2020

BYOD-Insure vs Existing Modalities for BYOD Security Assessment: A Comparison Study

Melva Ratchford
Dakota State University

Yong Wang
Dakota State University

Cherie Noteboom
Dakota State University

Omar F. El-Gayar
Dakota State University

Recommended Citation

Ratchford, Melva M.; Wang, Yong; Noteboom, Cherie Bakker; and El-Gayar, Omar, "BYOD-Insure vs Existing Modalities for BYOD Security Assessment: A Comparison Study" (2020). AMCIS 2020 Proceedings. 12. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/12

BYOD-Insure vs Existing Modalities for BYOD Security Assessment: A Comparison Study

Melva M. Ratchford
University, melva.ratchford@gmail.com

Yong Wang
Dakota State University, yong.wang@dsu.edu

Cherie Bakker Noteboom
Dakota State University, cherie.noteboom@dsu.edu

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

Recommended Citation

Ratchford, Melva M.; Wang, Yong; Noteboom, Cherie Bakker; and El-Gayar, Omar, "BYOD-Insure vs Existing Modalities for BYOD Security Assessment: A Comparison Study" (2020). *AMCIS 2020 Proceedings*. 12.
https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/12

BYOD-Insure vs Existing Modalities for BYOD Security Assessment: A Comparison Study

Melva M. Ratchford
Dakota State University
Melva.ratchford@trojans.dsu.edu

Yong Wang
Dakota State University
Yong.Wang@dsu.edu

Cherie Noteboom
Dakota State University
Cherie.Noteboom@dsu.edu

Omar El-Gayar
Dakota State University
Omar.El-Gayar@dsu.edu

Abstract

Often, organizations allow employees the use of their personally owned devices to access corporate data. This phenomenon is identified as Bring Your Own Device (BYOD), and organizations are adopting it without taking into consideration the inherent security risks introduced via BYODs. There are several approaches that organizations can consider for BYOD security. This paper addresses research questions related to the protection of BYOD environments. In general, how can organizations protect against the inherent risks posed by BYODs? What are existing modalities to do so? With this in mind, this research reviews existing BYOD security approaches, such as frameworks, checklists, best practices, and quantitative models, and performs a comparative analysis among such modalities. Based on our research, this comparative study shows that a quantitative model, BYOD-Insure, meets the requirements for security assessment of BYOD environments. The model provides a level of detail, granularity and specificity that existing modalities do not.

Keywords

Bring Your Own Device, BYOD Security, Assessment, BYOD-Insure, Design Science

Introduction

Organizations benefit when allowing employees to use personal mobile devices (a phenomenon known as Bring Your Own Device or BYOD) to access corporate data, since this type of access reduces cost and increases productivity (Bello Garba et al. 2015). This phenomenon is a by-product of IT consumerization (Ogie 2016). ‘BYOD is rapidly becoming the norm rather than the exception’ (Crossler et al. 2014). By 2020, 80% of the adults on earth will be using smartphones (RSA 2016). The BYOD market is predicted to increase from $30 billion in 2014 to an estimated value of $366.95 billion by 2022 (Insights 2016).

When organizations embrace BYOD environments without considering the inherent security risks of BYODs, a security problem is created. New security risks and challenges are raised with the use of BYODs (Wang et al. 2014). Personal devices can easily be lost or stolen. Many threats and attacks including spoofing, phishing, sniffing, spam, and denial-of-service have also been found targeting BYODs (Wang et al. 2014). Other findings help understand the use of personal devices in the work environment. For example, a recent study showed results that indicate that the millennials (people born between 1980 and 1995) embrace the use of BYOD based on the benefits they perceive, while ignoring the risks (Weeger et al. 2020). In addition, organizations are exposed to legal issues such as privacy laws that are protected by the Fourth Amendment of the U.S. Constitution in favor of the BYOD owners (Absalom 2012; Ratchford et al. 2018). Thus, organizations may face litigation problems that can drain their resources.

The research questions addressed in this paper relate to the security of BYOD environments. In general, how can organizations protect against the inherent risks posed by BYODs? What are existing modalities to do so? This paper follows a review and compare approach. After surveying the existing literature, we identify BYOD security requirements and current modalities for securing BYOD environments. The existing BYOD security modalities are classified into four categories, i.e., frameworks, checklists, best practices and quantitative models. Next, we conduct a comparative analysis among such models. Our analysis finds that, the quantitative model BYOD-Insure (Ratchford and Wang 2019), is the better option for securing BYOD environments.

The development of the BYOD-Insure model is based on design science research methodology principles (Ratchford and Wang 2019). It follows a problem-centered approach as described by Peffer et al. (2007). This approach includes *problem identification* (organizations adopt BYODs without considering inherent BYOD security risks), *definition of objectives for a solution* (to aid organizations to secure BYOD environments), *design and development (*the model is based on existing theory and algorithms suitable for security posture comparison based on extant literature review to identify security controls), *demonstration* (demonstration of each of the components of the model), *evaluation* (model's characteristics and utility based on descriptive scenarios), and *communication* (publication of model's initial proposal).

In order to show the advantages and usefulness of the BYOD-Insure model, we present an overview of the artifact followed by a demonstration of its utility. The latter is done through descriptive scenarios of security postures corresponding to low, medium and high security stance in organizations following the recommendations for design science research evaluation methods proposed by Hevner et al. (2004). The results of the model's execution show the security weaknesses and strengths for an organization, with respect to BYOD. The granular analysis can be noted at the organizational level, at the domains level (e.g. Mgmt., IT, user or mobile device), and at the security control level, as it identifies the domains that need attention, highlight the security controls that need to be strengthened, and recommends safeguards to mitigate security risks.

The organization of this paper is as follows: after this introduction, a set of requirements for BYOD security is defined, followed by a discussion of the existing modalities for securing BYOD environments. Then, a comparison analysis between the existing modalities vs BYOD-Insure, is performed. This is followed by a description of the model which includes the research methodology, model overview and a demonstration process. The paper concludes with a summary, research contribution, artifact limitations and future work.

Requirements for BYOD Security

When considering the problems discussed above, coupled with the need for organizations to secure their BYOD environments, and given the gap in current security modalities, requirements for BYOD security can be stated as follows: R1) the identification of risks and vulnerabilities associated with BYODs; R2) a comprehensive set of security controls aiming at a holistic approach to security where the main domains of an organization are addressed (i.e. management, IT, users and mobile devices); R3) a non-ambiguous assessment process that identifies the security vulnerabilities in an organization; and R4) the ability to provide actionable recommendations to mitigate BYOD related security risks (Ratchford and Wang 2019).

Modalities for Securing BYOD Environments

Best Practices

Best practices are discussed in industry publications as well as in academia. Romer (2014) discusses the need to select solutions that protect all confidential data and devices, have centralized control and monitoring, implement role-based access control to allow employees quick access to file-sharing, implement private cloud solutions, block risky services, and select proven solutions (Romer 2014). In industry, organizations such as Citrix Systems describe best practices that include issues related to eligibility, allowed devices, service availability, rollout, cost sharing, security and compliance, and device support and maintenance (Citrix Systems 2012).

Other best practices concentrate on the creation of BYOD policies that include topics such as on-boarding, identification & access control, communication, application control, risk control, compliance and maintenance (Alotaibi and Almagwashi 2018), as well as holistic best practice approach to BYOD security (Bello Garba et al. 2015). In addition, many publications focus on the understanding of BYOD risks, and the threats and challenges posed when adopting BYOD (Abubakar Garba et al. 2017; Ratchford et al. 2018; Wang et al. 2012; Wang et al. 2014).

Generic Frameworks

Various types of frameworks are described in scholarly works. One such framework is a comprehensive approach to BYOD security proposed by Zahadat (2015) - who presents a BYOD security framework that addresses issues related to technology, policy management, and people. The framework's objective is to present a solution to BYOD security concerns, and proposes a roadmap that includes a series of steps (i.e., plan -> identify -> protect -> detect -> respond -> recover -> assess and monitor) where each step is associated with specific set of controls that target BYOD security (Zahadat et al. 2015). As an example, for the 'protect' step, the controls refer to actions to take in order to achieve device authentication, wireless protection, network architecture, awareness and training, application store, application whitelisting and blacklisting, IPSec/VPN, mobile device management, location awareness, device fingerprinting, device encryption, sandboxing, virtualization, mobile OS patching, and application patching (Zahadat et al. 2015).

Another framework is presented by Bello-Garba et al. (2015) where a policy-based framework solution for organizations aims to protect information privacy and security. In this framework, the authors propose six components: information security standards and procedures, information privacy principles, information security privacy technical controls, liabilities, awareness & training program, BYOD user perception and behavior (Garba et al. 2015).

Checklists

Comprehensive and specific checklists that aim to protect BYOD environments can be found in several formats. For example, Sumate & Ketel (2014) present a list of items (in the form of questions) that need to be considered when designing a BYOD policy. The authors present a list of controls (e.g., to protect against insecure connections, lost or stolen devices, malware, work product created in mobile device, application streaming) that need to be considered in BYOD environments (Shumate and Ketel 2014).

ISACA (2016) designs a comprehensive checklist in the form of an audit/assurance IS program. Such presentation consists of a list of items/controls that need to be considered when implementing BYOD environments. The controls are grouped by topics such as security, risk management, governance, policies, and user & device management (ISACA 2016).

Quantitative Models

Quantitative models aim to assess an organization's security posture based on security measures adopted in the organization. Quantitative models provide the assessment based on the fact and associate data within the organization. However, challenges exist in quantitative models such as how to collect security measures and how to measure security attain levels. Due to the challenges, there are few assessment models in this category. BYOD-Insure (Ratchford and Wang 2019), falls into this category. The model performs the assessment by comparing the current security posture (with respect to BYOD) of an organization, against an ideal set of security controls (Ratchford and Wang 2019). Its design is grounded in existing mathematical algorithms in order to compare two security postures. The Euclidean's algorithm to calculate the distance between two matrices is an algorithm that serves this purpose. Casola et al. (2007) first proposed this type of analysis when comparing cryptographic policies. BYOD-Insure adopts this analysis and adapts it to BYOD security assessment. The model applies a holistic approach to security where four domains of an organization (i.e. Management, IT, User, and Mobile Device) work together in order to ensure confidentiality, integrity, and availability (CIA) of the organization's information. BYOD-Insure is composed of five modules as follows:

- *BYOD-Insure-Management:* Assesses the security posture of the Management of an organization with respect to BYOD.
- *BYOD-Insure-IT:* Assesses the security posture of IT of an organization with respect to BYOD.
- *BYOD-Insure-User:* Assesses the security posture of the BYOD Users of an organization.
- *BYOD-Insure-Mobile Devices: A*ssesses the security posture of the personally owned mobile devices that have access to the organization's information.
- *BYOD-Insure-Global: A*ssesses the overall security posture of the organization with respect to BYOD, once all the above modules have performed the respective assessment.

Comparison & Analysis

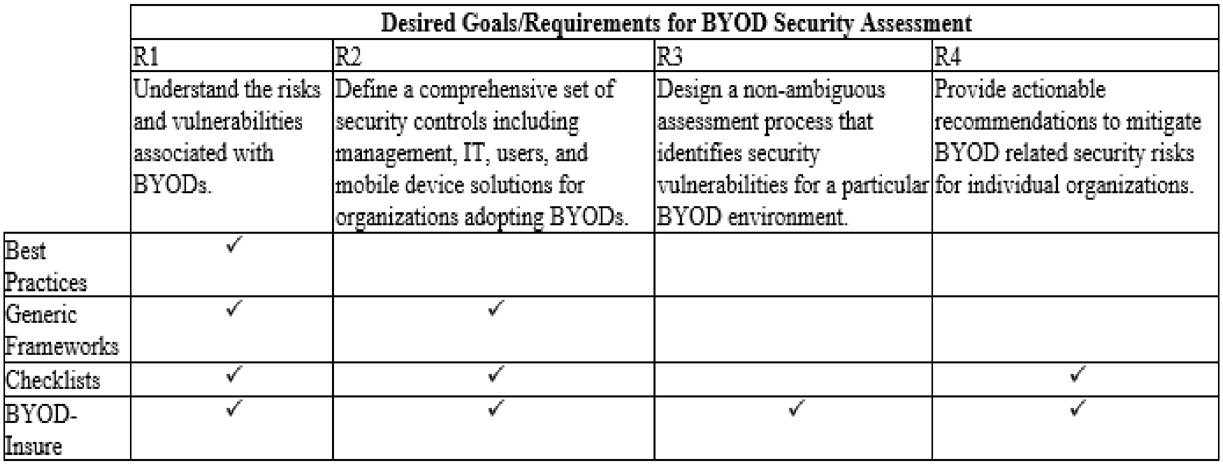
BYOD-Insure is a novel assessment model which has been recently proposed for BYOD security. When considering the four requirements, i.e., R1, R2, R3, and R4, for BYOD security, we present Table 1 which shows a comparison between the BYOD-Insure model and other existing modalities.

With respect to *best practices,* the existing literature provides ample understanding of the risks, vulnerabilities and challenges associated with BYOD. Existing works create awareness in organizations with respect to the inherent risks of BYOD, but do not provide a comprehensive set of controls, an assessment process nor an individualized approach for organizations.

Generic frameworks, on the other hand, do provide a roadmap for organizations to follow that includes a series of steps. Based on this information, the organization needs to devise its own method of assessment and extract the set of controls applicable to their BYOD environment.

Checklists provide a detailed and specific set of controls that can be easily 'checked-off'. However, the specific recommendations may not be present nor include clearly visualized diagrams indicating the individualized (i.e., to particular organizations) degree of exposure to BYOD risks. This type of approach is usually associated with an internal or external audit process.

BYOD-Insure is a quantitative model that encompasses all the above options. It produces graphical and individualized analysis of an organization's vulnerabilities, controls, and suggest recommendations to mitigate BYOD security risks. BYOD-Insure provides knowledge and understanding with respect to BYOD. Its approach is based on a holistic and comprehensive set of controls applicable to any organization with BYOD environments. It follows a non-ambiguous assessment process, and it provides results that are easily visualized, and recommendations that are individualized (Ratchford and Wang 2019).



	Desired Goals/Requirements for BYOD Security Assessment			
	R1	R2	R3	R4
	Understand the risks and vulnerabilities associated with BYODs.	Define a comprehensive set of security controls including management, IT, users, and mobile device solutions for organizations adopting BYODs.	Design a non-ambiguous assessment process that identifies security vulnerabilities for a particular BYOD environment.	Provide actionable recommendations to mitigate BYOD related security risks for individual organizations.
Best Practices	✓			
Generic Frameworks	✓	✓		
Checklists	✓	✓		✓
BYOD-Insure	✓	✓	✓	✓

Table 1. Comparison between different types of BYOD security modalities

As opposed to the existing modalities described above, BYOD-Insure is a security approach that meets the requirements as shown in Table 1. It not only provides organizational awareness with respect to BYOD but also identifies security weaknesses and highlights recommendations for BYOD risk mitigation. BYOD-Insure provides a level of granularity that is not present in the existing modalities discussed above. Frameworks, checklists and lists of best practices provide general information where the reader (expert or not) needs to decide what controls to implement. BYOD-Insure provides specific recommendations that are tailored to the organization.

BYOD-Insure meets all the requirements for BYOD security assessment and thus suitable for organizations to assess their security posture. In addition to its functionality, the analysis in (Ratchford and Wang 2019) also shows the ease-of-use of the model: the model is extendible since new security controls can be easily added as they are identified or required; the model is adaptable/scalable since security controls can be adapted as time changes and new domains/sub-domains are identified; the model is also flexible since it can be used by organizations of any size and can accommodate and implement controls based on their particular situation/priorities and budget constraints; the model has consistency since the same assessment approach can be applied to multiple modules and levels; the model provides fine-grained security assessment in both macro and micro levels; the results are easily visualized since its graphs depict clear indication of strengths and weaknesses; the model is also practical since the results provide individualized and actionable organization-specific recommendations based on the organization's security posture. BYOD-Insure is also programmable/automatable since the process is mechanical and repetitive. Once this artifact is automated, the usage of the model can be economical since the results are self-explanatory and may reduce the need to hire outside consultants.

In order to demonstrate the level of detail captured by BYOD-Insure, the next sections present an overview of the model and a demonstration of its results through a design science evaluation method using descriptive scenarios (Hevner et al. 2004). The scenarios describe BYOD security postures for organizations with low, moderate, and high security in BYOD environments. The security control weaknesses are identified, and safeguard recommendations are provided.

BYOD-Insure Model

Model Overview

Architecture. As described by Ratchford and Yong (2019), the objective of the model is to assess the security posture of an organization with respect to BYOD. The assessment process consists of four stages as follows: *Stage 1:* the generation of the optimal set of security controls, *Stage 2:* the extraction of an organization's BYOD posture, *Stage 3:* the comparison process and *Stage 4:* the generation of the results. This assessment is described in Figure 1. On the left-hand side of Figure 1, the 'Optimal Security Controls' shows the generation of an ideal set of security controls. These security controls are then organized and converted into a binary matrix. The right side of Figure 1 shows the recurring process (i.e., once for each organization).

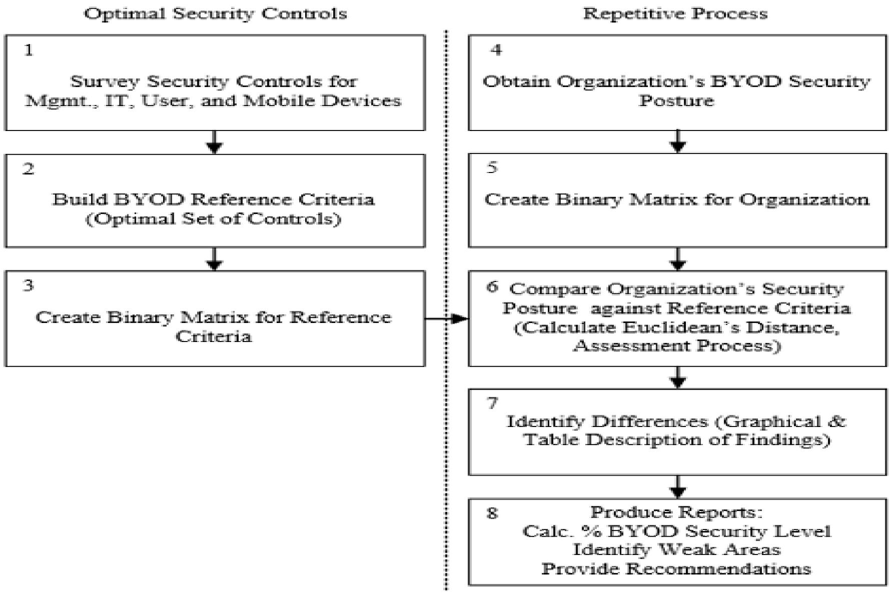

Optimal Security Controls
Repetitive Process
1 Survey Security Controls for Mgmt., IT, User, and Mobile Devices
2 Build BYOD Reference Criteria (Optimal Set of Controls)
3 Create Binary Matrix for Reference Criteria
4 Obtain Organization's BYOD Security Posture
5 Create Binary Matrix for Organization
6 Compare Organization's Security Posture against Reference Criteria (Calculate Euclidean's Distance, Assessment Process)
7 Identify Differences (Graphical & Table Description of Findings)
8 Produce Reports: Calc. % BYOD Security Level Identify Weak Areas Provide Recommendations

Figure 1. BYOD-Insure Assessment Process (Ratchford and Wang 2019)

The security controls of the organization's BYOD security posture are also converted to a binary matrix. After both matrices are built, the comparison (i.e., calculations based on Euclidian's distance algorithm) takes place. The results of these calculations assess the posture of an organization against a set of optimal security controls.

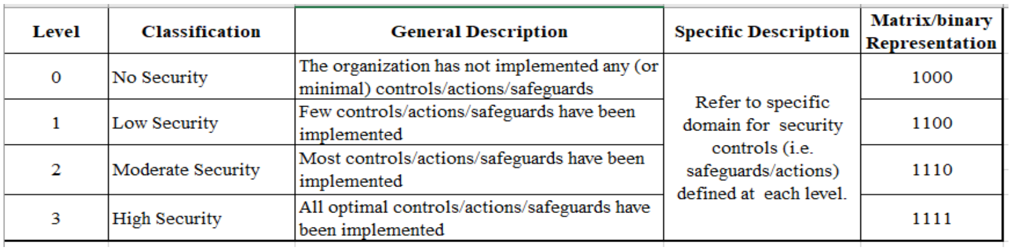
The comparison is based on a process designed by Casola et al (2007), where the difference between two postures is calculated using the Euclidian's algorithm to compute the distance (the difference in this case) between two matrices (Casola et al. 2007). Casola (2007) first demonstrated this when comparing cryptographic policies. Ratchford (2018) proposed a modified version of the same algorithm to evaluate BYOD policies (Ratchford 2018). For BYOD-Insure, the comparison is between the matrix that represents a company's BYOD security posture and the matrix that represents the optimal BYOD security posture. The result of this calculation provides a percentage security level for a specific domain. The security level analysis helps identify the weaknesses and vulnerabilities for each domain. Based on these results, organization-specific recommendations are provided.

Security Controls. The security controls discussed in this research are based on BYOD security issues identified through a systematic literature review (SLR). The concept of security issue refers to any type of security concern that represents a threat to organizational assets through the exploitation of a vulnerability where the implementation of controls is needed in order to mitigate the risks to the organization's assets (Disterer 2013; Fenz and Ekelhart 2009). These security issues are associated with an organization's domains corresponding to Management, IT, User and Mobile Device.

The SLR identified security concerns/issues associated with twenty-three areas as follows: access control, applications, best practices, BYOD programs, cloud access, compliance, data protection, education, employee attitude, IT consumerization, legal, malware, mobile device security, monitoring, network, policies, user privacy, risk management, security management, separation of data, governance, visualization and user support. These issues are mapped to specific security controls (i.e. identified through literature review), where the implementation of such controls becomes the responsibility of personnel associated with either management, IT, users, and/or security functions that need activation within the mobile device.

Model Demonstration/Evaluation Process

In the design science methodology, the evaluation of the artifact represents a crucial part of the research method, where the 'the utility, quality, and efficacy of a design artifact must be rigorously demonstrated via a well-executed evaluation method' (Hevner et al. 2004). Hevner et al. (2004) propose several types of evaluation methods for design science artifacts: Observational, Analytical, Experimental, Testing, and Descriptive. BYOD-Insure is evaluated using the Descriptive-Scenarios approach where the 'construction of detailed scenarios around the artifact demonstrate its utility', and the Experimental-Simulation method where the purpose is to 'execute artifact with artificial data' (Hevner et al. 2004). For BYOD-Insure, the descriptive and experimental evaluation methods demonstrate the utility and usefulness of the model when assessing different security postures that present security postures that fit the security classification depicted in Table 2. This approach also demonstrates the degree of granularity the model provides as the weaknesses and strengths can be visualized at the security control, domain, and organizational levels, as described in the following sections.



Level	Classification	General Description	Specific Description	Matrix/binary Representation
0	No Security	The organization has not implemented any (or minimal) controls/actions/safeguards	Refer to specific domain for security controls (i.e. safeguards/actions) defined at each level.	1000
1	Low Security	Few controls/actions/safeguards have been implemented		1100
2	Moderate Security	Most controls/actions/safeguards have been implemented		1110
3	High Security	All optimal controls/actions/safeguards have been implemented		1111

Table 2. Security Level Classification (Ratchford and Wang 2019)

Scenario 1 – Low Security Posture with Respect to BYOD

Model granularity at the security control level. Figure 2 presents the security posture of an organization with *low* security for most of the controls for the four domains: Management, IT, User, and Mobile Device. Based on the classification shown in Table 2, most of the controls corresponding to the Management domain reflect low security (i.e. level 1). The same can be observed for the IT domain, where the controls corresponding to BYOD Program, Education, Monitoring & Reporting, Virtualization, Mobile Applications, Anti-Malware, Mobile Device Content Mgmt. and Cloud Access were found to be at level 1 meaning that few controls have been implemented, whereas Risk Mgmt., Security Mgmt., Helpdesk, IT Consumerization, Policies, Best Practices, Network, Access Control, Data Protection, Mobile Device Security Management, are moderately secured. The control corresponding to Separation of Data needs IT attention, where the control for Third Party indicates that IT is implementing the necessary safeguards to ensure that BYODs used by third parties are in compliance. The same type of analysis can be observed with respect to the User and Mobile Device domains. The specific findings and recommendations are shown in Figure 3, which shows a partial sample of findings and recommendations (for Mgmt. and IT domains) for risk mitigation.

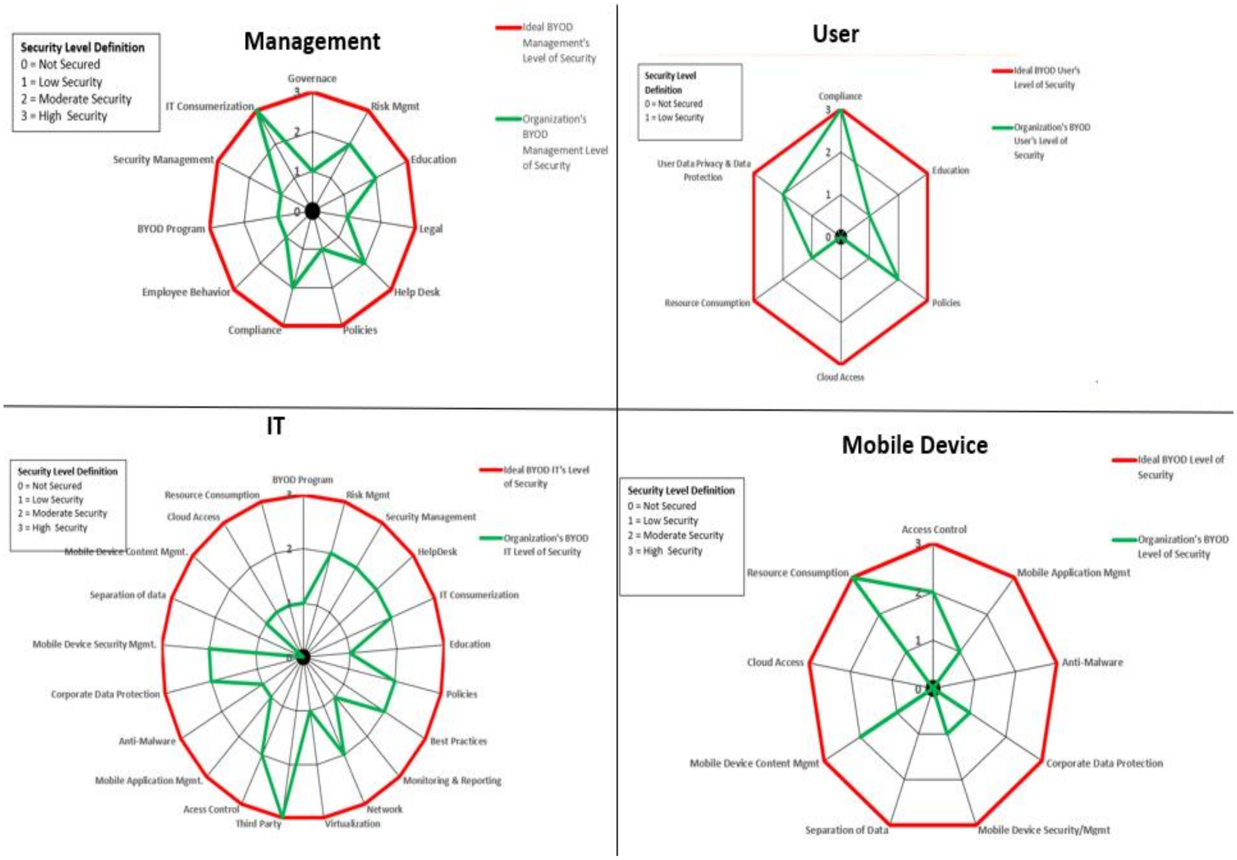
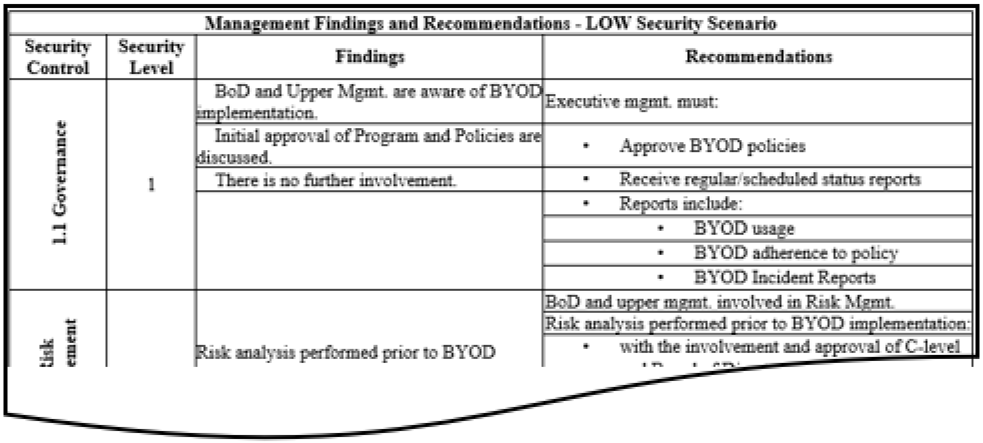


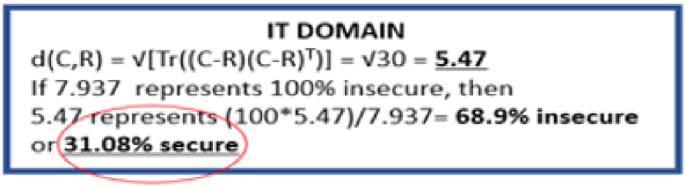
Figure 2. LOW Security Posture Scenario – Findings at the Security Controls Level



Management Findings and Recommendations - LOW Security Scenario			
Security Control	Security Level	Findings	Recommendations
1.1 Governance	1	BoD and Upper Mgmt. are aware of BYOD implementation.	Executive mgmt. must:
		Initial approval of Program and Policies are discussed.	• Approve BYOD policies
		There is no further involvement.	• Receive regular/scheduled status reports
			• Reports include:
			• BYOD usage
			• BYOD adherence to policy
			• BYOD Incident Reports
isk ement		Risk analysis performed prior to BYOD	BoD and upper mgmt. involved in Risk Mgmt.
			Risk analysis performed prior to BYOD implementation:
			• with the involvement and approval of C-level

Table 3. LOW Security Posture Scenario – Partial Findings & Recommendations Mgmt. Domain

Model granularity at the domain level. In order to calculate the security level at each domain, a security % analysis of each domain is performed. The Euclidian's algorithm, $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)}$, is applied to the matrices corresponding to each domain. Once the matrix calculations are performed for this scenario, it can be observed that the Management domain is at 30% security, IT domain is at 31.08%, User domain is at 38.65% and Mobile Device is at 20.6% as per security assessment calculations. Figure 4 shows an example of IT domain calculation.



IT DOMAIN

$d(C,R) = \sqrt{[Tr((C-R)(C-R)^T)]} = \sqrt{30} =$ **5.47**

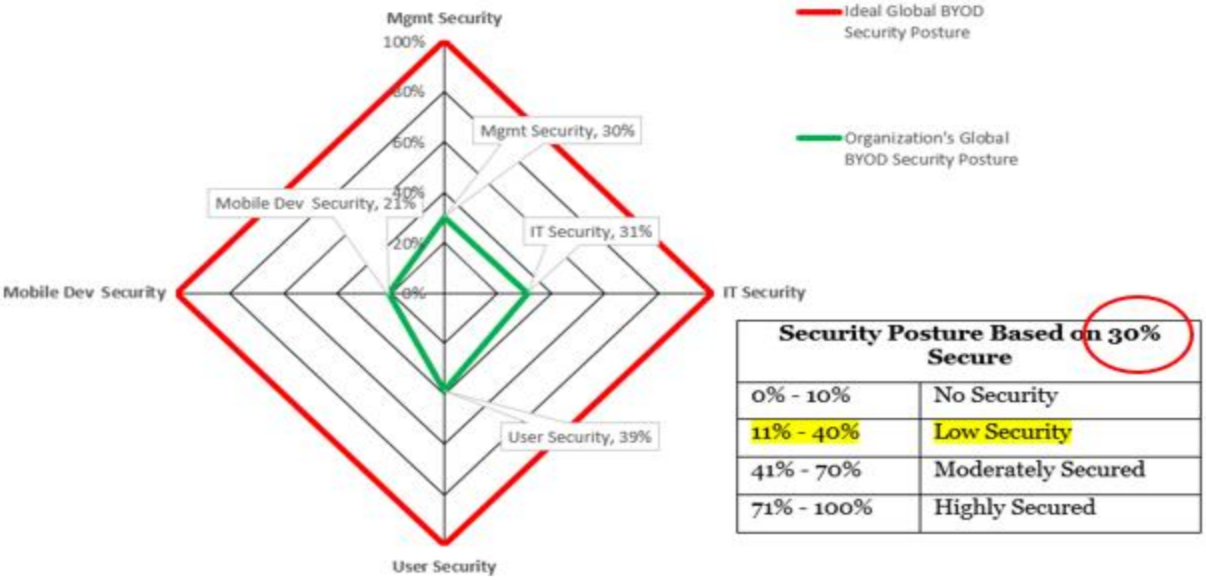
If 7.937 represents 100% insecure, then

5.47 represents (100*5.47)/7.937= **68.9% insecure**

or **31.08% secure**

Figure 4. LOW Security Posture Scenario: Security % Calculation for IT Domain

Model granularity at the organizational/global level. Figure 5 shows the graphical representation of the domains' findings. The average of these findings gives the organization's (global) % security posture, which, for this scenario is 30%. Using the range table shown in Figure 5, the overall security posture falls within the values corresponding to low security.

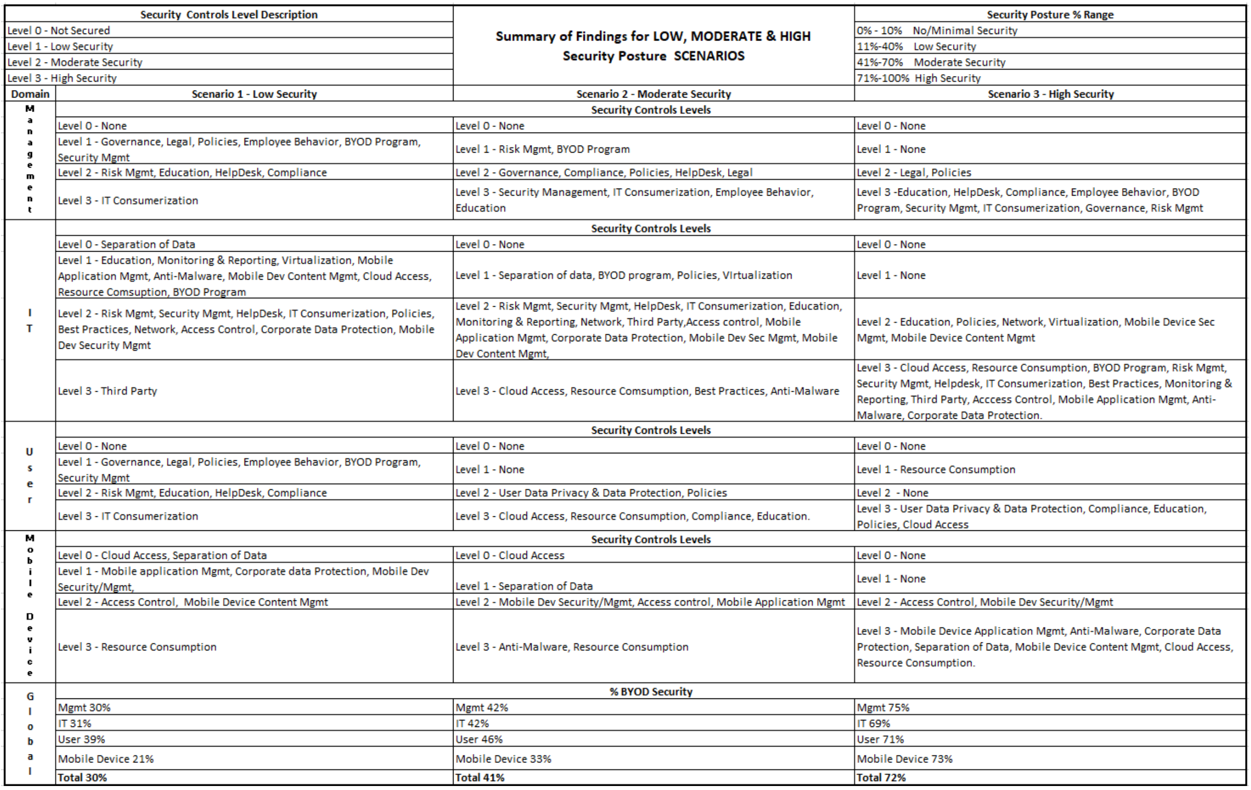


Security Posture Based on 30% Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

Figure 5. LOW Security Posture Scenario: Security % - Global

Scenarios 2 & 3 – Moderate and High Security Posture with Respect to BYOD

As with Scenario 1 described above, the same process, analysis, calculations and graphical displays are followed for Scenario 2 (Moderate Security Posture) and Scenario 3 (High Security Posture). However, due to page limitation, the information for all three scenarios has been summarized and presented in Table 4. The four domains (Mgmt., IT, User, Mobile Device) are identified, with the corresponding findings for the security control levels for each domain's scenario. For example, for the Moderate security scenario, it can be observed that the controls for the User's Domain, corresponding to User Data Privacy & Data Protection and Policies need to be strengthened since they are at Level 2. Ideally, all security controls should be at Level 3. In addition, the overall % security posture with respect to BYOD for Scenario 2 (Moderate security) for the organization as a whole, is at 41% where the weakest domain is the domain corresponding to Mobile Device with a security posture of 35%.



Security Controls Level Description		Summary of Findings for LOW, MODERATE & HIGH Security Posture SCENARIOS	Security Posture % Range
Level 0 - Not Secured			0% - 10% No/Minimal Security
Level 1 - Low Security			11%-40% Low Security
Level 2 - Moderate Security			41%-70% Moderate Security
Level 3 - High Security			71%-100% High Security
Domain	**Scenario 1 - Low Security**	**Scenario 2 - Moderate Security**	**Scenario 3 - High Security**
Management	**Security Controls Levels**		
	Level 0 - None	Level 0 - None	Level 0 - None
	Level 1 - Governance, Legal, Policies, Employee Behavior, BYOD Program, Security Mgmt	Level 1 - Risk Mgmt, BYOD Program	Level 1 - None
	Level 2 - Risk Mgmt, Education, HelpDesk, Compliance	Level 2 - Governance, Compliance, Policies, HelpDesk, Legal	Level 2 - Legal, Policies
	Level 3 - IT Consumerization	Level 3 - Security Management, IT Consumerization, Employee Behavior, Education	Level 3 -Education, HelpDesk, Compliance, Employee Behavior, BYOD Program, Security Mgmt, IT Consumerization, Governance, Risk Mgmt
IT	**Security Controls Levels**		
	Level 0 - Separation of Data	Level 0 - None	Level 0 - None
	Level 1 - Education, Monitoring & Reporting, Virtualization, Mobile Application Mgmt, Anti-Malware, Mobile Dev Content Mgmt, Cloud Access, Resource Comsuption, BYOD Program	Level 1 - Separation of data, BYOD program, Policies, VIrtualization	Level 1 - None
	Level 2 - Risk Mgmt, Security Mgmt, HelpDesk, IT Consumerization, Policies, Best Practices, Network, Access Control, Corporate Data Protection, Mobile Dev Security Mgmt	Level 2 - Risk Mgmt, Security Mgmt, HelpDesk, IT Consumerization, Education, Monitoring & Reporting, Network, Third Party,Access control, Mobile Application Mgmt, Corporate Data Protection, Mobile Dev Sec Mgmt, Mobile Dev Content Mgmt,	Level 2 - Education, Policies, Network, Virtualization, Mobile Device Sec Mgmt, Mobile Device Content Mgmt
	Level 3 - Third Party	Level 3 - Cloud Access, Resource Comsumption, Best Practices, Anti-Malware	Level 3 - Cloud Access, Resource Consumption, BYOD Program, Risk Mgmt, Security Mgmt, Helpdesk, IT Consumerization, Best Practices, Monitoring & Reporting, Third Party, Acccess Control, Mobile Application Mgmt, Anti-Malware, Corporate Data Protection.
User	**Security Controls Levels**		
	Level 0 - None	Level 0 - None	Level 0 - None
	Level 1 - Governance, Legal, Policies, Employee Behavior, BYOD Program, Security Mgmt	Level 1 - None	Level 1 - Resource Consumption
	Level 2 - Risk Mgmt, Education, HelpDesk, Compliance	Level 2 - User Data Privacy & Data Protection, Policies	Level 2 - None
	Level 3 - IT Consumerization	Level 3 - Cloud Access, Resource Consumption, Compliance, Education.	Level 3 - User Data Privacy & Data Protection, Compliance, Education, Policies, Cloud Access
Mobile Device	**Security Controls Levels**		
	Level 0 - Cloud Access, Separation of Data	Level 0 - Cloud Access	Level 0 - None
	Level 1 - Mobile application Mgmt, Corporate data Protection, Mobile Dev Security/Mgmt,	Level 1 - Separation of Data	Level 1 - None
	Level 2 - Access Control, Mobile Device Content Mgmt	Level 2 - Mobile Dev Security/Mgmt, Access control, Mobile Application Mgmt	Level 2 - Access Control, Mobile Dev Security/Mgmt
	Level 3 - Resource Consumption	Level 3 - Anti-Malware, Resource Consumption	Level 3 - Mobile Device Application Mgmt, Anti-Malware, Corporate Data Protection, Separation of Data, Mobile Device Content Mgmt, Cloud Access, Resource Consumption.
Global	**% BYOD Security**		
	Mgmt 30%	Mgmt 42%	Mgmt 75%
	IT 31%	IT 42%	IT 69%
	User 39%	User 46%	User 71%
	Mobile Device 21%	Mobile Device 33%	Mobile Device 73%
	Total 30%	**Total 41%**	**Total 72%**

Table 4. Summary of Findings for Low, Moderate, and High Security Scenarios

Conclusion

The BYOD paradigm may continue for some time as corporations and users find a balanced solution, where corporate-data protection and employees' personal satisfaction can co-exist in a secure fashion. However, corporations need to understand all the vulnerabilities and security risks introduced when BYODs are allowed, and thus the need to have BYOD security measures in place in order to mitigate risks and prevent data leakage/exposure.

In addition to providing security awareness with respect to BYOD, this paper has described current modalities, such as frameworks, checklists and best practices, to secure BYOD environments. It discussed a set of BYOD security requirements (Ratchford and Wang 2019) used as base for a comparative analysis among current approaches to BYOD security. The comparison includes a novel design science artifact, BYOD-Insure, which aims to provide organization with the means to assess and enhance their BYOD security posture. Based on our research, the comparative analysis showed that BYOD-Insure meets all the BYOD security requirements presented in this paper, while the existing modalities discussed do not. The utility of BYOD-Insure is demonstrated through the presentation of descriptive scenarios (Hevner et al. 2004) to reflect low, moderate, and high security postures for organizations. For a given organization, BYOD-Insure identifies vulnerabilities and suggests security controls. Other existing modalities, as identified in this research, provide general information.

This research has theoretical and practical implications. While the research contributes to the body of knowledge with respect to BYOD security, the design of the model is based on a non-ambiguous process suitable for further expansion of domains and modification of security controls. Theoretically, the basic concepts of this model can be applied to other types of assessments. Once the model is automated, its use in industry is beneficial to organizations that aim to mitigate the inherent risks of BYOD. Frameworks, checklists, and best practice documentation provide general information, whereas BYOD-Insure provides a level of granularity individualized to the organization.

The model in the current state is limited to manual process and computation. It is also limited to the security controls identified at the time of the research. Future work includes model automation through the design of a database and logic implementation with an appropriate programming language. In addition, the security controls can be revised and expanded as new technologies, ongoing risks, and new BYOD security risks emerge.

REFERENCES

Absalom, R. 2012. "International Data Privacy Legislation Review: A Guide for Byod Policies," *Ovum Consulting, IT006* (234), pp. 3-5.

Abubakar Garba, B., Murray, D., and Armarego, J. 2017. "A Systematic Approach to Investigating How Information Security and Privacy Can Be Achieved in Byod Environments," *Information and Computer Security* (25:4), pp. 475-492.

Alotaibi, B., and Almagwashi, H. 2018. "A Review of Byod Security Challenges, Solutions and Policy Best Practices," *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6.

Bello Garba, A., Armarego, J., and Murray, D. 2015. "Bring Your Own Device Organizational Information Security and Privacy," *ARPN Journal of Engineering and Applied Sciences* (10:3), pp. 1279-1287.

Casola, V., Mazzeo, A., Maxxocca, N., and Vittorini, V. 2007. "A Policy-Based Methodology for Security Evaluation: A Security Metric for Public Key Infrastructures," *Journal Of Computer Security* (15:2), pp. 197-229.

Citrix Systems, I. 2012. "Best Practices for Making Byod Simple and Securre," *White Paper*).

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. 2014. "Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap," *Journal of Information Systems* (28:1), pp. 209-226.

Disterer, G. 2013. "Iso/Iec 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security* (Vol.04No.02), p. 9.

Fenz, S., and Ekelhart, A. 2009. "Formalizing Information Security Knowledge," in: *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*. Sydney, Australia: ACM, pp. 183-194.

Garba, A. B., Armarego, J., and Murray, D. 2015. "A Policy-Based Framework for Managing Information Security and Privacy Risks in Byod Environments," *International Journal of Emerging Trends & Technology in Computer Science* (4:2), pp. 189-198.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS quarterly* (28:1), pp. 75-105.

Insights, G. M. 2016. "Bring Your Own Device (Byod) Market Size Worth Usd 366.95 Billion by 2022,").

ISACA. 2016. "Is Audit/Assurance Program for Byod," *Retrieved from www.isaca.org*).

Ogie, R. 2016. "Bring Your Own Device: An Overview of Risk Assessment," *IEEE Consumer Electronics Magazine* (5:1), pp. 114-119.

Ratchford, M., Wang, P., and Sbeit, R. O. 2018. "Byod Security Risks and Mitigations," in *Information Technology-New Generations*. Springer, pp. 193-197.

Ratchford, M. M. 2018. "Byod: A Security Policy Evaluation Model," in *Information Technology-New Generations*. Springer, pp. 215-220.

Ratchford, M. M., and Wang, Y. 2019. "Byod-Insure: A Security Assessment Model for Enterprise Byod," *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*: IEEE, pp. 1-10.

Romer, H. 2014. "Best Practices for Byod Security," *Computer Fraud & Security* (2014:1), pp. 13-15.

RSA. 2016. "2016: Current State of Cybercrime,").

Shumate, T., and Ketel, M. 2014. "Bring Your Own Device: Benefits, Risks and Control Techniques," *IEEE SOUTHEASTCON 2014*, pp. 1-6.

Wang, Y., Streff, K., and Raman, S. 2012. "Smartphone Security Challenges," *Computer* (45:12), pp. 52-58.

Wang, Y., Wei, J., and Vangury, K. 2014. "Bring Your Own Device Security Issues and Challenges," *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*: IEEE, pp. 80-85.

Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., and Grant, G. 2020. "Determinants of Intention to Paricipate in Corporate Byod-Programs: The Case of Digital Natives," *Information Systems Frontiers*:22), pp. 203-219.

Zahadat, N., Blessner, P., Blackburn, T., and Olson, B. A. 2015. "Byod Security Engineering: A Framework and Its Analysis," *Computers & Security* (55), pp. 81-99.