framework has to be developed in compliance with Information Security Management System like ISO/IEC, NIST.

The study shows that there is a gap that without a proper framework security framework an organization can allow employee devices to access resources. It would be difficult to manage the IT related issues if there are no specific guidelines and standards. Resources could be wasted if there is no specific policy and ultimately there is always fear of data leakage, data corruption and loss, and due to unmanaged circumstances, there can always be unavailability of services or resources.

5.2. Conclusion and Future recommendation

The result of the study reflects need of robust security framework while implementation of BYOD. The framework can be built in compliance with information Security standards ISO/IEC 27001 or NIST or CoBIT for privacy and integrity of corporate data from threats that comes along with employee owned devices (BYOD) in Nepal (27001, 2013).

The study shows that the following research objectives are met:

- To investigate the types of devices that people can bring in an organization and risks that devices can pose against data security in organization.

The types of devices that people can bring in an organization are mostly laptops, smartphones, tablets and rarely external storage like hard disks. The data shows that under BYOD policy, firstly laptop is brought respondent who strongly agree are 94.4%, secondly smartphones respondents who strongly agree are 77.6% and thirdly tablets respondents who strongly agree are 4%.

- Study of Impact of cyber threats that organization has to face with adoption of BYOD policy.
  An organization without robust security framework may have to face threats like virus, malware infection in corporate network from BYOD devices, there can be denial of service attack, hacking, phishing attack, social engineering from unwanted mobile apps installed in employees' personal devices. Unauthorized access to resources can result to data theft, confidential data leakage. The mobile devices can be lost, private data can be exposed to unauthorized people.
- To suggest a Security Framework that can control risks and threats that BYOD brings and find appropriate Information Security Management complaint for an organization.
  The ISO / IEC 27000 series is designed to help organizations of all sizes and types implement and operate information security. By using these standards, organizations can design and implement their own frameworks to manage the security of information assets. The ISO 27001 standard has strict requirements for BYOD, but BYOD is not mentioned in the ISO 27001 standard. However, organizations must use ISO 27001 to write their own security framework complaints. Despite of Risk associated with BYOD, there are many solutions available for managing it. The correct Framework, policy need to be tailored for using BYOD in organizations. Small as well as big organizations can take benefits of BYOD for employee comfort, creativity and increased productivity resulting in employee satisfaction and Information security.

5.3. Proposed Security Framework for BYOD

Organization wishing to adopt BYOD policy, have to follow a security framework standards and guidelines as provided in ISO/IEC 27000 or NIST, to protect corporate data from BYOD devices from, in and outside the organization. The proposed security framework for data protection is derived from KANYI Security frame work and ISO/IEC 27000 series and NIST standard & guidelines.

5.3.1. Security Framework is compliant with ISO/IEC 27000 Series

According to Kosutic Dejan, 2015, one can expect that ISO 27001 standard have strict requirements regarding BYOD (Dejan, 2015), but BYOD is not mentioned in ISO 27001 standard. However, an organization has to write its own security framework complaint with ISO 27001.
In the proposed framework, follow ISO 27001 controls:

Mobile Device Policy – This guideline can used to reduce risk, when developing a security policy for mobile devices. Therefore, the BYOD policy should be based on assessment of risks.

Remote Work - This guideline applies to employees' personal mobile devices as well as to the home. Control measures require employees to implement information access, handling and storage security measures when working in an external office.

Information Transmission Strategies and Procedures - This guideline needs documentation to protect data transmitted through any communicating equipment, also employees' mobile devices.

Electronic Information - Through this guideline, electronic information will be protected, which also applies to the BYOD policy.

5.3.2. Security Framework is compliant with NIST SP800-114 Rev. 1

According to Souppaya & Scarfone 2016, NIST has released user remote work and BYOD security guidelines. This document highlights specifically on the security of remote work and

involves remote access to organization network from home computing resources. It provides practical approach for protecting the operating system (OS) and apps of remote working computers and the home network used by computers. It provides basic advice for protecting mobile devices from remote work. This document provides guidance on securing information stored on remote work Pcs and external storage.
The document is divided into five main sections:

- Remote work and remote access overview and remote work device security introduction.
- A guide to protecting data stored on remote work devices.
- It is recommended to protect wired and wireless home networks for telecommuting.
- Discuss ways to protect BYOD personal computers (PCs) by updating software and installing and configuring anti-virus security and firewalls.
- Overview to protect the security of BYOD mobile devices.
- Introduce security considerations for third-party devices.

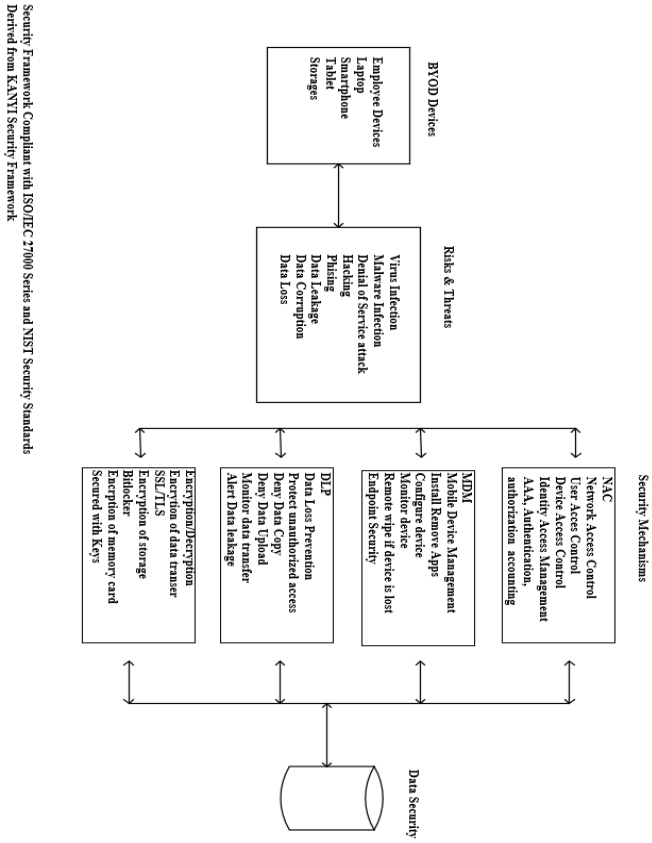

Figure 5.3: Proposed Security Frame work for BYOD

5.4. Security Framework Implementation Guidelines

1) BYOD devices

Identify devices used by employees, keep record of employee information, device login details, device name type details.

Employee devices are endpoint devices. Mobile devices like Laptop, Smartphones, Tablets have to protected with from virus malware infection and unwanted applications. Agent of antivirus, NAC, DLP, MDM, VPN are installed and registered in servers before allowing devices to be used by employee.

2) Identify and mitigate risks

Devices are configured with antivirus and malware infection protection. MDM installs corporate apps, protect devices from malicious app installation, monitor device. Unauthorized access to organization network is protected by NAC. Only registered users with policy-based authorization are allowed access in resources. Remote users, working remotely can access resources only through VPN, data is secured with SSL encryption.

3) Security Mechanisms:

Security framework for BYOD Policy should consists of:

NAC is a system for nodes to allow to access network resources on the basis of policy and set of protocols to ensure the security of data. VPN is for encrypted access to network resources. Identity Access Management, authentication, authorization and accounting are also managed by NAC system.

MDM (Mobile Device Management) is a kind of security system used by IT Units to control, configure, manage, and protect employee mobile devices and remotely wipe data when devices are lost.

DLP system is a strategy for making sure the BYOD devices are not sending confidential or critical data outside the organization network. The system protects organization from data leakage or data loss from copying or uploading data to external storages.

Encryption technology is used to protect confidential data at storage or data in transmission by implementing encryption such as ssl, tls, bitlocker etc. Data is encrypted with encryption algorithm so that lost data is unreadable and useless to others.

4) Data Security due to data redundancy technology like SAN, ISCI that has RAID implemented also keep data safe from corruption and loss due to hardware failure. Regular backup, and offsite backup also protects organization from disaster.

1.7 5.5 Future recommendation

BYOD is a growing trend that employee wants to work from their own device and organization cannot stop. It has become an inevitable and it is a part of IT consumerization. Tech Giants like SOPHOS, DELL, SYMANTEC & CITRIX have come up with efficient solutions for BYOD.

i**) Sophos Secure Endpoint Management system** is solution for managing end devices like windows 10 laptop, macOS, iOS phone, android phone relating to BYOD risk .Features like remote installation of apps, blacklist/whitelist of apps, inventory & access management, native OS containerization for secure email and documents, anti-phishing, malware, ransomware , PUAs , web protection web filtering are for endpoint BYOD devices (Sophos, 2019).

ii) **Dell W-Series ClearPass Access Management System** is a BYOD management system. It is designed to manage and protect wired, wireless and VPN access to virtually any network (Dell, 2019). ClearPass features include: BYOD devices provide secure network access and implement any network framework for centralized access to the entire network. Windows, Mac OS X PCs,

Android and iOS smart phones automatically configure enterprise-level endpoint protection and more health checks than standard network access control (NAC).

iii) **Symantec Data Loss prevention in BYOD environment**, Security Officers can manage BYOD ("Bring Your Own Device") policy while securing confidential data with Symantec DLP Mobile Email Monitor, which monitors corporate email being downloaded to the native mail app on company and employee-owned iPads and iPhones, and creates an inventory of confidential data being stored on them. It provides visibility into your mobile data loss risk and quickly pinpoints exposures if mobile devices are lost or stolen. Designed to support BYOD, Mobile Email Monitor does not require installation of any agents or apps on personal mobile devices (Park, 2014).

iv) **Citrix Xen MDM (Mobile Device Management)** is software designed to help IT administrators to control and secure mobile devices like smartphones and tablets used across an organization. IT departments use MDM server-agent connection to deploy and control apps on BYOD devices. MsDM allows IT admin, protects BYOD devices with device-wide encryption and automatically lock or wipe a device if it is lost or stolen (Citrix, 2019).

References

Bhatt A., 2019. Qualitative research: definition, types, methods and examples. [Online] Available at: https://www.questionpro.com/blog/qualitative-research-methods/. [Accessed 19 August 2019].

Citrix, 2019. Citrix Mobile Device Management. [Online] Available at: https://www.citrix.com/glossary/what-is-mobile-device-management-mdm.html [Accessed 19 August 2019].

Creswell, J. W., 2014. Research design: qualitative, quantitative, and mixed methods approaches (4th ed.). Thousand Oaks: SAGE Publications.

Dejan, K., 2015. How to write an easy-to-use BYOD policy complaint to ISO 27001? [Online] Available at: https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/ [Accessed 19 August 2019].

Dell, 2019. Dell W-Series ClearPass Access Management System. [Online] Available at: https://www.dell.com/en-us/work/shop/cty/dell-w-series-clearpass-access-management-system/spd/.powerconnect-w-clearpass. [Accessed 19 August 2019].

Dhingra, M., 2015. Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). International Conference on Information Security & Privacy (ICISP2015).

Donaldson, S. S. S. W. C. a. A., 2015. "Enterprise Cybersecurity Capabilities,". Enterprise Cybersecurity, pp. 01-311.

Faulkner, J., 2013. BYOD and Beyond - Implementing a unified access solution. [Online] Available at: http://h30458.www3.hp.com/media2.php/PDF/BYOD.pdf. [Accessed 11 August 2019].

Foley, B., 2018. What is SPSS? [Online] Available at: https://www.surveygizmo.com/resources/blog/what-is-spss/ [Accessed 19 August 2019].

Huffpost, 2016. BYOD in workplace, Benefits and Risks. [Online] Available at: https://www.huffpost.com/entry/byod-in-the-workplace-ben_b_10973342. [Accessed 16 July 2019].

Kaur, H. and Kautish, S., (2016). "An Implementation of Wireless Sensor Network Using Voronoi _PSO (Particle Swarm Optimization)", International Journal for Research in Applied

Science & Engineering Technology (IJRASET), Volume 4, Issue XI, November 2016, pp.361-368

Kautish,S. (2008), "Online Banking : A Paradigm Shift", E-Business, Vol. 8, No.10, pp. 5459.

Kautish S., Thapliyal M P, "Concept of Decision Support Systems in relation withKnowledge Management – Fundamentals, theories, frameworks and practices", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 1, Issue 2, October 2012 ISSN 2319 – 4847

Kautish S. 2013. Knowledge sharing: A contemporary review of literature in context to information systems designing. Academia 3(1). The South Asian Academic Research Journal: 101-113.

Kautish, S., & Thapliyal, M. P. (2013). Design of new architecture for model management systems using knowledge sharing concept. International Journal of Computer Applications, 62(11), 27–30.

Kumar, A., Rajpurohit, V.S. and Kautish, S., 2020. A Study on Technology-LED Solutions for Fruit Grading to Address Post- Harvest Handling Issues of Horticultural Crops. In Modern Techniques for Agricultural Disease Management and Crop Yield Prediction (pp. 203-221). IGI Global.

Kaur, R., & Kautish, S. (2019). Multimodal Sentiment Analysis: A Survey and Comparison. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 10(2), 38-58.

Leavitt, N., 2013. Today's mobile security requires a new approach. IEEE Computer Society, Volume 16-19, p. 46.

McCann, S. V., 2013. MetApp: an efficient and cost saving method for small businesses to create iOS applications. University of Texas, Electronic Theses and Dissertations.

Mcgaghie, W. &. B. G. &. A. J., 2001. Problem Statement, Conceptual Framework, and Research Question. Academic Medicine. 76. 923-924. 10.1097/00001888-200109000-00021.

Mohamed Al Kilani, V. 2., 2016. An Overview of Research Methodology in Information Systems (IS). Open Access Library Journal, pp. 3(2333-9721).

Morrow, B., 2012. BYOD security challenges: control and protect your most sensitive data. Network Security., Volume 8, p. 5.

Niraula, P. and Kautish, S., Study of The Digital Transformation Adoption in The Insurance Sector of Nepal. LBEF Research Journal of Science, Technology and Management, 1(1), pp.43-60.

NIST, 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise. [Online]
Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.
[Accessed 11 August 2019].

Device in SMMEs". IEEE.

Park, L., 2014. Symantec Data Loss Prevention: New Features Protect Against Insider Threats. [Online] Available at: https://www.symantec.com/connect/blogs/symantec-data-loss-prevention-new-features-protect-against-insider-threats. [Accessed 19 August 2019].

Penny, H., 2017. BYOD security: What are the risks and how can they be mitigated? [Online]
Available at: https://www.comparitech.com/blog/information-security/byod-security-risks/>.
[Accessed 16 August 2019].

Rani, S. and Kautish, S., 2018, June. Association Clustering and Time Series Based Data Mining in Continuous Data for Diabetes Prediction. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1209-1214). IEEE.

Rivera, D. G. G. P. P. M. S. &. K. S., 2014. Analysis of security controls for BYOD (Bring Your Own Device). Melbourne, The University of Melbourne.

Solms, J. F. v. N. a. R. v., n.d. Research Methodologies in Information Security Research: The Road Ahead. Research Methodologies in Information Security Research: The Road Ahead.

Sophos, 2019. Sophos Mobile. [Online] Available at: https://www.sophos.com/en-us/products/mobile-control.aspx [Accessed 19 August 2019].

Souppaya M., S. K., 2016. User's Guide to Telework and Bring Your Own Device (BYOD) Security. NIST Special Publication 800-114 Revision.

Techpublic, 2016. 10 Ways BYOD will evolve in 2016. [Online] Available at: https://www.techrepublic.com/blog/10-things/10-ways-byod-will-evolve-in-2016/ [Accessed 1 August 2019].

Wigmore, I., 2019. Bring Your Own Device (BYOD). [Online] Available at: https://whatis.techtarget.com/definition/BYOD-bring-your-own-device. [Accessed 11 August 2019].

Zahadat, N. B. P. B. T. &. O., 2015. "Byod Security Engineering: A Framework and Its Analysis,". Computers & Security, pp. 6-26.

Zoran, M. &. V. I. &. W. G. &. T. K., 2014. Introducing BYOD in an organisation: the risk and customer services viewpoints.