Characterising Risk Factors and Countermeasures for Risk Evaluation of Bring Your Own Device Strategy

Shefiu Olusegun Ganiyu*†, Rasheed Gbenga Jimoh**

* Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology Minna, P.M.B 65 Minna, Niger State
**Department of Computer Science, Faculty of Information and Communication Sciences, University of Ilorin, P.M.B 1515 Ilorin, Kwara State

†Tel: +234 806 160 1131, e-mail: shefiu.ganiyu@futminna.edu.ng

Abstract- Allowing employees to use their personal devices to perform official and private tasks through computing strategy known as bring your own device (BYOD) portends numerous benefits and security risks. The risks could propagate to enterprise information systems through some risk factors. Realistically, organisations anticipated the risks by implementing arrays of countermeasures. However, the characteristics that defined the relationships between the risk factors and the technical security controls are yet to be established. In order to evolve the features, this study conducted content analysis on some literatures which were selected through criteria developed for the research. Thereafter, the exploration revealed five characteristics that cut across risk factors, technical controls and the relationships between the former and the latter. Precisely, the derived characteristics are crucial toward achieving realistic risk evaluation process in BYOD strategy. Furthermore, the study opened more research directions as the risks circumscribing the strategy continue to emerge as global security challenge to vital information assets.

Keywords- Risk Factor; Countermeasure; Bring Your Own Device (BYOD); Risk Evaluation; Security Controls.

1. Introduction

Present day work environments are driven by several factors, among which is information pervasiveness. Bring your own device (BYOD) is a strategy that enables information pervasiveness by allowing employees to perform both official tasks and unofficial activities on their personal devices within and outside the enterprise perimeter [1][2][3]. The strategy fosters integration among business partners and interrelating enterprise processes, thereby leading to business convergence and agility [4][5]. Likewise, the pervasive nature of information through BYOD has continued to modify employees work life and productivity [6][7]. That is, workforces can process data and access information as at when needed through varieties of preferred personal devices and platforms. However, such flexible work environment often exposes vital organization resources to new security risks [8][9][10], such as data contamination and new patterns of mobile malware attacks [11].

Interestingly, every risk scenario is defined by set of factors which individually serves as source of risk or harm in particular situation [12]. Such risk factors or risk drivers are identified by risk professional as either internal or external factors [13]. In typical risk management task, risk factor could be attributed to several aspects including
technical [14], operational, environmental or policy [15] that surrounds a risky circumstance. For instance, [15] divided the risk factors for mobile access control into abstractions like authentication, location, timeout and condition. When risk factors are vividly identified, then envisaged threats and vulnerabilities relating to each factor could be anticipated and factored into risk assessment of computing environments like BYOD. Therefore, risk factor identification precedes other steps in risk management process [16].

Correspondingly, the main function of security control or countermeasure is to minimize the impact of security breach of confidentiality, integrity and availability (CIA) on information technology (IT) infrastructures and information assets [17]. These controls are in form of policy, technical tools or operational guidelines. Also, control could be classified as preventive, detective, or corrective depending on its role in addressing security challenges [18]. Thus, to mitigate threats inherent in IT, two or more controls are often stacked through a process known as layered security or defence in depth [19]. In line with this, consumerization of contemporary IT strategy like BYOD takes advantage of some existing controls to secure computing infrastructures and digital assets.

However, BYOD security challenges defied the capabilities of some traditional security measures due to peculiarities of its risk factors [20]. In line with this, innovative security mechanisms including mobile device management (MDM) and mobile application management (MAM) are becoming popular countermeasures in BYOD environment [11][21][22][23][24]. In addition to already available enterprise security solutions, research efforts are ongoing to curtail BYOD challenges through redesigned network [25], virtual solution with context switching [26], and prioritized defence deployment [27].

Risk evaluation is considered as subtask of entire risk management activity for quantifying or qualifying the consequence of hazardous operations through some risk metrics. In case of the former, the outcome of risk evaluation is monolithic value, whereas the latter expresses outcome in qualitative term. Irrespective of the nature of outcome, there is nothing like exact risk value [5]. Likewise, the ability of risk evaluation model to predict risk depends on risk factors [28] and available security controls [29][30].

Generally, before engaging in risk assessment of any domain, the list of risk factors and available security controls need to be defined and venerated [13][16]. This is to enable risk management team to understand risk pattern and to guide them in evaluating possible risk. In other words, knowing the sources of risks and available or missing controls will amongst others, assist the team to characterize potent threat sources, likely vulnerabilities and control effectiveness for use in risk evaluation process. Simply put, characterizing BYOD risk factors and controls is to identify components that could be exercised by attackers, relevant countermeasures and their possible combinations.

From the aforementioned, BYOD strategy as a global phenomenon brings some benefits to IT environments. On the contrary, it opens another frontier of security challenges [31][32], which could ultimately lead to loss of crucial information asset [33][34]. Unfortunately, security risk is receiving the least attention among present BYOD enrolee [9]. Therefore, there is need to address the challenges [32], possibly through risk assessment approach that takes characteristics of risk factors and differentiated security controls into consideration [35][36]. However, existing researches on risk factors and controls are yet to elicit the characteristics of BYOD collectively in term of relationships among the factors and countermeasures. This initial task is required to get off on the right foot with realistic risk management activities, such as risk estimation for BYOD [37].

Therefore, the aim of this paper is to evolve basic characteristics of risk factors and countermeasures for risk evaluation process of BYOD policy. To achieve the aim, existing literatures on BYOD strategy were consulted to uncover the risk factors and controls appertained to the strategy. The remainder of this paper is organized as follows. The next section presents a review of related literatures. Up next, the methodology section outlines the steps that guided the research. Lastly, the result, discussion and conclusion sections follow in that order.
2. Related Works

Being one of the relevant study in BYOD, [1] provided comprehensive guidance to organizations that intend to implement BYOD in areas like governance, control and strategies for mobility. Likewise [6] carried out brief survey on security models of BYOD from opposing perspectives namely, hands-off against hands-on devices. The author dwelled more on MDM and encryption as security controls for most security challenges. Similarly, [38] presented architectural perceptions and virtualization methods on the one side and MDM at the other to resolve BYOD security threats. In addition, [38] proposed a policy-based framework to manage risk relating to privacy and security of information in BYOD strategy. The framework utilized policy and controls that are similar to [1]. However, [1][6][38][39] did not include cloud, location and time as possible risk factors.

Also, in evolving BYOD security risk and controls, [8][40] reported network, mobile device and mobile application as risk factors and their security controls. Though, [8] conducted research on contemporary security challenges of BYOD with focus on malware threat agents and their possible solutions, whereas [40] proposed an architecture that allowed access to cloud service with BYOD.

Furthermore, [41] researched risk management quintet including users insights and user manners, controls, liabilities and adoption of BYOD. The research focused on security controls and discussed network and mobile device as risk factors. In related study, [22] examined both technical and nontechnical controls for BYOD, however, the former included controls for mobile device and applications. In addition, [11] listed the controls to mitigate risk from cloud-based file sharing, mobile device, mobile application and coexistence of personal and corporate data. Likewise, [37] identified potent risk factors for BYOD strategy using risk breakdown structure. In addition, the study identified working hour (time) as risk factor. However, only MDM was analysed as security countermeasure for all the risk factors identified in the study. This countermeasure is insufficient for BYOD security [24].

Similarly, [10] recognized network and lost (stolen) device as BYOD risk factors for small-medium and micro enterprises with their corresponding controls. The researchers fell short to provide countermeasures for other risk factors extracted from Control Objectives for Information and related Technology (COBIT), King III report (governance principles) and ISO 27002 (information security controls). Likewise, [42] developed enterprise secure centre as solution to security risk of mixing corporate and personal data on same mobile device. Apart from identifying location and network as risk factors, the researchers shared the same opinion with [32] that storage cards constitute risk sources for BYOD.

Again, [43] outlined MDM, application virtualization and desktop virtualization as possible countermeasures for some factors that increase the chances of risk in BYOD environment through literature review. The study also summarized the strength and weakness of the controls to aid security policy formulation for the environment. Though, the researcher elaborately discussed the security controls, there are still other countermeasures [1][10][42]. Also, the controls were not logically aligned to possible risk factors, because a control could mitigate threats to several factors. Such, alignment will assist security risk experts in understanding the relationships between risk factors, threats and controls.

The reviewed literatures predominantly covered different aspects of BYOD security through risk management techniques. Above all, each of them mentioned at least one risk factor and relevant security control. Thus, the review provided insight to what authors individually perceived to be risk factors and available countermeasures to minimize risk from the factors. Remarkably, no single literature captured all the prominent risk factors, their respective controls and interplay between the factors and controls. So, this section provided the baseline on which characteristics of BYOD risk factors and countermeasures were formed.

3. Methodology

This study employs document analysis which is guided by procedure depicted in Fig. 1 to unravel
the features of BYOD risk factors, security controls and their relationships. The analysis considered both academic and non-academic literatures for comprehensive coverage of the factors and controls. Actually, the decision to include the latter is premised on the fact that risk management in BYOD has enjoyed contributions from government regulatory guidelines and technical reports from IT vendors alike. The academic and non-academic literatures were classified as categories A and B respectively.

In order to retrieve literatures for category A, keywords like “BYOD security”, “BYOD risk control”, “BYOD risk”, “BYOD risk factor” were used on high impact academic databases including “IEEE”, “Science Direct”, “Springer”, “ACM” and others. Similarly, the same keywords were used to search the World Wide Web for documents in category B. The selection of documents for analysis from both categories were subjected to same selection criteria which were formulated before retrieving the documents as follows:

i. The author mentioned at least one risk factor and corresponding technical security control.

ii. The risk factor and control are primarily mentioned by the author of the article. That is, not cited as secondary source to avoid multiple entries.

iii. The literature should not be earlier than year 2010, this ensures recentness of risk factors and controls.

Prior to extracting the risk factors and controls from selected literatures, the assumption made was that the ultimate goal of any successful attack on risk factor will lead to data loss [1][6][44][45][46]. Therefore, data loss was not considered as risk factor. Also, the guideline stated below was derived to assist the extraction process:

i. Security controls are individually recorded for each risk control, even when multiple controls could mitigate a threat from risk associated with risk factor.

ii. The most popular name is chosen to represent a factor or control when authors differ on nomenclature.

iii. Related risk factors are grouped as sub-risk factor under a major factor.

4. Result

A total of 26 literatures comprising of 17 academic and 9 non-academic literatures, which met the selection criteria are shown in Table 1. Subsequently, the BYOD risk factors and security controls that were directly mentioned by authors of these literatures were analysed to understand the interplay between them.

**TABLE 1**
Analysed Documents for Risk Factors and Security Controls

<table>
<thead>
<tr>
<th>Category A</th>
<th>Category B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Type</td>
<td>Number</td>
</tr>
<tr>
<td>Journal</td>
<td>6</td>
</tr>
<tr>
<td>Conference Paper</td>
<td>11</td>
</tr>
<tr>
<td>Subtotal</td>
<td>17</td>
</tr>
<tr>
<td>Total = 26</td>
<td></td>
</tr>
</tbody>
</table>

4.1 Risk factors

The risk factors identified in the analysis and the number of authors who regarded them as such are described below and summarized in Table 2.

i. Mobile device: this means all portable devices the employee utilises for personal communication, entertainment, data storage and information processing. In addition, the staff uses same device to perform official activities. The device becomes likely source
of risk due to any of the following sub-risk factors:

a. Jail-broken or rooted device: user voids manufacturer security that prevents installation of unauthorised applications. The device that undergoes this process is known as jail-broken (iOS) or rooted (Android) device.

b. Stolen or lost device: the risk arising from stolen or misplaced device depends on the sophistry of the possessor of such demobilised device.

c. Coexistence of both personal or organisation data: this could give rise to illegal harvest or contamination of organisation data.

ii. Mobile application: mobile software including the enterprise developed or third-party applications (apps) and malware can be sources of risk leading to enterprise data loss [47][48].

a. Third-party applications: the vulnerabilities in legitimate apps that are developed by third-party, enterprise developed apps or downloaded from trusted online stores are not risk free [49].

b. Malware: some malicious apps are primarily developed to compromise CIA of enterprise information system [11].

iii. Network: data transfer in BYOD strategy takes place over different networks just like other computing environments. These networks which include Wi-Fi, Bluetooth, Cellular network, mobile telecommunication technology (3G or 4G) and the Internet at large have some loopholes that make them sources of risk [44].

iv. Cloud-based file sharing: several cloud-based file sharing platforms like Box, Egnyte, Dropbox and SugarSync offer file storage and synchronisation services to network enabled devices. These platforms which are not completely immune against security risks [50], are also utilised for BYOD leading to additional class of risk factor.

v. Work location or location of device: the risk of using device varies from one location to another [51], since IT crimes are also location dependent [52]. For example, the risk of using mobile device within physical environment of an organisation might be relatively lesser than when used in public places like train station or bus park.

vi. Time of access: accessing enterprise assets at certain time of the day or week could be a potential risk factor. Especially, when sensitive asset is accessed outside of employee planned work periods. More so, BYOD being a time independent strategy [45], will benefit from security controls built on time of access [53,54].

vii External storage card: losing possession of external storage card that contains organisation data could cause leakage of sensitive organisation data. Particularly, now that only few people care about safety of content on the card [42].

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Number of Times Mentioned by Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jailbroken Device</td>
<td>7</td>
</tr>
<tr>
<td>Stolen Device</td>
<td>21</td>
</tr>
<tr>
<td>Data Coexistence</td>
<td>11</td>
</tr>
<tr>
<td>Third-party App</td>
<td>15</td>
</tr>
<tr>
<td>Malware</td>
<td>14</td>
</tr>
<tr>
<td>Network</td>
<td>20</td>
</tr>
<tr>
<td>Cloud-based File Sharing</td>
<td>5</td>
</tr>
<tr>
<td>Work Location</td>
<td>5</td>
</tr>
<tr>
<td>Time</td>
<td>3</td>
</tr>
<tr>
<td>Storage Card</td>
<td>2</td>
</tr>
</tbody>
</table>

4.2 Technical security controls

The technical security controls extracted from the analysed literatures are explained below and summarized in Table 3.

i. Encryption: data encryption ensures safety of data, while at rest on mobile device and in transit between network endpoints using computational algorithms that turn plaintext to cyphertext. This control is a necessity for BYOD [41]. As a matter of fact, some data encrypted on particular storage medium of specific device will only decrypt when the medium is affix to the device [49].

ii. Firewall: it is traditional technical control which is still useful in BYOD for endpoints security [55]. To be effective in BYOD environment, a firewall should be able to block access to enterprise system using criteria such as nature of network, application type, network protocol and internet address [38].
iii. Global positioning system (GPS): almost all smart and portable devices are equipped with GPS facility [56] to give spatial and temporal information about the device [57]. This is a desirable countermeasure to assist in tracking of data, lost or stolen device in BYOD.

iv. Mobile application management (MAM): is to ensure security of data and applications on mobile device. Primarily, activities like updating, installing, patching, removing, whitelisting and blacklisting of apps are securely managed by MAM [47].

v. Mobile content management (MCM): in BYOD environment, the control offers fine grained access to data in storage media and those being shared through container that is secured by encryption [11]. One paramount feature of this control is the ability to lockdown access to data based on location through Geo-fencing [58].

vi. Mobile device management (MDM): this is a popular security control in BYOD environment with three basic functionalities namely; device management, security management and file synchronization [1]. It is used for enrolling, monitoring and configuring devices. Also, MDM assists IT security experts to monitor and manage data, operating systems and mobile apps installed on devices. In addition, it allows device tracking, remote data scrub and encryption as security features. In reality, specific implementations of these basic functions vary in scope and flexibility among MDM vendors [40]. Especially, the individual roles of MIM, MCM and MAM which are supposed to compliment MDM are now being incorporated into it by vendors to gain competitive edge. To this end, MDM is being advanced to a superior product called MobileIT [59].

vii. Mobile antivirus: high proliferations of mobile malware [60], necessitate the installation and regular update of antimalware on portable devices, particularly those partaking in BYOD. Basically, the roles of mobile antivirus are similar to the conventional antivirus developed for desktop computers and they include detection, quarantine and removal of malware.

viii. Secured container: this is otherwise known as sandboxing whereby data and application are placed in secured segment of mobile device participating in BYOD. Thus, access to the secured area is restricted to only authorised processes or programs. The control can be achieved by having right mix of MDM and MAM [51].

ix. Virtual environment: virtualisation is security control that prevents enterprise data and applications from residing permanently on device of user partaking in strategy that allows anytime and anywhere access to data [41][61]. Virtualised environment is a layered concept that can be achieved through any or combination of desktop virtualisation [62], application virtualisation and user virtualisation [63][64].

x. Virtual Private Network (VPN): it ensures integrity and confidentiality of data in transit by providing secure communication channel between enterprise system and mobile devices.

### TABLE 3

BYOD Control Measure Distribution

<table>
<thead>
<tr>
<th>Control Measure</th>
<th>Number of Times Mentioned by Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>26</td>
</tr>
<tr>
<td>Firewall</td>
<td>7</td>
</tr>
<tr>
<td>GPS</td>
<td>6</td>
</tr>
<tr>
<td>MAM</td>
<td>6</td>
</tr>
<tr>
<td>MCM</td>
<td>4</td>
</tr>
<tr>
<td>MDM</td>
<td>51</td>
</tr>
<tr>
<td>Mobile Antivirus</td>
<td>14</td>
</tr>
<tr>
<td>Secured Container</td>
<td>15</td>
</tr>
<tr>
<td>Virtualization</td>
<td>10</td>
</tr>
<tr>
<td>VPN Gateway</td>
<td>17</td>
</tr>
</tbody>
</table>

#### 4.3 Risk Factors and Controls

The information in Tables 2 and 3 were logically combined to derive the characteristics of BYOD risk factors and their corresponding controls as shown in Table 4. These relationships could easily be perceived as revealed in Fig. 2.
### TABLE 4
Risk Factors and Associated Controls

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Sub-risk Factor</th>
<th>Technical Security Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MDM</td>
<td>Firewall</td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stolen Device</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>Jailbroken/Rooted Device</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Personal and Organization Data Coexistence</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Storage Card</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mobile Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-party App</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Malware</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Cloud-based File Sharing</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Work Location</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Time</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>51</td>
<td>7</td>
</tr>
</tbody>
</table>

Fig. 2. Characterisation of BYOD security controls and risk factors.
5. Discussion

Unlike other initiatives in computing environment, network security control for BYOD strategy does not depend on router as core countermeasure. Surprisingly, not a single mention was made of router as specific security control for any risk factor. Rather, VPN gateway, encryption and firewall were prominent lines of defence for network related challenges. The alliance between VPN and encryption is plausible because VPN is dependent on encryption.

Obviously, MDM and encryption schemes remain significant tools to control security challenges arising from loss/stolen device in BYOD. In addition, the capability of MDM to remotely monitor or manage device could be strengthened when it is combined with GPS features. For instance, remote data wipe, device locking, device-level data encryption, device location monitoring could be easily achieved when the four controls are individually integrated into single solution.

From the document analysis, MDM or GPS appears to be the only control for jailbroken/rooted device and monitoring device location respectively. The case of location (risk factor) is surprising, because as context-awareness is becoming popular in information pervasive arena, only few authors mentioned location as risk factor. Similarly, mobile antivirus is the predominant countermeasure for malware, though MDM, MCM and secured container also play slight roles. Likewise, possible risk relating to time and external storage card could only be mitigated by MDM and encryption respectively. This indicates that at the moment, some risk factors have only one major control to address their security challenges.

Also, risk factors could be discerned based on their applicable controls irrespective of similarities among the factors. Really, malware and third-party apps are software inclined and could be exercise by same or similar threat. But MDM, secured container and virtualizations were revealed to be appropriate controls for third-party app whereas mobile antivirus remains the main control against malware. Likewise, cloud-based file sharing and coexistence of personal and organization data are concerned about data security, however, both do not share same controls.

Another point to note is that, a single control could assume many roles. Depending on the scenario at hand, the role might be preventive, detective or corrective. Typically, MDM is found to perform multiple roles in BYOD security landscape, but its roles can be classified after painstaking analyses by experts. Thus, considering the risk factors and controls discussed so far, the characteristics of BYOD strategy can be outlined as:

i. Multiple risk factors may be considered for a given risk management scenario.
ii. Security controls differ in terms of efficacy to risk mitigation.
iii. Multiple controls are sometimes assembled to address loophole in a risk factor.
iv. Different risk factors including those belonging to same major factor might require differing controls.
v. Control can operate in specific modes, i.e. preventive or corrective, or detective.

6. Conclusion and Future Works

Depicting the sources of risk and the available countermeasures to allay security threat in BYOD strategy is a basic requirement to achieve realistic evaluation of possible risk in the strategy. Apparently, the risk factors that defined BYOD as pervasive computing comprised both mundane and those specific to the computing stratagem. Due to vulnerabilities in BYOD tools and supporting IT infrastructures, novel security controls are being deployed to complement existing countermeasures. In addition, single or multiple controls with varying efficiency are often stacked to secure corporate data from risks alluded to BYOD environment. Likewise, it is possible for a countermeasure to address multiple security challenges or performs preventive, detective or corrective role in BYOD security framework.

No doubt, the nature of risk factors, the types and features of pertinent security apparatus and the relationships between the former and the latter as revealed by this study defined the characteristics of BYOD strategy. In the strategy, the characteristics are significant for some facets of security risk management and initiatives. For instance, we intend to use the characteristics to select risk
evaluation model for BYOD strategy in our future research. Also, upcoming studies need to provide answers to why location and time were sparingly mentioned as risk factors by authors. The two factors have security implications to “anywhere” and “anytime” concepts of BYOD environment.

References


