A Policy-Based Framework for Managing Information Security and Privacy Risks in BYOD Environments

Abubakar Bello Garba[1], Jocelyn Armarego[2] , David Murray[3]

[1, 2 & 3] Murdoch University, School of Engineering and Information Technology,
90 South Street, Murdoch WA 6150, Australia

Abstract

In a world where consumerisation of IT has driven individuals to acquire and use the latest technologies, an influx of employee personally owned devices has populated corporate environments. This phenomenon is known as Bring Your Own Device (BYOD). Managing organisational information resources has become increasingly complex with the concept of BYOD. Despite the perceived benefits of work flexibility, increased productivity, and efficiency of employees, BYOD raises many concerns relating to information security and privacy that can lead to confidential information loss. This prompts the demand for effective mobile device management tools, policies, standards and procedures. With most BYOD solutions failing to meet the requirement for holistic management of BYOD, this paper proposes a policy-based solution framework that organisations can adopt to achieve information security and privacy in BYOD environments.

Keywords: BYOD policies, security, privacy, risk management

1. INTRODUCTION

The adoption and usage of BYOD devices in the work place have become practices allowed by many organisations [1]. Employees walk in with their smartphones, tablet PCs, laptops, and other personally owned devices, possibly unaware or insensitive to the security and privacy risks they pose to their organisations and to their own personal data. While considerable evidence suggests that BYOD can offer the benefits of work flexibility, increased productivity and efficiency [2]-[3], the risks of confidential information loss may outweigh these benefits if BYOD security and privacy are ineffectively managed [4].

The goal of information security is to provide confidentiality, integrity and availability [5]. Likewise, the aim of privacy is to ensure confidentiality [6]. These can ideally be achieved if BYOD devices were confined to one area, within organisational control. However, the high mobility of BYOD devices, which are not controlled by the organisation, challenges information security and privacy, making their maintenance a complex and difficult task.

To enforce confidentiality of information means restricting access to information to only those authorised [7]. As BYOD users travel outside their work environment, they may use open wireless connections which tends not to be implemented for optimum security and privacy. Their open nature means they are not, or cannot be, secured or alternatively could be compromised, causing BYOD users to infect their organisational resources when connecting through that channel in order to work. Man-in-the-middle attacks could also be launched via such connections to capture unencrypted data. In addition, even when BYOD users use their own mobile data, the transfer of data from their devices might not always be encrypted because some of the applications in use can transmit data through unsecured channels. Although BYOD devices may have been authenticated and authorised before accessing organisational resources, malicious apps could also be doing so without BYOD users' knowledge, sending data to unauthorised locations or persons. Besides, not all BYOD users have knowledge that their personal data is transmitted or collected [4], let alone being aware of any privacy settings for its prevention. The probability for BYOD devices to get lost or stolen is also high, and devices that use unencrypted memory cards and default passwords can easily become accessible.

The failure to achieve confidentiality of information in BYOD environments is a failure in achieving integrity. If confidentiality of information is broken in BYOD, it will not take much for integrity (authenticity, accuracy, and trustworthiness) of information to be compromised. Also, achieving availability of information in BYOD means increasing the ability to access information resources as and when needed. This involves extending information access to users outside organisational control, and any restriction on this might reduce productivity and efficiency in BYOD practices.

Establishing how effective information security and privacy can be achieved in BYOD environments requires the identification of the key issues in those environments, and understanding how BYOD influences the current organisational values and practices in relation to information security and privacy management. Measures and controls for eliminating or reducing risks to organisational and personal information resources in BYOD also need to be explored, together with the best common practices for attaining successful information systems management.

An investigation of the information security and privacy risks inherent to BYOD indicated that BYOD can impact organisational resources and assets such as networks and applications, and also, at the user-end, the mobile devices themselves [8]-[9]. To complicate things further, BYOD can also stimulate litigation and liability issues. A study which examined and analysed BYOD practices, usage patterns, perceptions and behaviour in organisations showed that there are many risks associated with BYOD in the areas of physical threats, access control, communications and applications, and compliance [10]. Further evidence from this study suggests that most organisations either do not fully understand the engineering behind BYOD, or are unaware of its potential impact on confidential information resources. Organisations lacked adequate knowledge of how to implement appropriate controls and strike a proper balance between security and privacy to minimise user experience deficiencies. Additionally, many organisations applied only technical controls to manage BYOD, disregarding non-technical controls like policies and procedures.

Since many of the current mechanisms or approaches that protect information in BYOD environments are sacrificing or exposing confidential data, and destroying user experiences [8]-[11], there is increasing concern at the lack of availability of adequate and effective policies, standards and procedures for BYOD [12]-[13]. This highlights the requirement for effective solutions to manage BYOD.

This paper introduces a policy-based model that aims to strike a balance between security and privacy management of BYOD in organisations. The paper reports on current best practices to survive BYOD adoption, and contributes to building a framework for BYOD management within corporate environments

2. TOWARDS A BYOD SECURITY AND PRIVACY MANAGEMENT FRAMEWORK

BYOD spans many functional areas within an organisation, involving human resources, legal, IT, finance and operations [1]-[6]. Hence, BYOD challenges can be approached from multiple perspectives inclusive of organisational and technical. These provide several control dimensions for BYOD that relate to controlling data, controlling access, controlling networks, and managing devices, as well as creating explicit policies and procedures [14]-[15]. While many vendor-based technical solutions to manage BYOD exist, explicit policies and procedures that address security and privacy to support these technical solutions do not [16]-[11]. The implementation of explicit information security and privacy policies is a key control required in BYOD environments, because it can also incorporate or support the other control dimensions for BYOD [10].

However, before developing and enforcing BYOD policies, several issues need to be considered relating to: legal and liability aspects; the procedures and technical control measures needed to be employed; the impact of controls over BYOD users; the psychological impact of BYOD policy on users with regards to their behaviour and acceptance of the policy controls [17]-[10]. To address these issues, a proposed BYOD policy-based management model which recommends six control components, should be considered:

- Information security standards and procedures
- Information privacy principles
- Information security and privacy technical controls
- Liabilities
- Awareness and training program
- BYOD user perception and behaviour.

These components are selected based on indications from information security and privacy theories [18]-[19] that they are important when trying to achieve a high level of data protection in organisations. Figure 1 depicts the BYOD policy-based management model, which examines each component to identify suitable control measures that can be included in BYOD policies. A cross analysis of the relationships between the components is undertaken to strike a balance between security and privacy, so as to identify control measures that will not affect the BYOD experience of organisations and employees.

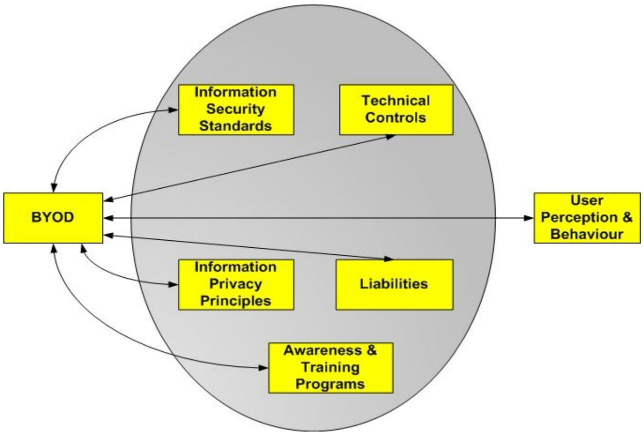
Information Security Standards
Technical Controls
BYOD
User Perception & Behaviour
Information Privacy Principles
Liabilities
Awareness & Training Programs

Figure 1 BYOD policy-based management model

21.Adapting information security standards for BYOD

Information security standards ensure that a sufficient level of information security is achieved, and the best security practices are adopted and implemented in an organisation. When dealing with BYOD, information security standards can help organisations implement effective security control mechanisms to ensure the confidentiality and integrity of information. There are different types of information security standards that can be applied by organisations to manage threats and vulnerabilities in BYOD environments. These include ISO 27000 series standards [20], COBIT [21], SOGP [22], and ITIL [23].

2.2Adapting information privacy principles for BYOD

Information privacy principles comprise guidelines and procedures on how to protect private and confidential information. These principles can also control privacy breaches and exposure of individual and organisational personal information in BYOD environments. There are several types of information privacy principles that are internationally recognised and accepted. Among them is the Organisation for Economic Co-operation and Development (OECD) privacy principles [24], which have been the foundation for creating privacy programs to tackle confidentiality problems related to information technology usage. The OECD has eight principles which all could be used as a stepping stone by organisations to ensure the confidentiality of corporate information on BYOD devices, and the confidentiality of BYOD employees' personal information.

2.3Adapting information security and privacy technical controls for BYOD

Organisations adopting BYOD consider technical controls to leverage the risks and reduce the likelihood for legal and liability issues in BYOD practices [11]. Organisations must ensure that any controls enforced or used to manage BYOD, do not violate important regulations or law. The implementations of technical controls to cope with BYOD risks can have specific impacts on BYOD users' experience.

The most common technical control mechanisms used by organisations for BYOD are full mobile device management solution systems, which are found to be intrusive and give too much control to organisations [14]. However, the evaluation of BYOD management solutions [8] indicated that some approaches that involve network, virtualisation, and phone-centric such as containerisation, Virtual Private Network (VPN), data encryption, access control, and the remote wiping of devices, can be implemented in a tactical manner to manage BYOD.

2.4Understanding liabilities for BYOD

Liabilities make BYOD not just an IT issue, but also the concern of organisational legal departments. Legal units must ensure that both the organisation and BYOD users' liability risks are well managed and contained. When corporate or personal data is exposed, intentionally or not, neither the employee nor the organisation will want to be liable. Therefore, when implementing control measures for BYOD, users' liability must be assessed for organisational data, legal ramifications of damages must be considered, and organisational liability must also be assessed for BYOD users' personal data.

2.5Understanding awareness and training programs for BYOD

BYOD security and privacy issues require awareness and training programs. It is psychologically possible that when BYOD users are informed through awareness and training about the possibility of their identity to be compromised when using a mobile device, they will be more security and privacy vigilant [25].

An awareness and training program concerning security and privacy for BYOD should encompass networks, applications, and web-based security and privacy threats and vulnerabilities. This is important as BYOD users are mostly not inclined to accept full mobile device management by their organisations [10]. Training programs should be tailored to adequately demonstrate BYOD device vulnerabilities. In order to avoid BYOD users perceiving training as a burden, the training program sessions should be short and concise, and remain effective in relaying information to the users.

2.6Understanding BYOD user perception and behaviour

BYOD can have an unexpected impact on employees' perceptions and behaviour when it comes to acceptance of liabilities, and technical controls used by organisations. It has been accepted in information systems research that users' perceptions with respect to a specific technological system determines their intention to use, which also determines the users' behaviour [26]. When exploring security and privacy measures for BYOD, it is essential to consider users perceptions, characteristics and behaviour, as they can determine whether the measures are likely to be successful.

3. Balancing Security and Privacy Controls for BYOD

A key challenge in BYOD is how organisations can protect their information and at the same time manage and control BYOD users and their devices without violating privacy. The use of excessive security measures by organisations can affect BYOD users' privacy. Likewise, the high consideration of BYOD users' privacy by organisations, coupled with fear of lawsuits, can affect the adequate usage of security measures to protect organisational confidential information resources. Therefore, some level of balance is required between security and privacy when implementing BYOD control measures.

Figure 2 examines the relationship between the components in the BYOD policy-based management model (Figure 1) to strike a balance between security and privacy controls for BYOD.

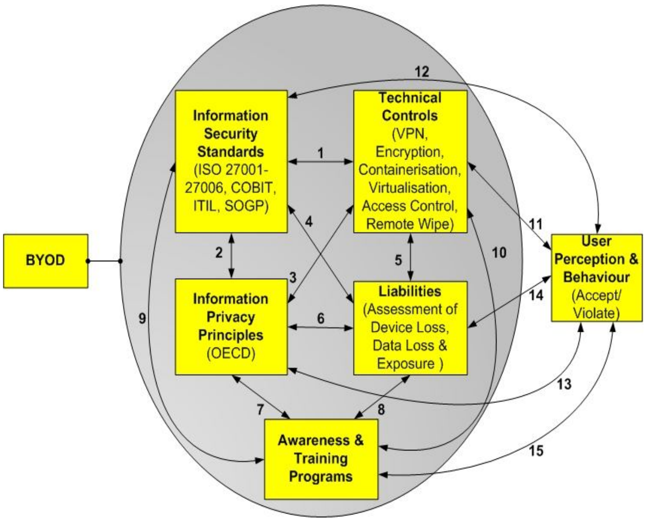
Information Security Standards (ISO 27001-27006, COBIT, ITIL, SOGP)
Technical Controls (VPN, Encryption, Containerisation, Virtualisation, Access Control, Remote Wipe)
BYOD
Information Privacy Principles (OECD)
Liabilities (Assessment of Device Loss, Data Loss & Exposure)
User Perception & Behaviour (Accept/ Violate)
Awareness & Training Programs
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Figure 2 BYOD policy-based management model (instantiated with BYOD controls)

Relationship #1: The access to organisational resources in BYOD should be managed by a combination of information security standards and technical controls. Generally, the implementation of technical security and privacy controls may require significant operating considerations. Information security standards and procedures can support the selection of technical controls and define how they should be used by organisations in a stable and consistent manner.

Relationship #2: A blurring exists between personal information and organisational information on BYOD devices. Information privacy principles, coupled with information security standards, might define this line for organisations and employees to mitigate issues of privacy violation in BYOD practices. Applying information privacy principles and security standards can allow organisations to delegate more responsibility to BYOD users (such as how to avoid and report security and privacy incidents in a timely manner), while the organisation maintains monitoring and controlling of BYOD devices at minimal levels.

Relationship #3: The strategies to mitigate BYOD privacy risks may include the use of technical controls. These technical controls will require significant operating modes. Information privacy principles will select and define how technical controls should be used by organisations in a manner that ensures protection of both BYOD users' personal information and organisational data.

Relationship #4: Information security standards may reduce liability in BYOD. When security problems arise in BYOD practices and generate liabilities, information security standards can be reviewed by organisations to highlight ways to avoid additional exposure to such liabilities.

Relationship #5: The use of technical controls has a direct impact on liability that is linked with BYOD practices. For example, using encryption for data downloaded from organisational resources to BYOD devices may directly relieve BYOD users from specific liability, especially when data is compromised. Additionally, this could help BYOD users feel protected against other potential liabilities in BYOD.

Relationship #6: Information privacy principles may decrease liability associated with BYOD. When privacy issues arise and generate liability, information privacy principles could limit and regulate all claims with respect to damages caused in BYOD practices.

Relationship #7: Regular awareness and training programs may educate employees on how to mitigate privacy risks in BYOD environments, since most employees are either not aware of the level of BYOD privacy they are entitled to from organisations, or have no knowledge of the information privacy principles to which their organisation must abide [10].

Relationship #8: Awareness and training programs may assist organisations in avoiding or reducing liability associated with BYOD, particularly in the case where there is non-compliance to policies by BYOD users.

Relationship #9: Information security standards may structure organisational awareness and training programs. The standards will assist organisations with the development of training plans, in addition to the BYOD security awareness and training programs.

Relationship #10: Awareness and training programs concerning technical security and privacy controls may provide a strong level of defense for organisations against BYOD threats. The awareness of new malware, viruses, phishing attacks, identity thefts, coupled with training on how to apply technical controls to minimise the impact of these threats and vulnerabilities will reduce the risks to information in BYOD practices.

Relationship #11: Technical controls used by organisations may have a direct impact on BYOD user perception and behaviour. BYOD users will most likely find ways to bypass technical controls and policies if they know a possibility exists for their devices data to be accessed, modified or deleted without their approval [17]. In addition, BYOD user behaviour can indirectly impact technical controls. Password-based authentication control can be weakened if BYOD users decide to use simple passwords, or share their passwords with colleagues and friends.

Relationship #12: BYOD users may have a positive perception and develop good behaviour when they know their organisation is in compliance with information security standards, and has tailored the standards to suit BYOD. Users can assume that the best and fair security practices are adopted, and cogitate before violating policies.

Relationship #13: Users behaviour may change when they are aware their organisation is in compliance with privacy laws. Information privacy principles that protect organisational data and employee personal information will encourage good policy compliance behaviour by BYOD users, and reduce the likelihood of liabilities.

Relationship #14: BYOD users' perception and behaviour may either increase or decrease liability. Positive behaviour from BYOD users can reduce both the organisation and the users' liabilities when security and privacy incidents occur through BYOD devices.

Relationship #15: The majority of employees' perceptions about information security and privacy is usually positive [27]-[28]. Therefore, there is a tendency that the more BYOD users are exposed to security and privacy awareness and training programs, the better behaviour they will have towards securing their devices and complying with organisational policies [25].

Taking into consideration the controls from the components of the BYOD policy-based management model, and the relationships between the components examined to strike a balance between BYOD security and privacy, the next section offers effective BYOD policy framework and guidelines for organisations.

4. BYOD Policy Framework and Guidelines

Every organisation should have a security and privacy policy that protects information resources and guides employees' behaviour. A BYOD policy has to address constraints on access, control and protection of organisational information resources by both internal and external users. Based on the BYOD policy-based management model in Figure 2, a BYOD policy architecture which organisations can adopt is proposed in Figure 3. This is followed by discussions on the policy regulations in Table 1 to Table 7.

The BYOD policy architecture has three layers that can be administered by organisations to bring control and defense-in-depth in BYOD environments: operational; tactical; and strategic. The operational layer (Table 1) is the core of regulating BYOD devices and users, and operates hand in hand with the other layers.

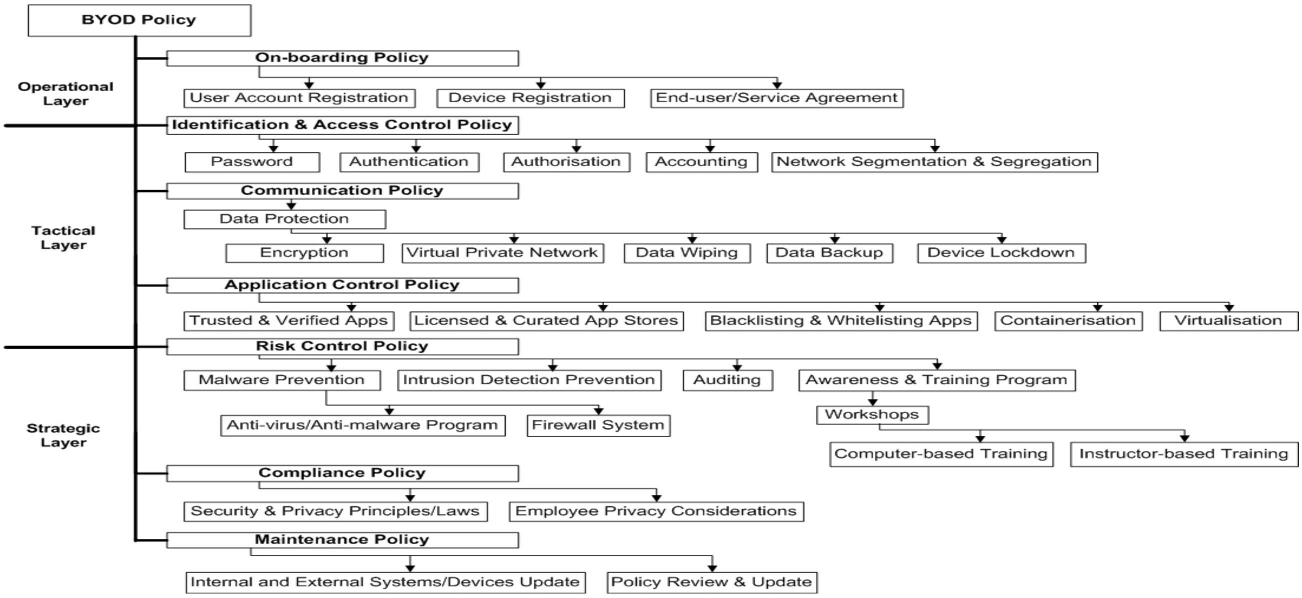

Figure 3 BYOD policy architecture

The tactical layer (Table 2 to Table 4) supports functions for information security and privacy administration. The final layer is the strategic layer (Table 5 to Table 7), which includes the overall risk management and governance aspects. The procedures of all the layers are discussed in the following tables.

The concept behind the BYOD on-boarding policy in Table 1 is to provide a systematic and comprehensive approach to familiarise BYOD users on the requirements to get on-board, and also to inform them of obligations and expectations.

Table 1: BYOD on-boarding policy

Operational Layer	
1. On-boarding Policy *Objective:* To determine who can on-board BYOD devices, including the types of BYOD devices that will be allowed access, as well as the number of BYOD devices each person can on-board to organisational systems.	
1.1 User Account Registration	*Control:* BYOD users should provide verifiable information about themselves such as employee ID, job position/role, and department etc, in order to create an account and register their devices
1.2 Device Registration	*Control:* BYOD users should provide their device information such as make/model, serial number, IMEI number, and MAC address.
1.3 End-user/Service Agreement	*Control:* BYOD users must agree to sets of requirements concerning information resources usage, and liabilities (device and data loss/exposure).

The identity and access control policy is intended to specify and define procedures and access control measures to protect unauthorised access to BYOD devices, as well as unauthorised access to organisational information resources in BYOD environments. Table 2 specifies the security and privacy requirements and controls to manage identity and access control in BYOD practices.

Table 2: BYOD identification & access control policy

Tactical Layer	
2. Identification & Access Control Policy	
2.1 Password Objective: To protect unauthorised access to BYOD devices and organisational systems.	
Repeated and sequential characters	*Control:* Restrict BYOD users from using repeating and sequential characters in their passwords.
Alphanumeric values, upper/lower case characters, and special characters	*Control:* Passwords should contain both upper and lower case characters and have at least two letters, one number, and one special character such as !, @, #, $, %.
Password length	*Control:* At least 8 characters long.
Password age and history	*Control:* Password should be changed on a regular basis (e.g every 90 days). The new password should not be accepted if it matches three previously used passwords by the BYOD user.
System logout and auto lock	*Control:* Automated system logout and device lock should be initiated when organisational systems, BYOD users and their devices are idle for a period of time (e.g 15 minutes).
Failed password attempts	*Control:* A maximum number of failed password attempts should be set for corporate emails and applications, followed by a selective remote data wipe after exceeding the limits of password attempts.
2.2 Authentication *Objective:* To identify and verify BYOD users and devices.	
Multi-factor authentication	*Control:* “Knowledge” authentication factors such as username and passwords should be used for BYOD users’ authentication, while “Possession” authentication factors such as trusted Digital Certificates signed using the Digital Signature algorithm, can be exchanged between BYOD devices and organisational systems to authenticate the devices.
2.3 Authorisation *Objective:* To grant BYOD users and devices different access rights to organisational systems and resources.	
Access privileges	*Control:* Mapping confidential information resource to the right BYOD device should occur within the context of authentication. Rules must be implemented to determine the kind of activities, or resources a BYOD user or device is permitted to access and use.
2.4 Accounting *Objective:* To have visibility of BYOD users and devices activities and measure the resources they consumed.	
Tracking and monitoring usage	*Control:* IT administrators should have visibility of the types of BYOD devices being used by users; which users and their devices are currently logged on; how the users were authenticated; how long users have been in the current session; and their IP and MAC addresses.
2.5 Network segmentation & segregation *Objective:* To minimise access to sensitive information for BYOD users and devices.	
Guest/BYOD users network	*Control:* The key organisational network should be partitioned into a smaller network (guest/BYOD users’ network) to develop and enforce a rule set that controls which BYOD users and devices are permitted to communicate with which organisational systems.

The goal of the communication policy in Table 3 is to control confidential data storage, access, and exchange or transfer between BYOD devices and organisational systems. The policy prevents the inappropriate usage or unauthorised disclosure of confidential information in BYOD environments.

Table 3: BYOD communication policy

Tactical Layer	
3. Data Protection	
3.1 Encryption *Objective:* To protect the confidential information resources of organisations residing on BYOD devices.	
Device internal memory encryption	*Control:* Encryption algorithms like DES, AES, or Blowfish, should be used to protect email and text messages, contacts list, calendar, and other credential information situated in the BYOD device built in memory.
Device external memory encryption	*Control:* Encryption applications should be installed on BYOD devices to protect all information stored in removal/flash memory cards.
3.2 Virtual Private Network (VPN) *Objective:* To preserve the integrity of data during communication.	
VPN applications and settings	*Control:* Mobile VPN and other VPN application controls should be used to maintain information in transit accuracy during data exchange and communication between BYOD devices and organisational systems.
3.3 Data Wiping *Objective:* To protect confidential information when BYOD devices are lost or stolen.	

Remote wipe	*Control:* IT administrators should be able to remotely wipe lost or stolen BYOD devices with the full consent of the device owners/users or in accordance with the end-user/service agreement.
Selective wipe	*Control:* IT administrators should be able to selectively wipe organisational information resources on BYOD devices that are infected or highly vulnerable to malware /viruses, or if users violate control measures.
Device auto wipe	*Control:* BYOD users and IT administrators should be able to activate automatic built-in device wipe features installed, after a series of failed password attempts.
3.4 Data Backup *Objective:* To maintain the availability of BYOD user personal information in the event of device/data loss or corruption.	
Encrypted backup service	*Control:* Device data should be backed up regularly either remotely via the internet or through cable, using encrypted data backup software and services.
3.5 Device Lockdown *Objective:* To lockdown BYOD devices remotely when they are lost or stolen.	
Device lockdown software	*Control:* IT administrators and BYOD users should use applications to remotely lock or shut down compromised devices.

The application control policy in Table 4 is intended to prevent BYOD users and devices from accessing or using malicious applications that can compromise security and privacy. Additionally, the intent of the application control policy is to prevent the muddling of personal and corporate data, as well as the possibility for data exfiltration between personal and corporate applications on BYOD devices.

Table 4: BYOD application control policy

Tactical Layer	
4. Application Control Policy	
4.1 Trusted and Verified Apps *Objective:* To avoid the installation and usage of uncertified applications on BYOD devices.	
In-house IT applications	*Control:* All in-house applications developed for BYOD devices should be certified by the IT managers of the organisation.
Applications testing and deployment	*Control:* All applications should be tested by the organisation information security team, followed by approval from executive management before usage on BYOD devices.
Third party and external applications	*Control:* BYOD users should only install code-signed applications by developers.
4.2 Licensed and Curated Application Stores Objective: To avoid the installation and usage of malware applications on BYOD devices.	
Secured application stores	*Control:* BYOD users should download and install applications either from organisational application stores, or from licensed application stores (such as apple store) where applications are thoroughly tested before being available for commercial download.
4.3 Blacklisting and Whitelisting Applications *Objective:* To identify uncertified and malicious applications.	
Applications blacklisting	*Control:* All malicious and untrusted applications should be securely removed from BYOD devices and blacklisted so that they cannot be installed on the device or be operable on organisational systems and network.
Applications whitelisting	*Control:* A list of trusted and certified applications should be maintained to eliminate the risk of installing unknown and unwanted applications on BYOD devices.
4.4 Containerisation Objective: To protect and separate organisational data from personal data on BYOD devices.	
Application and device integrated containers	*Control:* Organisational applications should be wrapped or encased in secure containers and deeply integrated into BYOD devices operating systems to segregate work and personal spaces.
4.5 Virtualisation *Objective:* To prevent unauthorised manipulation of organisational data by BYOD devices.	
Virtual desktop infrastructure	*Control:* Desktop virtualisation should be employed for executing applications and storing data, rather than from the BYOD devices.

The risk control policy in Table 5 defines controls and responsibilities to ensure that organisational confidential information resources used in BYOD, including BYOD users and devices, are protected against potential risks, threats and vulnerabilities.

Table 5: BYOD risk control policy

Strategic Layer	
5. Risk Control Policy	
5.1 Malware Prevention *Objective:* To protect and prevent BYOD devices and organisational resources from malware attacks.	
5.1.1 Anti-virus/Anti-malware Program *Objective:* To detect and destroy viruses on BYOD devices.	
Anti-virus/anti-malware program functionality	*Control:* In addition to protecting BYOD devices and applications, anti-virus and anti-malware programs should be able to scan BYOD devices thoroughly to

	detect and remove latest viruses, Trojan horses, worms, Adware, spyware, and Rootkits.
Tested, licensed, and password protected anti-virus/anti-malware program	*Control:* Only well-known and verified anti-virus and anti-malware programs should be run on BYOD devices. These programs should be password protected by organisations to stop BYOD users from uninstalling or disabling them.
Anti-virus/anti-malware program updates	*Control:* Maintain regular updates of anti-virus and anti-malware programs on BYOD devices with the most recent signatures.
5.1.2 Firewall Program *Objective:* To block inbound and outbound malicious connections and filter traffic demands of BYOD devices and applications.	
Firewall program functionality	*Control:* In addition to blocking network traffic from suspected malicious source, the firewall should be able to filter and restrict BYOD device access based on network connection type (cellular or Wi-Fi), applications type, and other packet attributes such as IP address.
Firewall program rule set	*Control:* A set of rules should be defined for firewalls with respect to BYOD user authorisation to access resources, as well as their behaviour and compliance with policies.
Tested and certified firewall program	*Control:* Only well-known and verified firewall programs should be run on BYOD devices.
5.2 Intrusion Detection Prevention *Objective:* To detect/prevent unauthorised access and attacks from or through BYOD devices.	
Intrusion detection system	*Control:* Network access points for BYOD devices should be integrated with intrusion detection system to act as a security sensor that can identify and stop unauthorised access and threats from compromised BYOD devices.
Documenting incidents	*Control:* Logs of identified threats and communications between BYOD devices and organisational resources should be maintained for at least a minimum period of one year.
5.3 Auditing *Objective:* To determine the effectiveness of control measures around protecting data on BYOD devices, as well as BYOD user compliance with policies.	
Unified and periodic auditing of devices	*Control:* All BYOD devices should be audited regularly to check that control measures are operational and BYOD users are complying with policies.
5.4 Awareness and Training Program *Objective:* To educate BYOD users on how to avoid threats and vulnerabilities when using their devices, as well as comply with organisational BYOD policies.	
Computer-based training workshop	*Control:* BYOD users should be frequently engaged in online and distance training programs about current and future potential risks in BYOD environments and how they can be mitigated.
Instructor-based training workshop	*Control:* BYOD users should be regularly engaged in face-to-face training programs, in order to increase their focus on threats and vulnerabilities and establish dialogues with instructors on mitigation strategies.

The compliance policy controls in Table 6 minimise the potential for litigation and liability issues for organisations concerning BYOD practices. The policy guides organisations on how to avoid engagement in unlawful conduct in BYOD that violates BYOD users privacy or the sovereignty of the country in which they are operating their business.

Table 6: Compliance policy

Strategic Layer	
6. Compliance Policy	
6.1 Security/Privacy Principles and Laws *Objective:* To comply with information security and privacy standards, and abide by the principles and laws of nations with regards to information protection.	
Complying with national information security and privacy laws	*Control:* Security and privacy policies should be developed, modified or updated according to specific country laws or the region in which an organisation is operating its business.
Complying with information security and privacy standards	*Control:* In addition to compliance with information security and privacy standards, the standards should be adapted to accommodate and manage BYOD.
6.2 Employee Privacy Considerations *Objective:* To maintain the privacy of BYOD users' personal data.	
Data collection limitation	*Control:* BYOD users' personal data should only be obtained in a legal and fair manner with the knowledge/consent of the data subjects.
Purpose specification of data access and collection	*Control:* BYOD users' personal data access and collection by organisations should only be carried out when there is a satisfactory warrant in accordance with the authority of law.
Data use limitation	*Control:* BYOD users' personal data should not be disclosed or used for other purposes, rather than those specified in the end-user/service agreement, or except with the permission of the data owners.
Individual	*Control:* BYOD users should be allowed to

participation	challenge any data collected related to them, to either be erased or amended.
Technical safeguards	*Control:* Reasonable techniques that involve disk partitioning, or containerisation and virtualisation should be used to segregate BYOD users' personal data and organisational data to allow selective wipe of data when employees leave the organisation or BYOD devices are lost or stolen.

Table 7: Maintenance policy

Strategic Layer	
7. Maintenance Policy	
7.1 Internal and External Systems/Devices Update *Objective:* To improve infrastructure of organisations and BYOD devices.	
Updating control systems and devices	*Control:* Organisational infrastructure and BYOD devices operating systems and applications should be regularly updated to resolve security vulnerabilities and threats, as well as provide performance options and features to users.
7.2 Policy Review and Update *Objective:* To assess and bring policies up to date.	
Reviewing and updating policies	*Control:* BYOD policies should be reviewed and updated regularly to ensure adequate control measures that are in compliance with regional laws are in place, and can cope with the continuous demands of BYOD.

The maintenance policy in Table 7 is to ensure that the correct strategies for managing BYOD are employed, and all associated risks and potential threats are effectively managed.

5.DISCUSSION

Managing BYOD is about determining and understanding its level of adoption and practices, potential threats, vulnerabilities and incidents, and putting the right processes or controls in place that are in accordance with good practice. Considering the growing list of risks associated with BYOD, organisations should re-examine the effectiveness of their information security and privacy frameworks across a wide range of components that include: technical controls; policies; standards and procedures; and user awareness/training programs. All these can be combined to develop a BYOD solution framework comprising policy architecture and sets of guidelines for organisations.

Organisations can employ the BYOD policy framework and guidelines proposed in this paper to reduce the risk of confidential information loss in BYOD. The framework adopts a three layered approach with all the layers implemented fully. Alternatively one of the layers or its controls can be implemented by an organisation to support their BYOD control methods. Factors such as the selection of individual controls from the model will depend on the nature of the organisation, its IT security and privacy budget, and the level of risk tolerance.

Overall, it is highly recommended for organisations to periodically review their BYOD security and privacy controls and policies to ensure proficiency with varying BYOD practices.

6.CONCLUSION

The future of BYOD practices in the workplace is evolving. Organisations need to implement or update their existing policies to include conduct parameters for BYOD in order to mitigate security and privacy risks. The BYOD policy-based framework proposed in this paper can be expanded to include more control measures in order to keep up with the continuous security and privacy demands of BYOD. It is also very important to recognise that if organisations want to be effective in managing BYOD and its associated risks and threats, understanding how to strike a balance between security and privacy controls for BYOD is vital.

References

[1] B. Hayes and K. Kotwica, Bring Your Own Device (BYOD) to Work: Trend Report. Oxford UK: Elsevier, 2013.

[2] A. M. French, C. Guo, and J. Shim, "Current Status, Issues, and Future of Bring Your Own Device (BYOD)," Communications of the Association for Information Systems, vol. 35, p. 10, 2014.

[3] J. Keyes, Bring Your Own Devices (BYOD) Survival Guide. Boca Raton, FL: CRC Press, 2013.

[4] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, pp. 53-55, 2012.

[5] M. E. Whitman and H. J. Mattord, Principles of information security. Boston USA: Cengage Learning, 2010.

[6] N. Mooradian, "The importance of privacy revisited," Ethics and Information Technology, vol. 11, pp. 163-174, 2009.

[7] T. R. Peltier, Information security fundamentals: CRC Press, 2013.

[8] A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, "Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments," Journal of Information Privacy and Security, vol. 11, pp. 38-54, 2015.

[9] M. Eslahi, M. V. Naseri, H. Hashim, N. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in Computer Applications and Industrial Electronics (ISCAIE), IEEE Symposium, pp. 189-192, 2014.

[10] A. B. Garba, J. Armarego, and D. Murray, "Bring your own device organizational information security and privacy," ARPN Journal of Engineering and Applied Sciences, vol. 10, pp. 1279-1287, 2015.

[11] D. Rivera, G. George, P. Peter, S. Muralidharan, and S. Khanum, "Analysis of Security Controls for BYOD

(Bring your own Device)," The University of Melbourne, Melbourne, 2013.

[12] K. J. Smith and S. Forman, "Bring Your Own Device—Challenges and Solutions for the Mobile Workplace," Employment Relations Today, vol. 40, pp. 67-73, 2014.

[13] L. Guan, "Established BYOD management policies needed," Government News, vol. 32, p. 9, 2012.

[14] A. Dedeche, F. Liu, M. Le, and S. Lajami, "Emergent BYOD security challenges and mitigation strategy" The University of Melbourne, Melbourne, 2013.

[15] A. Ghosh, P. K. Gajar, and S. Rai, "Bring your own device (BYOD): Security risks and mitigating strategies," Journal of Global Research in Computer Science, vol. 4, pp. 62-70, 2013.

[16] ZixCorp. "Zix Corporation and Ponemon Institute Survey Reveals Limitations and Frustration with First Generation Bring-Your-Own-Device Security Products," Jul. 29, 2013. [Online]. Available: http://investor.zixcorp.com/phoenix. zhtml?c=108645&p=irol-newsArticle&ID =1875802&highlight

[17] T. Y. Andrew and A. T. Yang, "Risk Management in the Era of BYOD," in Symposium on Usable Privacy and Security (SOUPS), 2013.

[18] C. P. Pfleeger and L. P. Shari, Security In Computing. Upper Saddle River, NJ: Prentice Hall PTR, 2006.

[19] OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Commonwealth law bulletin, vol. 7, p. 1078, 1980.

[20] ISO 27000 Directory. An Introduction to ISO 27001, ISO 27002....ISO 27008. Mar. 13th 2014. [Online]. Available: http://www.27000.org/ contact.htm

[21] ISACA, "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT," ed. Rolling Meadows, USA: ISACA, 2012.

[22] Information Security Forum. The Standard of Good Practice for Information Security. Mar. 20th 2014. [Online]. Available: http:// www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf

[23] ITIL, IT Infrastructure Library, Service design, 2nd ed.: Stationery Office., 2007.

[24] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: OECD Publishing, 2002.

[25] M. A. Harris, K. Patten, and E. Regan, "The need for byod mobile device security awareness and training," in Americas Conference on Information Systems, Chicago, 2013.

[26] V. Venkatesh, M. G. Morris, D. B. Gordon, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS quarterly, pp. 425-478, 2003.

[27] I. Kirlappos, A. Beautement, and M. A. Sasse, "“Comply or Die” Is Dead: Long live security-aware principal agents," in Financial Cryptography and Data Security, ed: Springer, pp. 70-82, 2013.

[28] R. W. Woodman, D. C. Ganster, J. Adams, M. K. McCuddy, P. D. Tolchinsky, and H. Fromkin, "A survey of employee perceptions of information privacy in organizations," Academy of Management Journal, vol. 25, pp. 647-663, 1982.