A Bring Your Own Device Risk Assessment Model

Oonge S. Omboga *soonge@maseno.ac.ke*
School of Computing Department of Information Technology
Maseno University
Maseno, P.O. Box 333-40105, Kenya

Muhambe, T. Mukisa *muhambe@maseno.ac.ke*
School of Computing Department of Information Technology
Maseno University
Maseno, P.O. Box 333-40105, Kenya

Ratemo, M. Cyprian *makiya@kisiiuniversity.ac.ke*
Department of Information Technology
Kisii University
Kisii, P.O. Box 408 – 40200, Kenya

Abstract

Bring Your Own Device (BYOD), a technology where individuals or employees use their own devices on the organization's network to perform tasks assigned to them by the organization has been widely embraced. The reasons for adoption are diverse in every organization. In spite of the security control strategies implemented by these organizations to safeguard their information resources, there has been an upsurge in information security breaches as a result of existing vulnerabilities in these systems and the legacy systems in use. Various approaches have been employed to deal with security challenges in BYOD, but according to literature, risk assessment has proved to be the first key step towards improving security of the BYOD environment in an enterprise. Risk assessment models have been proposed by various researchers, although, most are largely influenced by the degree of technological advancement and utilization as well as the working cultures within institutions. The existing models were largely developed in technologically advanced countries and thus do not fit well in developing countries. This study sought to develop flexible BYOD risk assessment model that can be adopted by varied institutions to secure their information resources. The study was carried out in Five (5) purposively selected state universities in Kenya. The research adopted a mixed research design approach with mixed sampling technique utilized to select the participants. Reliability and validity of data collection tools were evaluated and recommended by IT security and network experts. The qualitative and quantitative data was collected by interviewing experts and administering a questionnaire to sampled participants. The developed model was validated both statistically and by experts. The findings revealed that threats and vulnerabilities contributed to 39.9% and 69.2% respectively to the risk of the BYOD environment while Data Encryption (DE) and Software Updates (SU) came out strongly as intervening variables which have a major impact on the relationship between the dependent and independent variables.

Keywords: BYOD, Risk Assessment, Risk Assessment Models, Information Security.

1. INTRODUCTION

Information technology (IT) has progressed from being a commodity service provider to a strategic asset in the current business operations. IT has become a means to achieve greater efficiency and productivity [1], while the use of cloud services has emerged as a popular solution by institutions providing cheap and easy access to externalized IT resources. These resources are commonly accessed by user owned devices [2] with a growing phenomenon where companies allow employees to perform the assigned tasks on their personal devices. This is

popularly referred to as BYOD and defined by [3], as an alternative strategy that allows employees, business partners and other users to use personally selected and purchased client tablets/ e-Readers, smart phones and other devices to execute enterprise applications, access data and do personal stuff while on the organizational network.

BYOD was first introduced in 2009 by Malcolm Harkins, after realizing an increased need by employees to use their own mobile devices in the workplace [4]. Organizations, including enterprise, higher education and healthcare embraced BYOD to tap to a wide range of benefits that comes from the workforce or end-users being able to access corporate/managed resources on their own devices. According to a survey by Cisco Networks [5] 85 percent of organizations allowed some form of BYOD on their institutional network. Higher academic institutions like other organizations have embraced BYODs' for a wide array of purposes, which [6] classified into seven main functional areas; administration, collaborative, interactive, referential, location aware, data collection and microworld.

The 21st century student and end-user in general, bring along multiple devices they own to university with high expectation that universities will avail or allow them download the resources needed on those very devices to accomplish their work or assignments while in college. Meanwhile, the learning institutions have had to find innovative ways of making campus-based learning resources available not only off-campus, but on non-managed, user owned devices too. The COVID-19 pandemic has rapidly accelerated the need for BYOD in universities with off-campus access to IT resources now becoming the norm [7].

Use of BYOD tags along many benefits that include globalization, cheaper, easier, quicker and more efficient borderless communication, portability, productivity and time-to-work flexibility [8]. Technologies like Virtual Private Networks (VPNs), Voice over Internet Protocols (VoIPs), virtual meetings, cloud technology, and other work collaboration tools are now into heavy use to enable remote working and communication [5]. This has led to an explosion of personal devices with the most modern technologies accessing work networks remotely [9]. The influx of the diverse sets of devices on the network weakens the information security defenses inviting information security risks to the very assets that need protection [10].

The main objective of this study was to develop a cheaper, ease to use BYOD risk assessment model for limited budget organizations. To develop the model, the researcher explored the BYOD-related risks, assessed the existing risk assessment models and adopted some optimal variables from the existing models. The study's intention was to help institutional decision makers to understand the implications of introducing BYOD in their institutions and the effective way to address the identified risks and finally bridge the theoretical gap in the subject.

1.1 Approach of The Study

This study began with a review of the pertinent literature in order to identify risks related to the introduction of the BYOD concept in institutions of higher learning. An analysis of the risk assessment models from literature were evaluated to establish suitable variables that can be borrowed specifically for BYOD in an open academic environment. The developed risk assessment model was tested in two different learning institutions to assess its capability and efficacy.

2. RELATED WORK

The education sector in developing countries just like their developed counterparts hold vast amounts of valuable data that includes student and staff information, partners' information, alumni databases, and highly valuable research data [11] however studies posit that universities are inadequately prepared to protect their informational resources [12]. This is majorly because universities often work with legacy systems that are supported by teams that are not equipped to deal with the evolving sophisticated attacks.

BYOD adoption in such institutions bring along major information security concerns surrounding the software, hardware, deployment and technical aspects as outlined by [13]. Most academic institutions implement BYOD with little or poorly crafted policies [14] posing unexpected information security threats through the devices and the applications running on them. Among the major concerns to the institutions are privacy of information both on the user and the institution devices, decisions on device enrolment, licensing evaluation, security policy and compliance, education and security training [15].

Higher learning institutions who adopted BYOD have been valuable targets by cybercriminals. The threats and cyber-attacks go beyond loss of personally identifiable information and may include institutional information, operational, reputational, and/or financial impacts. Research shows that in the year 2020, 54% of UK universities reported a data breach to the ICO (Information Commissioner's Office) with 86 universities admitting serious shortcomings in their ability to prevent data breaches [16] [17]. Hacking, malware and unintended disclosures were the most commonly reported security breaches within institutions [18] [19]. Attacks such as eavesdropping, theft of sensitive information through social engineering, malicious software infection, theft and intrusion of mobile devices have also been on the rise [20] [21]. [22], affirms that the top risks for educational institutions include phishing, harassment, ransomware, IP theft piracy, account hacking, and denial of service attacks. It is further noted that majority of members of the management within these institutions do not know what these attacks are and are not aware of the risks that each pose to their institutions.

In a study done by [23], issues related to security breaches of data due to adoption of BYOD were identified as the major challenges facing institutions of higher learning in South Africa. The study further reports that unauthorized access to sensitive data stored on mobile devices and on the institution's network, attacks from malicious software and impersonation are a common feature. BYOD in most Ethiopian higher learning institutions was adopted without considering transparent policies, security and privacy issues, device and application management tools, end-user security/privacy awareness and training [24]. Further, it is noted that the excessive freedom to access the network has posed major security and privacy risks and bandwidth constraints. In Kenyan higher learning institutions, [20] established that user security unawareness was the leading IT security challenge followed closely by the varied device platforms challenges. The author further stated that loss of device control and lack of visibility of devices on the institutions' networks make them susceptible to intrusion, data leakage, and device and data theft. Viruses and malware are common among the student devices as they keep sharing information without minding the status of the other device before connection [17] [18] [25]. The human aspect of security in BYOD plays a big role. As cited by [17], humans are a major threat to information security due to their negligence and sometimes deliberate actions. The non-compliance behavior of humans in a BYOD environment may result to data leakages causing major institutional losses [24]. It is further stated that one in every five institutions suffers from a security breach involving a mobile device connecting to malicious hotspots and malware [17] [25].

While it is true that making institutional data available and accessible to students and employees can contribute to productivity, literature clearly shows that it poses risks that can lead to major losses. According to [26], controlling different devices and platforms which connect across multiple networks is a potential cybercriminal minefield that universities are keen to avoid. There are also concerns around who takes responsibility for data loss and replacing the device in the event of it being lost, stolen or malfunctioning.

Allowing access to university systems, and services through network connections on unchecked and unmanaged machines carries risks. If the endpoints are infected with malware, there is a chance for this to further infect university systems. Furthermore, users with malicious intentions present a higher risk to systems that allow BYOD devices if not managed properly.

It is evident that most institutions that adopt BYOD are exposed to emerging IT security challenges. These security challenges are varied and dynamic in nature. For this reason, [27]

recommends that establishing challenges due to BYOD adoption should not be a onetime activity but a continuous process. It therefore becomes necessary that institutions should continuously take precautions to prevent and mitigate information security breaches through the adoption of risk assessment. Institutions that do risk assessments understand better where their strengths and weaknesses are when it comes to ensuring the security of their sensitive data. It is further noted that risk assessment exposes the efficiency of the organization's controls, determines risk factors, detects vulnerabilities and uses them in crafting detailed plans and solutions that offer options of how to alleviate them.

There are various security assessment types [28]. Pen Testing (penetration testing) aims to simulate an attacker to see how well security measures of the organization work [29] [30], risk assessment [31] that detects risks and potential losses that can be caused by them and vulnerability assessment [32] whose aims is to identify vulnerabilities of the security measures and offers solutions to alleviate them. This paper develops a BYOD risk assessment model for open institutions with limited budgets by borrowing concepts of the existing risk assessment models combined with other factors from literature review.

2.1 Risk Assessment Models

Broadly [33] [34] divide risk assessment models into qualitative and quantitative. Quantitative models use measurable objective data to determine; asset value, probability of loss, and accompanying risk(s) while qualitative methods use a relative measure of risk or asset value based on ranking or separation into expressive categories such as low, medium, high; not important, important, very important; or on a Likert scale. [35] [36] compare the two model types by highlighting the advantages of each and expresses need to integrate the advantages of each in the risk assessment process.

To establish the existing risk assessment models, articles were identified by searching relevant databases, such as ERIC, JSTOR, SciNet, EBSCOhost, and Google Scholar. The most recent and relevant journal papers were selected with most of them having been published in less than seven years. A comparison of the most recent and supported models was done. Only models that explicitly defined and decomposed risks, as well as suggest either taxonomy of factors or a formula for computing risks based on these factors were selected. The literature search identified twenty-five risk assessment models in existence [37] [38] [39]. For the purpose of this study, the models were classified in four categories as shown in table 1. This first selection iteration excluded some models from the study based on essential model features; if the model is a method or guideline, if the model identifies Information System (IS) risks or not, if it has current documentation and if it has regular reviews.

Name of risk assessment model	Method or Guideline?	Identifies IS Risks	Documentation?	Last Review	2nd Iteration?
Octave	Method	Yes	Free	Up-to-date	Yes
Mehari	Method	Yes	Free	Up-to-date	Yes
MAGERIT	Method	Yes	Free	Up-to-date	Yes
IT-Grund schutz	Standard and Method	Yes	Free	Up-to-date	Yes
EBIOS	Method	Yes	Free	Up-to-date	Yes
NISTSP800-30	Guideline	Yes	Free	Up-to-date	No
FAIR	Method	Yes	Free	Up-to-date	Yes

Name of risk assessment model	Method or Guideline?	Identifies IS Risks	Documentation?	Last Review	2nd Iteration?
TARA	Method	Yes	free	Up-to-date	Yes
RISK RANKER	Method	Yes	Free	Up-to-date	Yes
CRAMM	Method	Yes	Expensive	Up-to-date	No
MIGRA	Method	Yes	Expensive	Up-to-date	No
MAR	Guideline	No	Free	Up-to-date	No
ISAMM	Method	Yes	Unavailable	N/A	No
GAO/AIMD-00-33	Guidelines and Case Studies	Yes	Free	N/A	No
IT System Security Assessment	Guideline	Yes	Unavailable	N/A	No
MG-2 and MG-3	Guideline	Yes	Unavailable	N/A	No
Security Risk Management Guide	Guideline	Yes	Unavailable	N/A	No
Dutch A&K Analysis	Method	Yes	Unavailable	Obsolete	No
MARION	Method	Yes	Unavailable	Obsolete	No
Austrian IT Security Handbook	Guideline	Yes	Unavailable	Up-to-date	No
Microsoft Security risk management guide	Guideline	Yes	Free	Up to date	No
Risk IT	Framework	No	Available	N/A	No
BYODRAM	Method	Yes	unavailable	obsolete	No
CVSS	Method	yes	Yes	Up to date	Yes

TABLE 1: First Selection of the Risk Assessment Models.

The criteria reduced the initial collection of models to 9 models. The models with a “yes” at the first iteration column were selected for further consideration where the study subjected them to another set of standards suggested by the author. The five (5) selection criteria applied are described below:

i. Complexity and effort skills and preparation needed to implement the model. Using the criteria; Little preparation needed, preparation needed, extensive preparation and effort needed.
ii. The risk assessment approaches; e.g. self-assessment, interviews, workshops).
iii. Supporting tools; Free tool, paid tool, no supporting tool but has supporting documentation (e.g. worksheets, questionnaires, forms)
iv. Origin/source of the tool e.g. Academic; Governmental; Commercial.

The second iteration, considering the four characteristics cited, dropped six of the nine selected models from the first iteration. The three remaining models; OCTAVE, IT-Grund schutz and CVSS with their characteristics are described in table 2.

Model	Description	Strengths	Drawbacks
OCTAVE	- Provides a standardized approach to risk-driven and practice-based information security evaluation	For risk-based infosec. strategic assessment and planning Methodology is self-directed and easily modified. Used as the foundation risk assessment component or process for other risk method Thorough and well-documented. Freely available Encourages corroboration between various company groups.	The process requires a significant time commitment, and the documentation is large and vague (Joshi, 2014). There are planned updates to OCTAVE that may impact its downsides, but the exact effects are currently unknown. Fairly Complex Framework Qualitative not quantitative risk model
IT-Grund schutz	To identify and implement computer baseline security measures within an organization	is based on the risk analysis approach that focuses on threat identification, assigning likelihood of occurrence and selection of suitable information security measures and their respective implementation costs	Complexity and voluminous nature which necessitates the need for more people to implement. A hindrance to most 'developing' institutions. [33][34][35]
CVSS	free, open, quantitative risk assessment	Identifies and scoring underlying vulnerabilities Is suited for organizations, industries and governments Assessment and quantification of the impact of software vulnerabilities Standardized vulnerability scores, A numerical score that indicates the severity of the vulnerability on the assets; a low , medium, high or critical	Does not clearly provide a method for aggregating individual scores across system Unsuitable for managing IT risk because it does not consider mitigation strategies CVSS assumes that vulnerabilities are independent which is not the case

TABLE 2: Strengths and Drawbacks of the Selected Risk Assessment Models.

This study borrowed the flow of activities from the three risk assessment models to help come up with the BYOD risk assessment model. The study adopted the strengths of each of the three risk assessment models; OCTAVE, IT-Grundschutz and CVSS to enable the research not only to become simple to implement and easy to use, but also captures both qualitative and quantitative approaches in accomplishing its functions, hence, preferred in varied environments and good especially in a limited resource BYOD environment.

OCTAVE's qualitative approach on threat and infrastructure vulnerabilities identification as highlighted by [40] was used in the threats and vulnerabilities identification process. [40] proposes IT-Grund schutz, model based on the risk analysis approach that focuses on threat identification, assigning likelihood of occurrence and selection of suitable information security measures and their respective implementation costs to contribute immensely to the adoption of a risk based risk assessment model development. The quantitative aspect of risk assessment was adopted from CVSS model that uses the numerical score approach that indicates the severity of the vulnerability on the assets which helps develop a low, medium, high or critical criteria for risk ranking. The BYOD risk assessment model will help prioritize risks by their financial impacts and at the same time involve people who are not experts in the information security field to perform regular risk assessments [18].

2.2 Conceptual Model Development

Literature review identified threats that are common in the higher learning institutions from various countries. It was however necessary for the study to classify the threats into suitable categories. Students and staff using own devices may find themselves losing the Device through theft, forgetting or misplacement of the device. Thus it is difficult to know who finds it and what will happen to the sensitive data in the device. Theft of data, loss or destruction of BYOD asset, fraud, unauthorized access to the network services, infection with malicious code, disclosure of someone's personal data and identity theft [41] [42] [43] were classified together as Malicious Human Attacks (MA).

Downloading and installing third party applications to user (students and staff) devices while disregarding security concerns [44], exposing the institutional data to security threats when connecting to unsecured networks or browsing malicious WebPages [45], not installing third party security software on devices [41] and forgetting guidelines set by policies or at times being unaware of existing policies were classified together as Lack of User Security Knowledge (LDSKU). Another institutions of learning biggest concerns their employees' and students' lack of security awareness [45]. It sighted lack of security awareness amongst students and staff, lack of skilled IT security staff within the institution have been classified together as lack of user security knowledge.

Illegal access to information by Bluetooth access, free Wi-Fi access, and open hot spots access was classified as wireless network attacks by the mobile devices (WIA).

According to [46], a security survey conducted by Google indicated that as many as 65% of people reuse the same password for multiple or all accounts. Students and staff alike have a tendency of sharing passwords, creating weak passwords, or reusing passwords across devices or for a long time leaving the network they access vulnerable to intrusion and attacks. These vulnerabilities were classified as "Poor Password Management" (PPMGT).

Poor System Configuration (PSYSCON) consisted of; unpatched security flaws in server software, enabled or accessible administrative and debugging functions, administrative accounts with default passwords, SSL certificates and encryption settings that are not properly configured [47]. These vulnerabilities were realized from higher learning institutions that were inadequately prepared to protect themselves due to the lack of competent information security experts.

Improper physical access controls into the institutions legacy system, improper maintenance procedures or non-adherence to security identification procedures were grouped as Weak Authentication Procedures (WA).

Learning institutions can reduce malware attacks through Keepings the devices operating system and social network software's up to date to ensure protection against most mobile security threats. Choosing mobile security software from a trusted providers and keeping it up to date. Installing firewall to provide with digital threats and to allow online privacy. Insisting on use of passcode on phone to reduce chances of compromising information whenever loss or physical

theft of a mobile device occurs. Downloading apps from official app stores that vet the apps they sell employ mitigating feature(s) in BYOD devices such as on device encryption as well as certificates and tokens. Virtual Private Networks (VPNs) and application containers separate user applications and data from corporate ones, and device virtualization [48] [49] [50]. Strong encryption could also mitigate wireless network attacks and data transmission vulnerabilities. Use of Mobile Device Manager (MDM) and BYOD policy could minimize poor system configuration while training all the users on BYOD policy security and password management is important for user knowledge boosting.

To determine the effects on the mitigation solutions, a selected line of variables was scrutinized after allocating them causal relationships and assigned as intervening variables, and their effects hypothesized and tested. Table 3 summarizes the three categories of variables and their respective measurable attributes as used in the study.

Item	Model Construct	Measure Attributes	Measurement Scale
Independent variable (threats)	Malware Threat Attacks (MTA)	Malicious Actors, Malicious Applications, Malwares,	Ordinal
	Malicious Human attacks (MA)	Malicious Users / Attackers, Break-in, Physical access Device Loss/theft Data loss/leakage through sharing, data breach, media corruption Device malfunction Improper decommissioning	Ordinal
	Device loss or stolen		Ordinal
	Lack of device Security knowledge (LDSKU)	IT Support, IT training	Ordinal
	Wireless Network attacks (WIA)	Bluetooth access, Free Wifi access, Free Hot sports.	Ordinal
Independent Variable (Vulnerabilities)	Poor Password Management (PPMGT)	No secure / strong passwords, Poor password management Shared passwords, weak or stolen passwords, reuse passwords	Ordinal
	Data Transmission Vulnerabilities (IDT)	No encryption, Jailbroken or Rooted OS, Untrusted Applications, open channels like Bluetooth, using unsecured public wireless network, forget to apply security filters or policies	Ordinal
	Poor System Configuration (PSYSCON)	Jailbroken or rooted OS, Vulnerable Applications, Malicious Applications Unpatched system & applications Super user or Admin Account Privileges	Ordinal
	Weak Authentication Protocol(WA)	Improper Physical controls, Improper maintenance Procedures or Non Adherence to Procedures	Ordinal
	Lack Of Device security Knowledge of user (LDSKU)	No proper compartmentalization, Admin Privilege misuse. employees' lack of security awareness,	Ordinal
	System Flows	System flaws, programming errors , configuring security settings, use of custom keyboard extensions, Insecure inter-process communication (IPC).	Ordinal

	Malware Attacks (MA)	Unauthorized Modifications/ Access Lack of Antivirus software or Firewalls.	Ordinal

TABLE 3: Measurable Attributes.

2.3 The Proposed Conceptual Model

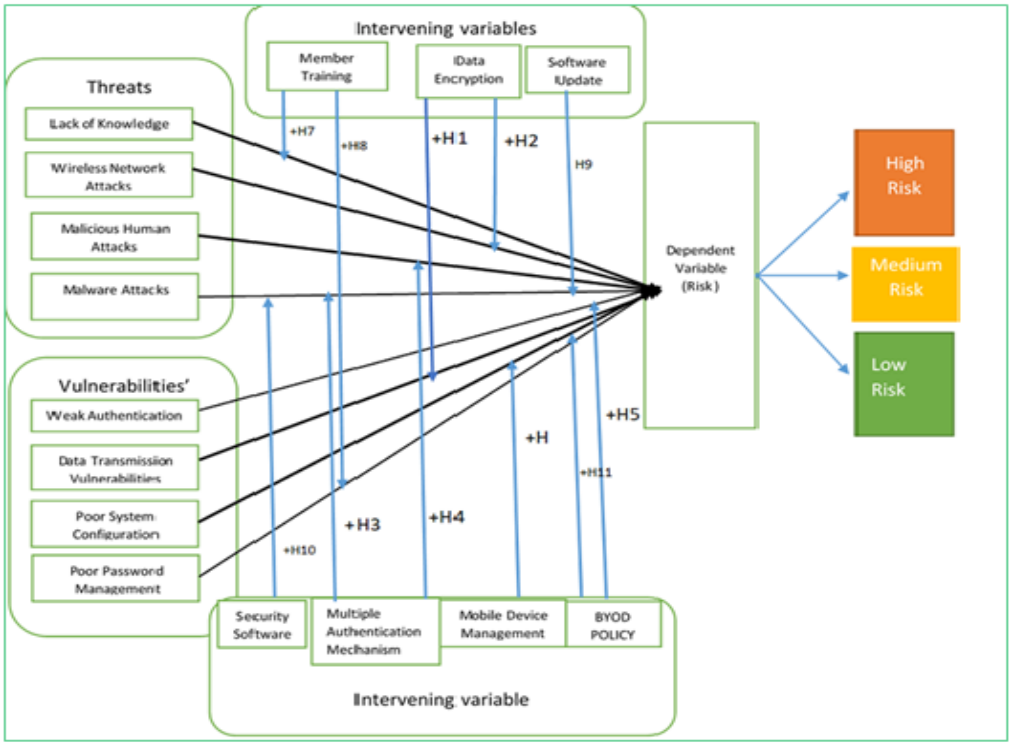

FIGURE 1: Proposed Conceptual Model.

3. METHODOLOGY

The study was carried out in five (5) of the thirty-one (31) public chartered universities in Kenya, selected by use of purposive sampling on the basis of year of establishment, information systems infrastructure and the level of BYOD adoption. Mixed sampling technique (Purposive sampling to choose participating learning institutions and simple random sampling to pick respondents in the student, teaching, non-teaching and administration cadres, to ensure each member in the set has equal chance of inclusion to guarantee representation of the sample; stratified sampling to select participants based on cadres; ICT services staff, management staff, support staff, academic staff and the students [50] [56] [57]).

A simplified formula by [58] for determination of sample size was used. The formula yielded a sample size of 400 participants for the study. As [59] puts it, there is need to add 30% of the sample to compensate for people who fail to fill the questionnaire or commit errors during the filling which topped it up to 520 participants. This study involved different carders; the university non-teaching staff, teaching staff and students. These variations prompted the researcher to add further 30% more participants so that the outcome may be more reflective of the population as cited by [59]. This settled for sample size of 699 (six hundred ninety-nine) distributed as indicated in table 5.

Carder	Carder	Sample size
University staff	Lecturers	26
	ICT staff	8
	Administrative staff	46
	Management	15
Students	Students	604
	Total	**699**

TABLE 5: Sample size on each Carder.

An online five point Likert scale questionnaire was distributed to participants who included lecturers, non-teaching staff, management and students while interviews were conducted to senior ICT officers to highlight on the readiness and impacts of BYOD adoption. Data was analyzed using SPSS version 23 and NVIVO version 12 for quantitative and qualitative statistics respectively while model validation was done using Path coefficient analysis (β) coefficient of determination also called of R2 (R square), impact value f2 and the predictive relevance also called q2 tests using SmartPLS version 3. To ensure credibility, triangulation, a method for cross-checking data from the perspective of multiple research tools was performed on the outcome of both qualitative and quantitative.

3.1 Measurement (Outer) Model Validation

Model validation was done at both construct and indicator level to establish the fitness of the variables. Normality of data was tested by calculating the skewness and Kurtosis values using SmartPLS which realized values of between greater than +1 and lesser than -1 indicating heavily skewed data, hence, better for Partial Least Square-Structural Equation Modelling PLS-SEM) other than the simple inferential statistics. Despite failing the normality test, the data passed the multi-collinearity test which is an indicator of independence between the variables used in the study.

Face validity for the research tools was done by subject experts who included; IT and information security lecturers, supervisors and peers while a review of literature helped in ensuring content validity. A successful discriminant validity matrix indicating the uniqueness of constructs was done by running a PLS algorithm using SmartPLS software and values below 0.71 were established as recommended by [60].

3.2 Structural (inner) Model Validation

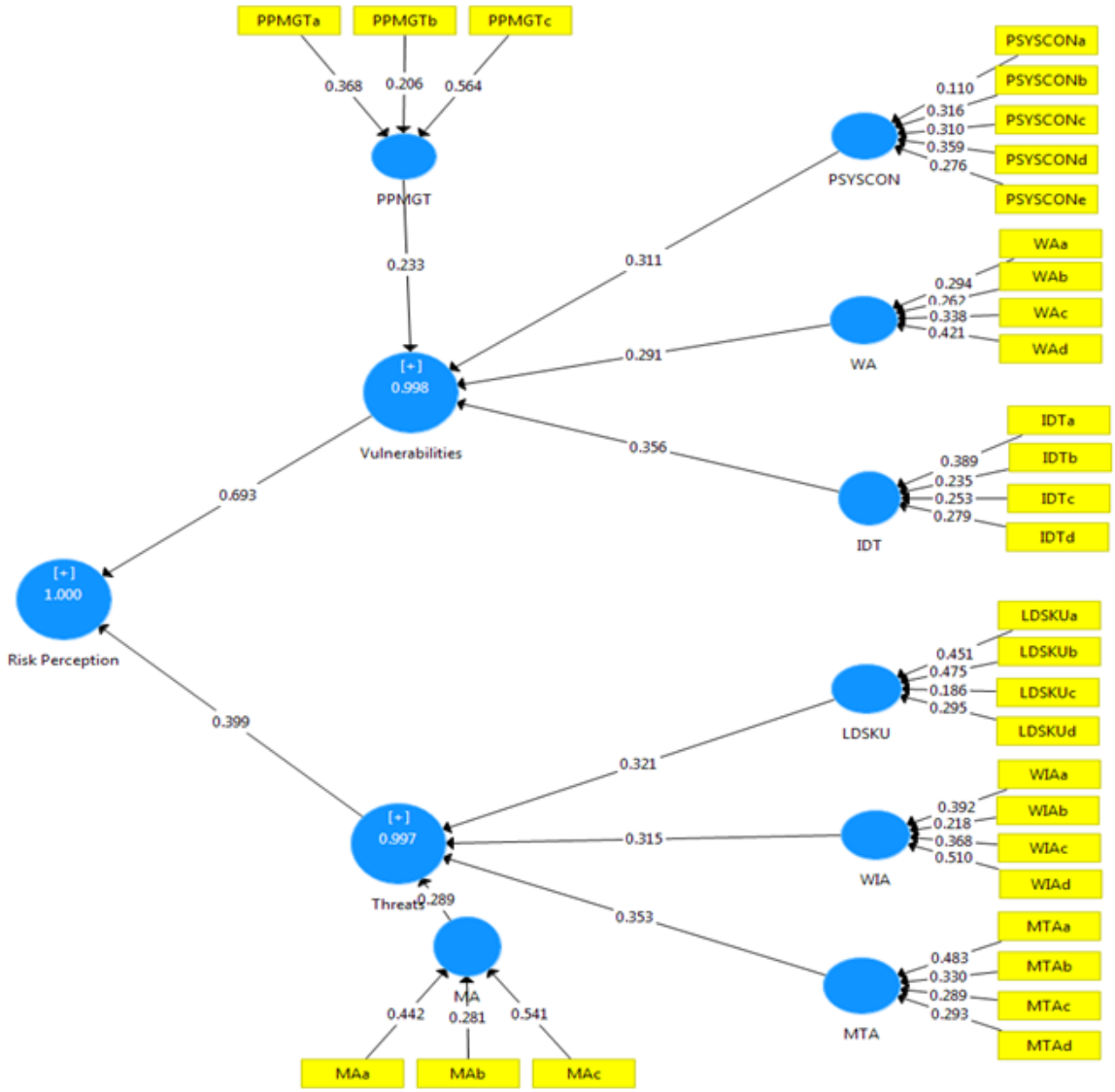

FIGURE 2: Threats and Vulnerabilities Path Diagram.

The inner model was validated using Path coefficient analysis **(β)** in figure 2 (shows significance of the indicators), coefficient of determination also called of $\mathbf{R^2}$ (R square), impact of respective exogenous variables to the endogenous variable of the model value $\mathbf{f^2}$ and the predictive relevance also called $\mathbf{q^2}$.

The path coefficients whose (values) range from 0-1 show the strength, direction and significance of the independent variables to the dependent variable. A minimum of 0.1value is expected for the path coefficients. **Figure 2** shows the strengths of indicators in their respective constructs are all above 0.1 a show of their strength. The higher the value of the indicator, the more it contributed to the respective construct.

An $\mathbf{R^2}$ (square) model test was done using SPSS software and a value of 0.275 was realized, meaning that the new model's independent variables explain 27.5% of the dependent variable which is a significant figure as supported by [60]. This means that apart from threats and

vulnerabilities, there are other major factors that contribute to the insecurity of information systems within an institution.

The effect size f^2, was calculated by running a PLS algorithm using SmartPLS while excluding a single independent variable in each case. It was realized that threats have a weak effect size of 0.007 on the dependent variable compared to a high value of 0.21 of vulnerabilities. According to [61], $f^2 \geq 0.02$, $f^2 \geq 0.15$, and $f^2 \geq 0.35$ represent small, medium, and large effect sizes, respectively, meaning that compared to threats vulnerabilities of a system contributes more to risks than threats.

The predictive power, q^2 of the structural model was calculated by running a blindfolding procedure in SmartPLS. The blindfolding procedure was conducted with a recommended omission distance of 7. Positive values greater than zero (threats=0.036; vulnerabilities=0.160) were realized indicating that the variables were well constructed and the predictive power was achieved [60].

3.3. Moderating Variables Analysis

Ten moderating variables were identified in the conceptual framework (Member training (MT), Data Encryption (DE), Software Updates (SU), Security Software (SS), Multiple Authentication Management (MAM), Mobile Device Policy (MDP) and Mobile Device Management (MDM)) hypothesized and tested, however only two had a significant impact on the relationship between the stated independent variable and the dependent variable. Data Encryption (DE) registered a path coefficient **(β)** value of -0.099 with a p-value of 0.03 (<0.05) between Insecure Data Transfer (IDT) and risk level while Software Updates (SU) had a path coefficient **(β)** value of 0.076 with a p-value of 0.024(<0.05) having an impact between Malware Attacks (MA) and risk level. The significant moderating variables were integrated into the model. Summarized in the table 6.

Moderator Variable	Causal path	Hypothesis	Path Coefficients (β)	T Statistics (|O/STDEV|)	P Values
(DE)	DE_IDT -> RISK PERCEPTION	H1	-0.099	2.173	0.03
	DE_WIA -> RISK PERCEPTION	H2	0.007	0.189	0.85
(MAM)	MAM_MA -> RISK PERCEPTION	H3	-0.035	0.75	0.453
(MDM)	MDM_MTA -> RISK PERCEPTION	H4	0	0.002	0.999
	MDM_PSYSCON -> RISK PERCEPTION	H5	0.023	0.535	0.593
(MDP)	MDP_PSYSCON -> RISK PERCEPTION	H6	0.017	0.593	0.553
(MT)	MT_LDSKU -> RISK PERCEPTION	H7	0.017	0.48	0.632
	MT_PPMGT -> RISK PERCEPTION	H8	0.045	1.22	0.223
(SS)	SS_MA -> RISK PERCEPTION	H9	0.072	1.697	0.09
(SU)	SU -> RISK PERCEPTION		0.036	0.825	0.41
	SU_MA -> RISK PERCEPTION	H10	0.076	2.259	0.024

TABLE 6: Moderating Variable Analysis.

4. THE FINAL BYOD RISK ASSESSMENT MODEL

The analysis of the causal relationships between the independent, moderating and the dependent variables resulted into the formation of a new model in figure 3. It was realized that out of the ten moderating variables, only two; Software Updates (SU) and Data Encryption (DE) had an effect between Malicious Attacks (MA) and risk and Insecure Data Transfer (IDT) and risk respectively.

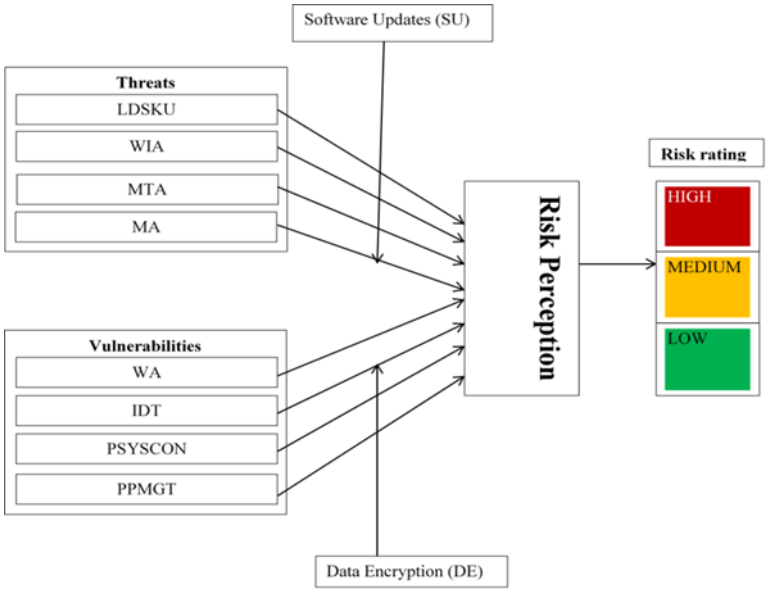

FIGURE 3: The BYOD Risk Assessment Model.

4.1 Model Calibration

The path coefficient weights (Figure 2) were used to get the decomposed variance for each construct. The decomposed variance when summed together add up to 1 (one) which was then used to award points that are used for calibration. The weights values in figure 2 are shown in column 3 of table 6. This was done by taking the individual decomposed variance of a construct divided by the total decomposed variance, multiplied by 100 and rounded to a whole number. Threats as a predictor variable contributed less than system vulnerabilities to the dependent variable, risk. From the analysis the dominant threats for BYOD environment were Insecure Data Transfers (IDT) with 14 points, and major vulnerabilities were Malicious Human Threat attacks (MTA) with 14 points also.

Predictor variable	Constructs	Weights	Decomposed variance	Percentage contribution (%)	Points awarded	Predictor variable contribution
Threats	IDT	0.356	0.144	14.4	14	**48**
	PPMGT	0.233	0.094	9.4	9	
	PSYSCON	0.311	0.126	12.6	13	
	WA	0.291	0.118	11.8	12	
Vulnerabilities	LDSKU	0.321	0.130	13.0	13	**52**
	MA	0.289	0.117	11.7	12	
	MTA	0.353	0.143	14.3	14	
	WIA	0.315	0.128	12.8	13	
	Total	**2.469**	**1.000**	**100**	**100**	**100**

TABLE 7: Model calibration.

The calibration table assisted in assigning values to specific questions that were used in risk assessment as shown in table 8.

4.3 Final BYOD Risk Assessment Model Calibration

Using the points awarded column in table 6, calibration for individual indicators was done. The path diagram in figure 2 had weights for each indicator (question in the questionnaire). To get a score for an individual question in the final model, total scores for the indicators in each construct was done. Then a percentage of each indicator was sought which helped to realize the number of points to be awarded from the assigned points column in table 8.

Factor	R2	Assigned points	Indicators	Max. score	Verdict options	Item Score Range
IDT	0.144	14	BYOD devices used to carry university data and information around.	5	Never allowed	5
					Rarely allowed	4
					Occasionally	3
					Often allowed	2
					Always allowed	1
			BYOD users save sensitive data on flash drives	3	Never allowed	3
					Occasionally allowed	2
					Always allowed	1
			BYOD users share sensitive data on social media	3	Never allowed	3
					Occasionally allowed	2
					always allowed	1
			BYOD users access Unsecured WIFI for data transfer	3	Never allowed	3
					Occasionally allowed	2
					Allowed	1
PPMGT	0.094	9	No clear password policy for access to university resources.	3	Policy exists	3
					Draft exists	2
					Not available	1
			Minimum character policy for Password enforcement	2	Policy enforced	2
					Policy exists	1
					Policy missing	0
			Password complexity enforcement	4	Fully Enforced	4
					Rarely enforced	3
					Exists	2
					Missing	1
PSYSCON	0.126	13	BYOD access configuration done	1	Access config Done	1
					Access config Not done	0
			BYOD devices monitored	4	Always monitored	4
					Often monitored	3
					Rarely monitored	2
					Not monitored	1
			Information access hierarchy implementation	4	Fully implemented	4
					Partially implement	3
					exists	2
					Not implemented	1
			Policy on Password change	4	Fully Enforced	4
					Partial enforced	3
					Exists	2
					No policy	1
WA	0.118	12	Policy on same profile concurrent access	3	Fully enforced	3
					Partially enforced	2
					Not enforced	1
			Access to network resources without configuration allowed	2	Not allowed	2
					Allowed	1
			Some university information resources accessed without a password	3	Not Possible	3
					Occasionally possible	2
					Always possible	1

Factor	R2	Assigned points	Indicators	Max. score	Verdict options	Item Score Range
			Authentication policy	4	Fully enforced	4
					Partially enforced	3
					Exists	2
					No policy exists	1
LDSKU	0.130	13	Users lax with security on their BYOD devices	4	Never true	4
					Rarely true	3
					Occasionally true	2
					Always true	1
			Users' BYOD devices left unattended	4	Never true	4
					Rarely true	3
					Occasionally true	2
					Always true	1
			Technology awareness done	2	Yes	2
					No	1
			Threats and their consequences made known to users	3	Very true	3
					True	2
					Not true	1
MA	0.117	12	Personal devices used to steal organization data	4	Not true	4
					Rarely true	3
					Occasionally true	2
					Always true	1
			Theft of BYOD devices by insiders and/or outsiders common	3	Never true	3
					Rarely happens	2
					True	1
			Virus injection to BYODs common	5	Never true	5
					Rarely true	4
					Occasionally true	3
					Often true	2
					Always true	1
MTA	0.143	14	Malicious software is a challenge	5	Never true	5
					Rarely true	4
					Occasionally true	3
					Often true	2
					Always true	1
			BYOD Devices with updated antivirus software difficult to identify	3	Not true	3
					Occasionally true	2
					Always true	1
			BYOD Devices with expired antivirus allowed to connect	3	Not true	3
					Occasionally true	2
					Always true	1
			BYOD Devices connect irrespective of their antivirus software status	3	Not true	3
					Occasionally true	2
					Always true	1
WIA	0.128	13	BYOD Users always connecting to free WIFI	3	Not true	3
					Occasionally true	2
					Always true	1
			Users able to identify rogue WIFI	2	Yes	2
					No	1
			Bluetooth always deactivated	3	Always true	3
					Occasionally true	2

Factor	R2	Assigned points	Indicators	Max. score	Verdict options	Item Score Range
					Never true	1
			Hotspot establishment	5	Always controlled	5
					Often controlled	4
					Occasionally controlled	3
					Rarely controlled	2
					Never controlled	1

TABLE 8: Calibration Table.

4.3 Testing The Proposed BYOD Risk Assessment Model

The proposed BYOD risk management model (Figure 3) was tested in order to establish an optimal approach to addressing the BYOD related risks. The elements of this model were used for posing the interview questions to the institutions ICT administrators. This was implemented by using the calibrated BYOD risk assessment model as developed in table 8. Lower final scores indicate higher risks, middle scores indicate medium risks while higher scores represent secure BYOD environments.

4.4 Model Capabilities and Limitations

In terms of its practical application, the BYOD risk assessment model is useful for conducting case studies and also in-house evaluations (i.e. internal revisions). The management and security experts of an institution are responsible for taking decisions that contribute to the institution's development, where the presented approach may be of great assistance. Since the model is simple to understand, security managers can use it as a tool to obtain information and adopt rational decisions. At the operational level, the model is useful for IT staff drafting plans and identifying critical security areas since its application allows them to obtain answers to questions that cannot be answered by conducting isolated technical or economic analyses. Such questions may, for instance, include the following: How efficient is the institution security? Is it efficient enough? How does it compare to other institutions? If there is a need for more reliable results, the model can be used in combination with other decision-making models (e.g. for establishing whether a certain measure recommended as a solution by the mode will, in fact, pay off). If an institution using the model finds that it is necessary to implement a new measure or improve the existing one, it can, for example, hereinafter use more complex performance-based earned value technique to measure technical performance for achieving planned functionality.

The main limitation of the model emanates from the development process, majorly from using a relatively small sample. The target group included experts, who are dealing with the management of information security professionally and on a daily basis. Since the development of risk assessment model relied on measuring the importance of a vast quantity of variables, the sample should have been larger in order to meet general and formal statistical requirements. When considering the fact that the levels of professional public participation in research studies related to information security is very low and that it is almost impossible to compile a list of the entire population of experts, it was decided that an interactive group assessment of criteria is sufficient for setting the foundations of the model. However, any additional use of the model for market or scientific research would most certainly require a larger sample**.**

5. CONCLUSIONS AND RECOMMENDATIONS

In conclusion, this study has established that the adoption of the BYOD phenomenon does not come free of challenges and there is no single solution for all the security challenges or universal remedy for solving all the risks and concerns related to BYOD. It is therefore imperative to introduce appropriate BYOD (e.g. security) and other specifically tailored institutional policies (e.g. employee, privacy) which can increase not only overall BYOD security but also the satisfaction and privacy of employees, thereby minimizing the overall risk for the organization. It is also a sound idea to assess the institutions systems from time to time in order to create a starting

point where the institution needs to focus their attention, and can quickly set an actionable plan to help improve security measures, and ultimately improve security posture within. In-depth information security risk assessments can give scoring metrics for the different areas of security providing the institution with a numeric baseline indicating the severity of the risk not only to help in making improvements, but also provides the ability for everyone in the institution to speak the same language about security. The assessments will provide the necessary recommendations to make immediate improvements to the score, and the overall security posture.

This study recommends automation of this model using suitable programming languages to enable the model to be readily available, easy to update, maintain and distribute to other organizations. The model should also include optimal mitigation strategies to help control the security loopholes found during assessment. The risk mitigation strategies proposed should be easy and flexible to implement for organizations that have limited budgets. Having in mind the limited sample size in this research, it is suggested that further studies are performed using a larger sample from different organizations in order to increase the generalizability of the BYOD model**.**

6. REFERENCES

[1] J. Macus, “Is BYOD Trend Fading, Technivorz,” 11 8 2015. [Online]. Available: https://technivorz.com/is-byod-trend-fading. [Accessed 11 8 2020].

[2] M. Turek, “Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research,” 3 8 2016. [Online]. Available: https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research . [Accessed 23 4 2021].

[3] R. Meulen, R. Janess., “Mobile Communication Devices by Region and Country, 4Q13 . Technical Report,” Gartner, Stamford, 2013.

[4] J. Roman, “BYOD: Get Ahead of the Risk,” Information Security Media Group, Princeton, 2012.

[5] CISCO, “Cisco Bring Your Own Device: Device Freedom Without Compromising the IT Network.,” Cisco Press, San Jose, 2012.

[6] B. Patten, “Designing collaborative, constructionist and contextual applications for handheld devices,” Computers & Education, vol. 46, no. 1, pp. 294-308, 2006.

[7] Z. Yan, “10 technology trends to watch in the COVID-19 pandemic,” 21 4 2020. [Online]. Available: https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth/. [Accessed 04 04 2021].

[8] B. Networks, 2012. [Online]. Available: https://campustechnology.com/Articles/2013/05/21/Report-85-Percent-of-Educational-Institutions-Allow-BYOD-Yet-Security-Lags-Behind.aspx . [Accessed 15 02 2021].

[9] S. Dahlstrom, “The Consumerization of Technology and the Bringing your Own Everything (BYOT) Era of Higher Education,,” education report, 2013.

[10] O. Education., “Cybersecurity Considerations for Institutions of Higher Education,” 2017. [Online]. Available: https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf. [Accessed 4 4 2021].

[11] B. Patten, “Designing collaborative, constructionist and contextual applications for handheld devices,” Computers & Education, vol. 46, no. 1, pp. 294-308, 2006

[12] K Bechkoum, “university world news,” 18 7 2021. [Online]. Available: https://www.universityworldnews.com/post.php?story=20200717134543848. [Accessed 23 4 2021].

[13] B. Maumita, “A New Business Challenge,” in Proceedings of The 5th International Symposium on Cloud and Service Computing (SC2 2015), IEEE CS Press, SmartCty, 2016.

[14] M. French, C. Guo, & J. Shim, “Current Status, Issues, and Future of Bring Your Own Device (BYOD).,” Communications of the Association for Information Systems, , vol. 10, pp. 192-197, 2014.

[15] R. Ogie, “Bring your own device: an overview of risk assessment.,” IEEE Consumer Electronics Magazine, vol. 5, no. 1, pp. 114--119, 2016.

[16] L. Irwin, “54% of universities reported a data breach in the past year,” IT governance, London, 2020.

[17] J. Grama, “Just in Time Research: Data Breaches in Higher Education,” EDUCAUSE Research, 2014.

[18] L. Wilbanks, “Cyber Security Requirements for Institutions of Higher Education .,” NASFAA Presentation, 2016.

[19] H. Security, “Malicious Cyber Actors Target US Universities and Colleges.,” 16 01 2016. [Online]. [Accessed 5 4 2021].

[20] T. Nataliya W. Shevchenko, “Threat Modeling: A Summary of Available Methods.,” Software Engineering Institute | Carnegie Mellon University, 2018.

[21] A. Siani, “BYOD strategies in higher education: current knowledge, students’ perspectives, and challenges,” New Directions in the Teaching of Physical Sciences, vol. 12, no. 1, 2017.

[22] D. Maguire, “Dealing with cyber security threats to universities and colleges,” 25 9 2019. [Online]. Available: https://www.jisc.ac.uk/blog/dealing-with-cyber-security-threats-to-universities-and-colleges-25-sep-2019. [Accessed 23 4 2021].

[23] R. &. F. De Kock, “Mobile device usage in higher education institutions in South,” Information Security for South Africa (ISSA), pp. 27-34, 8 2016.

[24] K. Adane, “Threat introduction by Bring your own Device(BYOD) Adoption in an Ethiopian Higher Learning Institution,” solutions to Security and Privacy, vol. 16, no. 2, pp. 7-29, 2020.

[25] M. Kashoda &. W. Timothy, “E-Readiness survey of Kenyan Universities (2013) report,” Kenya Education Network, Nairobi, 2014.

[26] P. COOKE, “BYOD trends of the past and future,” software2, 01 07 2020. [Online]. Available: https://www.software2.com/resource-centre/byod/byod-trends. [Accessed 08 04 2021].

[27] E. Ounza, L. Samuel and O. Solomon, “Emerging Security Challenges due to Bring Your Own Device Adoption: A Survey of Universities in Kenya,” International Journal of Science and Research (IJSR), vol. 7, no. 1, 2018.

[28] Dave, “Why an Information Security Risk Assessment is Important,” BANKERS EQUIPMENT SERVICE, 13 07 2020. [Online]. Available: https://www.bankersequipment.com/2018/07/26/why-an-information-security-risk-assessment-is-important/. [Accessed 08 04 2021].

[29] J. Aileen G. Bacudio, “AN OVERVIEW OF PENETRATION TESTING,” International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 6, 2011.

[30] S. Sengupta, “A survey of moving target defenses for network,” IEEE Communications Surveys & Tutorials, 2020.

[31] A. Alshamrani, “A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851-1877, 2019.

[32] J. Kim, “Burp suite: Automating web vulnerability scanning,” a Ph.D. dessertation Utica College, 2020.

[33] D. Kiran, “A Comparative Analysis on Risk Assessment Information Security Models.,” International Journal of Computer Applications, vol. Volume 82, no. 9., pp. 0995-8887, 2013.

[34] A. Ghulam Nabi, “The Impact of Entrepreneurship Education in Higher Education: A Systematic Review and Research Agenda,” Academy of Management Learning and Education, vol. 16, no. 2, pp. 277-299, 2017.

[35] N. Mikaeilvand., “New Framework for Comparing Information Security Risk Assessment Methodologies.,” Australian Journal of Basic and Applied Sciences, vol. 5, no. 9, pp. 160-166, 2011.

[36] S. Lencer, “Auditing the BYOD program: the growing business use of personal smartphones and other devices raises new security risks,” Institute of Internal Auditors, Inc., vol. 70, no. 1, p. 23+, 2013.

[37] ENISA, “Inventory of Risk Management / Risk Assessment Tools.,” 01 07 2020. [Online]. Available:https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools?b_start:int=20. [Accessed 09 04 2021].

[38] Z. OS, Zain O and R. Kadir, “Security-Based BYOD Risk Assessment Metamodelling Approach.,” in Twenty First Pacific Asia Conference on Information Systems, LANGKWAI, 2017.

[39] I. Veljkovic and A. Budree, “Development of Bring-Your-Own-Device Risk Management Model: A Case Study from a South African Organisation.,” The Electronic Journal of Information Systems Evaluation, vol. 22, no. 1, pp. 1-14, 2019.

[40] N. Mikaeilvand, “New Framework for Comparing Information Security Risk Assessment Methodologies.,” Australian Journal of Basic and Applied Science, vol. 5, no. 9, pp. 160-166, 2011.

[41] B. Guttman, “An Introduction to Computer Security.” in The NIST Handbook, Fb&c Limited, 2018.

[42] L. Greitzer, “Insider Threats: It's the HUMAN, Stupid!” in NCS '19: Proceedings of the Northwest Cybersecurity Symposium, 2019.

[43] S. Frank, L. Greitzer, “Positioning your organization to respond to insider threats,” IEEE Engineering Management Review, vol. 47, no. 2, pp. 75-83, 2019.

[44] J. Roman, “(2012). BYOD: Get Ahead of the Risk. Retrieved May, 2, 2015.,” 11 1 2012. [Online]. Available: https://www.bankinfosecurity.com/byod-get-ahead-risk-a-4394. [Accessed 23 4 2021].

[45] Y. Ratchford, “BYOD-Insure: A security assessment model for enterprise BYOD.” in Fifth Conference on Mobile and Secure Services (MobiSecServ), 2019.

[46] V. Combs, “Google: Most people still have terrible password habits,” tech republic, 4 6 2019. [Online]. Available: https://www.techrepublic.com/article/google-most-people-still-have-terrible-password-habits/). [Accessed 22 3 2021].

[47] L. Jason Andress, “Conduct Security Awareness and Training, in Building a Practical Information Security Program, 2017),,” 2017.

[48] L. Scarfo., “New Security perspectives around BYOD.,” in Seventh International Conference on Broadband, Wireless computing, 2012.

[49] D. Milligan, “Business Risks and Security Assessment for Mobile Devices. In Proceedings of the 8th Conference on 8th WSEAS,” in Int. Conference on Mathematics and Computers in Business and Economics, Dallas, Texas, USA, 2007.

[50] S. Gajar, “Bring Your Own Device (Byod): Security Risks and Mitigating strateegies,” Journal of Global Research in Computer science, pp. 62-70, 2013.

[51] C. Prashanth G. Rajivan, “Update now or later? Effects of experience, cost, and risk preference on update decisions,” journoal of cyber security, vol. 6, no. 1, 2020.

[52] M. Jr, “Training employees how to recognize and defend against cyber-attacks is the most under spent sector of the cybersecurity industry,” cyber Risk aware, 2019.

[53] E. TUVEY, “Mobile security trends we expect to see in 2019,” wandera, 4 12 2018. [Online]. Available: https://www.wandera.com/mobile-security-trends-for-2019/. [Accessed 17 5 2021].

[54] A. Jan, H. Delcker, “MOBILE DEVICE USAGE IN HIGHER EDUCA,” in 13th International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2016), Mannheim, Germany, 2016.

[55] O. Dogerlioglu, ““Bring your own device” policies: Perspectives of both employees and organizations,” Knowledge Management & E-Learning, vol. 11, no. 2, pp. 233-246, 2019.

[56] A. Barreiro, “Population and sample. Sampling techniques. Management Mathematics for European Schools,” , J. P.MaMaEusch, vol. c21, 2001.

[57] W. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches., Sage publications., 2013.

[58] T. Yamane, Statistics, An Introductory Analysis, 2nd Ed., New York: Harper and Row, 1967.

[59] G. Israel, “Determining Sample Size. University of Florida Cooperative Extension Service, Institute of Food and Agriculture Sciences, EDIS, Florida.,” University of Florida, vol. PEOD, no. 5, 1992.

[60] P. Pavel Andreev, “Validating Formative Partial Least Squares (PLS) Models: Methodological Review and Empirical Illustration.,” in Thirtieth International Conference on Information Systems, Phoenix, Arizona., 2009.

[61] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, NJ: Lawrence Erlbaum, Mahwah, 1988.

[62] W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, sage, 2014.

[63] C. group, “ Cyberthreat Defense Report,” CyberEdge, Annapolis, 2018.