2019 First International Conference of Intelligent Computing and Engineering (ICOICE)

Theoretical Bases of Identifying Determinants of Protection Intentions towards Bring-Your-Own-Device (BYOD) Protection Behaviors

Ibrahim Mohammed Al-Harthy[1,*], Fiza Abdul Rahim[2,3], Nor'Ashikin Ali[2,3], Amando P. Singun Jr.[4]
[1]Computer Services, Educational, Technologies Centre, Higher College of Technology, Muscat, Sultanate of Oman
[2]Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia
[3]College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia
[4]Information Technology Department, Higher College of Technology, Muscat, Sultanate of Oman
** Corresponding Author: Ibrahim.alharthy@hct.edu.om*

***Abstract*—Bring-Your-Own-Device (BYOD) has been acknowledged as a very good practice in the workplace. With its increasing popularity where personal as well as organizational data are accessed using BYOD, there have been raising concerns on privacy and security. Most BYOD risks are related to unauthorized access to policy changes and information, leaking sensitive information to people, breach of organization data and privacy, access control, misuse, and even stolen devices. Privacy violations are of widely security breaches in business organizations when users are using their own personal devices. In this paper, it presents the appropriate theories and models to derive a set of validated determinants of protection intentions towards the protection behaviors of BYOD. The introduction of BYOD calls for a thorough investigation of whether or not such a practice poses vulnerabilities and threats to organizations.**

Keywords—BYOD; theories and models of BYOD; protection intentions; protection behaviors; determinants of BYOD

I. INTRODUCTION

Bring-Your-Own-Device (BYOD) has been acknowledged to facilitate both personal and business needs [1] where employees and/or business partners may bring their own device to access data and run workplace applications [2]. BYOD may include a variety of devices such as laptop computers, netbook computers, smartphones/handhelds, tablet computers, e-book readers, and audio players.

The breakthrough of BYOD paves its way from enterprises down to law firms and manufacturers and other organizations where employees are acquiring their private mobile gadgets and voluntarily use them in the workplace [3].

However, IT experts are concerned about the challenges it may pose to security [4] as such technology adoption is unstructured [5] resulting in security breaches, infringement to privacy, and infrastructure control. This calls for organizational leaders to ensure that vulnerabilities and threats shall be evaded through deploying effective security solutions [3].

The mobility advantage provided by these devices present great worth and thus fosters the BYOD embrace which has been fuelled by the advent of the consumerization of these products. Enterprises across industries are starting to understand that they must adapt to the consumerization of IT and the remote working trends already underway in organizations [6].

There have been legal concerns that should be addressed when BYOD should be adopted. For instance, staff who patronizes BYOD would be using applications that are not officially registered with the organization [7]. The organization should have robust network management where there is more effective control over software and devices. BYOD policies (for example, mobile device management policy) could monitor compliance and/or solve legal and privacy concerns that pertain to its implementation.

Moreover, [8] companies should also adhere to the rules and quality requirements related to a document, archive, and back-up data. For example, when used BYOD implementation for private and business purposes through mobile devices, the private data of users should be protected separately from company access to company data at the same time. The paper endeavors to answer the following research questions:

1. What are the theoretical bases underlying BYOD for proper implementation?
2. What are the determinants of protection intentions towards the protection behaviors of BYOD based on the theories and models?

It should be noted that the paper-at-hand is preliminary scientific documentation of the theoretical bases of identifying determinants of protection intentions towards BYOD Protection Behaviours. The authors proposed frameworks of such bases based on content validity and are thereby visually illustrated in the subsequent figures. This documentation may lead to further studies as mentioned in the 'Conclusion and Future Works' section.

The paper is organized as follows: The next section discusses the review of related literature, followed by the introduction of related theories and models, and the detailed discussion of the determinants of BYOD. Future work is presented at the end of the manuscript.

II. REVIEW OF RELATED LITERATURE

This section presents the literature reviews related to BYOD such as its advantages, risks, policy, and protection intentions.

A. Advantages of BYOD

The advantages of BYOD implementation that can be highlighted both for the users and organization. BYOD enables the employee to combine their personal and work lives seamlessly [9]. According to a study by an Asia-Pacific [10], when an organization allows employees to use BYOD implementation, such leads to an increase in the employees' satisfaction. Additionally, this study reported that 64% of employees admitted using private devices to perform assigned tasks in the workplace.

According to [11], BYOD provides the leeway of cost provision with a shift of reference from employer to employee which means that BYOD becomes even more attractive for

978-1-7281-4487-0/19/$31.00 ©2019 IEEE

employees and would not anymore be limited to the organization's resources and cost-effectiveness is apparent as IT-related items and services are now getting away from the company. Thirty percent of organizations that make use of BYOD raises staff satisfaction and increases the level of creativity, critical thinking skills, and problem-solving skills [12].

In addition, a study by A Frost & Sullivan [13], found out that when staff is using their own device, it is more efficient by 34% as it increases their productivity, saving at least 58 minutes every working day. This finding is supported by the executive enterprise mobility report [14] which claimed that more than half (53%) of all staff are productive when working with their own device, leading to a decline in the training curve while improving usability.

Overall, there are different advantages of using BYOD implementation in organizations. However, there are possible risks in BYOD implementation.

B. Risks of BYOD

Issues related to BYOD which is basically about the security and privacy of the data [15]. While there are obvious flexibility and functionality brought about BYOD, there are also drawbacks embed into its use. In other words, while there are manifested inefficiencies while implementing BYOD, there are also possible risks that call for a more secured working environment.

According to [16], using BYOD means an inevitable exposure to security threats especially when the organization in question is not adamant about its vulnerability to malicious software or attacks, unauthorized access, and unnecessary loss of data [17]. Organizations are warned about drafting an appropriate BYOD policy that would safeguard the user credentials, personal and financial information, web accounts, and other sensitive information. Some educational institutions that are practicing BYOD are at the same time strictly implements Network Access Control (NAC).

Also, some businesses are starting to have concerns about employees wearing devices like smartwatches, fitness trackers, smart glasses and virtual reality headsets on commercial premises as they see them as a possible risk to the security of confidential data and few options are available for controlling employees wearable BYOD devices [18].

As listed by [19], the possible security risks and privacy issues that require immediate and appropriate action, including but not limited to malware embedded into BYOD, integration of unregistered mobile OS and applications, penetration of untrusted networks through BYOD, inadequate physical security infrastructure and imminent security risks on BYOD.

Other issues highlighted are the legal issue, especially in enforcing the BYOD policy as well as in protecting users' privacy and access control [20]. In addition [21] has concerned about the legal issues regarding data management and device security, which also involves data loss prevention (DLP) software that can violate users' privacy.

Preventing security breaches through surveillance on the use of smartphones may pose invasion to privacy among when smartphones of staff are being checked periodically, contributing to another social issue. There are three offensive vectors covering and distinguishing the potential attack models for the threat on BYOD smartphones are a malware attack vector, proximity propagation attack, and co-location attack [22].

Indeed, there has been a balanced trade-off between the cons and pros of using BYOD. In as much as it is beneficial in some aspects (e.g. flexibility and mobility, ease of use, functionalities, etc.), it may also pose some aspects of drawback such as security vulnerabilities [23] such as the security perpetrators who access loopholes of the architectural design of BYOD and the workplace to gain personal interest [24].

According to [25] businesses employ casual employees to fill the skills gaps in the market. Some of such casual employees include the freelancers who devout their services when needed, the contractors who tend to complete an undertaking within a set deadline, and other temporary and contingent workers. The statistics reveal that the employment of temporary workers soared to eight percent year over year, further illustrating an increased practice of such an employment scheme. According to statistics claim by [26] 40% of America's workforce will be a freelancer by 2020. The organization may hire a freelancer to complete some projects but the use of its own device may impact security and policies set to protect an enterprise. In addition, some organizations may accept the student to do on-job-training without any restrictions to use their own devices. This allows an open door for data breach and potentially sensitive information to be stolen.

Since many organizations now rely on a growing number of temporary employees brought in on a short term basis to keep their business operating, the organizations need to balance flexibility with security: ensuring that users are who they say they are, in order to protect their data and manage the risk of compromised user accounts. Hence, there is a need for organizations to be responsible for upgrading the privacy, security, and regulatory concerns related to BYOD implementation [27].

Also, [28] has mentioned that contractors and temporary employees may or may not be part of an overall BYOD initiative but at some level and in some ways should be. When such casual employees are allowed to access the network using their own devices, this would open a door for them into unauthorized and careless access to sensitive and confidential data. Organizations should be vigilant in implementing BYOD among casual or temporary employees. Providing access to organizations' services from temporary employees owned devices increases the risk of compromising system security [29]. According to [30] reported that over 60% of employees use personal file sharing applications or personal devices to access and share company information. For this, organizations that allow using BYOD implementation should at least be aware of the most major risks.

C. BYOD Policy

As discussed in the previous section, the biggest risks for the organization that allow BYOD environments are security and privacy. Deploying and enforcing security controls through the BYOD policy may help the organization to monitor the implementation. According to [15] BYOD policy should stipulate provisions related to Secure Device Management (SDM) in order to track and monitor mobile applications. It should also specify guidelines on how employees and employers collaborate when using BYOD.

It has been reported that few American Companies are embracing BYOD due to lack of policies that effectively govern its implementation [31]. Some related policies are: on usage, on support, and on risk management. Inherent to its implementation, it requires operational cost which should be allocated for extensive training, sustained monitoring, and strict compliance to security.

It has been raised by [32] that there should be a reasonable level of security when BYOD is adopted. Diversify the pertinent provisions between an enterprise owned device and a temporary employee-owned device. It has been added that the organization has privileges to perform changes on systems configuration, to apply encryption/decryption, to monitor usage and misuse/abuse, and to detect suspicious activities.

In the study by [33], it had been reported that 19% of the businesses where BYOD was implemented have a proper policy for the personally owned device used for business activities. Such implementation is in accordance with the universal quality standard for market research.

The following are the appropriate tools that could be utilized to manage the implementation of BYOD: (i) the Mobile Device Management (MDM), (ii) the Mobile Application Management, and (iii) the Mobile Information Management. For example, MDM may is a key solution to limit privacy and security concerns in BYOD deployments. When installed in an organization server, MDM can detect mobile devices attempting to access the network. It can manage and control the devices' data, applications, and configurations.

Some of the procedures suggested by [34] are the following countermeasures: (i) use of a strong login credentials, (ii) automatic system's lock when workstation is idle, (iii) improvement of security infrastructure, (iv) updating software, (v) backup mechanism, (vi) updating antivirus software, and the like [34].

BYOD policy usually stated on the basic security requirements for BYOD. For example, [35] illustrated a phenomenon in which the devices must concord to prescribed security policy stipulating the courtesy of not accessing applications while using the system. Once the user complies with such policy then he has to also check to what extent is his privilege in terms of installing a new application.

As stated by [36] there is no single solution would solve different type of BYOD risks. Policies should be reinforced across the organizations. These should be constantly revisited to ensure that these are updated due to the fast-pacing technology.

The success of security is dependent on user behavior because has become a very important topic in security [37]. Users operate technological and physical security measures to protect information assets and information systems in their respective environments. Thus, it is very important to understand how user behavior may affect the protection of information assets towards various types of vulnerabilities such as breach data and information. There is a general consensus in the literature that user behavior poses a significant risk in the protection of information assets [38].

D. Protection Intention of BYOD

Many end users may not have the necessary level of knowledge or capability to protect themselves from online threats. Furthermore, they may not be equipped to operate the technology to safeguard against these threats. Thus, it is important that end-users are educated with regard to protecting information assets [39]. Protection intentions are linked to users' intentions [40] against security attacks as raised in the fear-appeal. It has been clarified by [41] that awareness can be classified to threat awareness and countermeasure awareness.

Researchers proposed including users' information security awareness in information security models so there is a need to better evaluate their information security awareness intentions within their personal lives and in workplaces [42].

It has been observed by [43] that when users encountered security threats, they are most likely trying their capability to counterattack the said threats. However, some users also feel that there is an increase in the users' intention to keep themselves more secured if they perceive that they are more vulnerable, especially if they are aware that there is a severe threat by [43]. On the other hand, [44] said that users would appreciate the benefits of performing risky unsecured actions which would otherwise weaken their intention to reinforce adaptive protective response threats.

In contract, users are reluctant to proceed with the performance of protective behaviors due to the cost, time, and effort required to get secured. It has been observed by [43], [45], [46]. Thus, [41] investigated the considerable outcome of individuals' protective intentions towards their actual protective behaviors. The researcher also explored the intervening security concerns that may arise between the workplace and home setting which require sufficient security knowledge.

Based on the study of [47], "behavioral performance is categorized under personal control". It has been stated that the behavioral intention turned out to be positive for those who acquired ample knowledge of adaptive responses. Only when individuals experience vulnerability and/or understand its huge impact that they may consider it helpful.

III. Related Theories And Models

This section discusses and reviews four theories on users' behaviors. The theories could be used to research the BYOD technological concept from several perspectives. Theories such as motivation theories have been utilized as the proposed model for various BYOD related research.

A. Theory of Reasoned Action (TRA)

TRA [48] helps one to draw logical decisions about innovations. It has been claimed by the researchers that when a decision was derived based on such theory then this would lead to the acceptance of innovations. The theory states that "the decisions or behavioral intentions depend on the attitudes toward innovation and the local subjective norms." [49], [50] argued that users adopt innovation when they are encouraged by their peers, family, and significant others. Thus, it has been argued that users' attitudes are related to behavioral intentions as shown by the correlation with the actual adoption of innovation as shown in Fig. 1.

A study by [51] reported that BYOD mobile devices are significantly influenced by the users' attitudes toward the perceived benefits of BYOD. The study claims that perceived benefits and perceived uncertainty significantly influence employees' attitudes towards BYOD. As a result of the study, three (3) classes of issues clarifies the theoretical explanation for the antecedents of employees' uncertainty towards the concept of BYOD, namely: (i) security, (ii) privacy, and (iii) legal concerns.

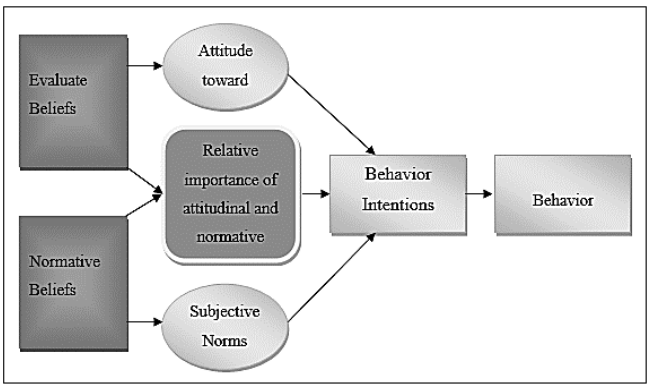

Fig. 1. Theory of Reasoned Action (TRA)

In another study conducted by [52] used TRA to validate the additional constructs expected to strengthen TRA and demonstrated their effects on technology use in an information systems discourse. They also suggested the possibility of applying TRA in an information systems discourse, with additional constructs, which is a precursor of the extended theory of reasoned action.

B. Theory of Planned Behaviour (TPB)

TPB was initiated as a TRA way back in 1980 and was essential in predicting a persons' intention in indulging behavior at a time and at a specific place [48]. The intention of TPB was to provide an explanation of all behaviors which people have the ability to control. However, TPB ignored the characteristics of the innovation itself as in Fig. 2.

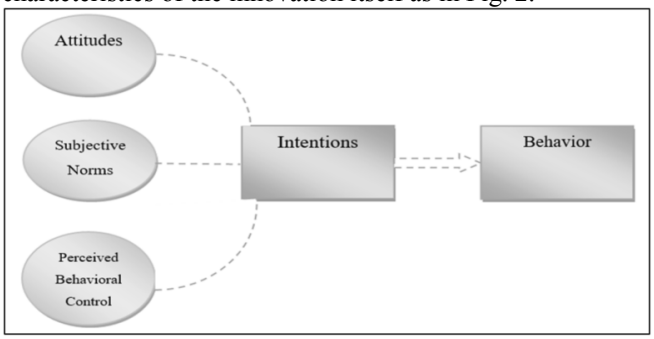

Fig. 2. Theory of Planned Behaviour (TPB)

There are three constructs that comprise of the TPB in predicting the following: (i) individual's intention and behavior, (ii) attitude, (iii) subjective norms, and (iv) perceived behavioral control.

According to [48] the perceived behavioral control construct justifies the availability of assets, support and services, equipment, and facilities that users may consider as vital requirements for decision-making if innovation is feasible for adoption. Therefore, the TPB assumed users' attitudes towards technology adoption and their perceived power which influences their behavioral intention, which in turn, affects the utilization of technologies.

Consequently, and in comparison, the TPB appears to be more variable and specific in interpreting the behavioral intention than the theory of reasoned action.

C. Protection Motivation Theory (PMT)

PMT was coined by Rogers in 1975 to understand better fear appeals and how people overcome them as such. Not too long thereafter, Rogers expanded the theory in 1983 to a more general theory of persuasive communication. The theory was a derivative work of Richard Lazarus who spent much of his work on how people would react and what coping mechanism they would employ during stressful situations. In his book entitled 'Stress, Appraisal, and Coping', he expounded the idea of cognitive appraisal processes and stress coping mechanisms [53]. He states that people have different approaches, interpretations, and reactions to certain types of events. While it was true that he came up with many of the fundamental ideas used in the protection motivation theory, Rogers was the first to apply the terminology when discussing fear appeals. The graphical representation of the PMT, as shown in Fig. 3.

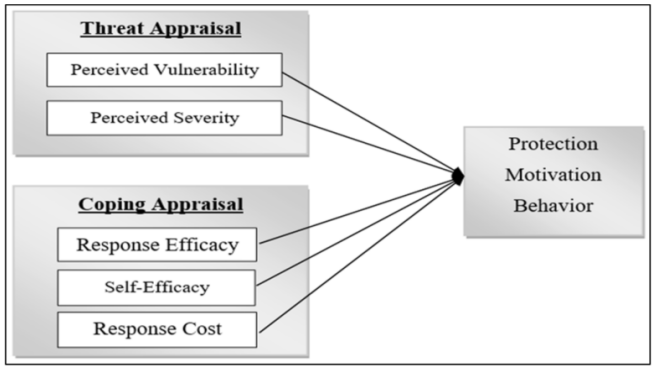

Fig. 3. Protection Motivation Theory (PMT)

The fundamental idea of the PMT is that individuals engage in adaptive actions when challenged around with risks through two (2) main cognitive processes of (i) "threat appraisal" and (ii) "coping appraisal" The threat appraisal assesses the level of threat in terms of perceived vulnerability (PV) and perceived severity (PS) of the individual. Subsequently, the coping appraisal process follows. The latter refers to an individual's assessment of his/her ability in responding to the perceived threat and therefore avoiding a certain risk. It comprises of three (3) sub-components such as Response Efficacy (RE), Self-Efficacy (SE), and Response Cost (RC) [37].

In a particular study of [54], it has proposed theoretical model that explains users' information security awareness in BYOD programs. The model is based on the PMT as well as the general deterrence theory. The study provided useful information related to user's cybersecurity inertia, a personal security management procrastination tendency on the user's security awareness of organization information resources. After evaluating this study, the said model would enlist helpful guidelines to appropriately implement BYOD security management.

Also, another study by [55] made use of multi-group structural equation modelling (MSEM) methods for the development of a conceptual model that is based on the

Protection Motivation Theory in a BYOD Australian institution. The study explored the intention to perform information security behaviors which varied due to the change of context.

D. Technology Acceptance Model (TAM)

Davis formulated the original technology acceptance model [56], [50], [49], [57] which explains technology adoption in terms of the impact of motivational factors (i.e. perceived usefulness and perceived ease of use) on the attitudes of potential adopters [58]. However, the subjective norm construct has been disregarded by TAM; hence, there has been a call for more studies [50] to widely increase the effective use and validity of the TAM. More studies in different fields and locations should be conducted to strengthen the evidence of the relationships of the factors as illustrated in Fig. 4.

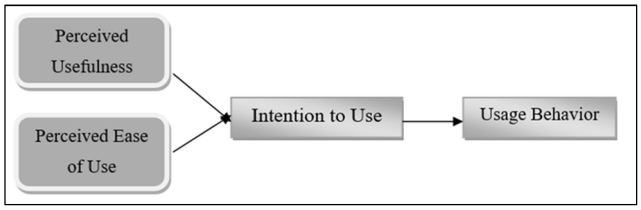

Fig. 4. Technology Acceptance Model (TAM)

Subsequently, the use of TAM has been evolving to reveal other factors that could help in technology adoption decision-making. One improvement of the TAM was the reduction of the attitude construct which has a weak mediating effect on perceived usefulness and ease of use of technology factors [59], [50]. Thus, [58] the TAM had been slightly modified to consider situations where adopters had behavioral intentions and neutral attitudes. Thereafter, the model has been adjudged to be more effective in justifying the influence of perceived usefulness and ease of use on the actual use of technology [50].

Later, [59] extended the original TAM to include voluntariness and subjective norm institutional factors, namely: (i) job relevance, (ii) output quality, and (iii) result indemonstrability, (iv) perceived ease of use technological factors, (v) experience and (vi) image personal factors. It is credited to the extensive demand for increased reliability in explaining the adoption of technology. The extended TAM incorporated previous acceptance models to effectively evaluate the intentions of potential technology adopters [56], [50].

It has been reported by [57] that the original TAM explained less than 40% of the variance in technology adoption while another study thereafter by [56] reported that the model explains over 50% of the variance in adoption.

E. Other Related Studies on Theories and Models

Related works focused on papers that published the last five years and reviewed the protection behaviors. A recent study by [15] elaborates on how BYOD provides an impact on the employee's productivity and job satisfaction. So, the findings from this study have significance to practical and managerial implications if BYOD is going to be implemented across the organizations. The study by [60] has provided an analysis of the studies about workaround behavior in the Information Systems (IS) area, addressing its positive and negative aspects and raising the key-related issues. [61] has presented the advantages as well as the potential risks of BYOD-related practices. This study highlights new possible risks resulting from BYOD adoption and identifies various security concerns of entrepreneurs and staff within the world of small and medium-sized enterprises (SMEs).

Another study by [62] provides a current best practice approach that can be used to identify and manage BYOD security and privacy risks faced by organizations that use mobile devices as part of their business strategy. This paper tackles the beauty and the danger of using BYOD as a warning to ensure that mitigation strategies should be in place before its implementation. So, the findings from this study have indicated that there are many risks associated with BYOD in the areas of physical threats, access control, communications and applications, and compliance. Critical data that are at risk and those confidential data that should not be divulged to another party should be safeguarded through BYOD countermeasures in place, along with an individual's awareness and knowledge about BYOD.

Based on [63] they mentioned BYOD favors the use of personal and public devices and communication means in corporate environments. In this dynamic and heterogeneous setting, the purpose of this paper is to present a methodology called opportunity enabled risk management (OPPRIM), which supports the decision-making process in access control to remote corporate assets.

A study by [64] shared his findings of a longitudinal investigation into the BYOD project which offers new insights into the digital divide issues in the context of evolving teaching and learning practices across three levels, namely, digital access, digital capability, and digital outcome. It has been mentioned that the information security behaviors of smartphone users in an affluent economy of the Middle East and smartphone users are more worried about malware and data leakage than targeted information theft.

Privacy and security concerns related to Android OS through the so-called permission mode have been discussed by [65]. Access to personal information of the users is by definition neither problematic nor unlawful because smartphone OS does not necessarily provide an adequate facility of protection on user's data. It has been added that we could mitigate the privacy concerns of users of smart devices. In the data protection legal framework, the users should stop-transfer the data outside smart device. Also, stop saving organization data and use the data legally in requirements specified only.

According to a study by [66] have aimed to summarize the legal and ethical foundations of privacy with connections to work emails and text messages, describe trends and challenges related to BYOD, and propose legal and no legal questions these trends will raise in the foreseeable future.

The all-embracing power of mobile technologies hardly manages the boundaries between work and non-work domains. Previous theories of work-life boundary management suggest boundary management approaches to do segmentation and integration of work-life domains, though technology role has not been properly addressed [67].

The young generation who comprise of most-likely tech-savvy would view the use of their own gadgets or devices 'more of a right than a privilege' which draws them toward IT consumerization. Needless to say that several organizations are already deploying BYOD programs, allowing employees to use personal devices for work-related activities, but other managers remain reluctant about the implications of such programs [68].

Another study by [66] has examined how advances in unified communications (UC) technologies are enabling radical changes in workplace redesign. Cost-effective and easily accessible technologies enable users to work and complete their job-related tasks in a manner that was impossible decades ago. Mobile hardware, networking infrastructure, and robust UC platforms are making work less location- and time-dependent. Whereas these technologies provided the catalyst for the reimagining of the workplace in the early to mid-2000s, it was the explosion of BYOD in recent years that has caused organizations to reconsider innovative workplace usage.

IV. Determinants of Protection Intentions of BYOD

Based on the foregoing related literature and related studies, the researchers come up with the list of determinants of protection intentions of BYOD based on theories and related models. Such theories and related models provide the variables and the relationship between determinants of protection intention towards BYOD protection behaviors.

A. Theories Selections and Justification

From a theoretical viewpoint, a study by [15] to identify and understand attitudes and behavior towards factors, values, and issues associated with privacy to evaluate the case of BYOD in organizations. The theoretical perspective of TPB indicates a strong connection between values, practices, beliefs, perceptions, and behavior. The theory can be used to predict behavior and will be used as an underlying framework for this study. In the current contribution, the theory will serve as a guideline to create the model to find the determinants of protection intention towards BYOD protection behavior by adopting the attitude and behavior control as in Fig. 5.

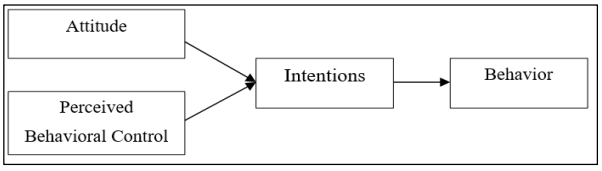

Fig. 5. Adapted Variables from (TPB)

PMT provides a lens to examine individual behaviors as a person confronts a potentially threatening situation. PMT has been used to observe users' protective behavior in online transactions [51], [70] and broadly accepted as a tool for predicting behavior. In this study, four variables from PMT namely perceived vulnerability, perceived severity, response efficacy, and self-efficacy are adapted in the proposed model as in Fig. 6.

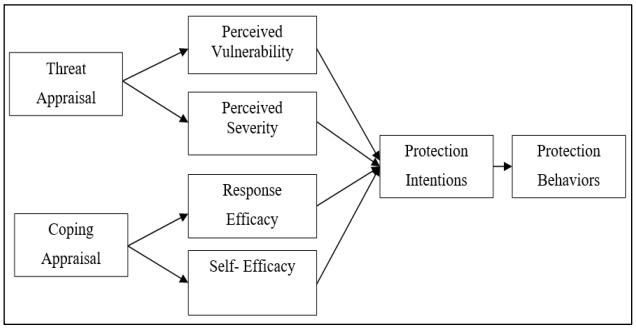

Fig. 6. Adapted Variables from PMT

B. Digital Skills in Protection Behavior Studies

Digital skills have started a project with the main objective to develop instruments because there is recognition amongst researchers that the measures typically used in empirical work are not sufficiently nuanced [71]. The objective of this project was to develop measures that allow for testing of the models suggested paths from social to digital inclusion by constructing indicators for digital engagement and outcomes and a set of digital skills that influences these links. So, there are five digital skills which are: (i) operational skill, (ii) mobile internet skill, (iii) information navigation skill, (iv) social skill, and (v) creative skill. In this study, four (4) skills will be adopted as follows:

a) Operational Skills: An operational skills definition is the statement of procedures used in defining the terms of a process or set of validation tests needed to determine the nature of an item or phenomenon. These are skills to operate digital media, the skills to handle the special structures of digital media, the skills to search, select and evaluate information in digital media and the skills to employ the information contained in digital media as a means to reach a particular personal or professional goal [71]. These skills are the basic skills of using the internet such as downloading/uploading files, using shortcut keys, adjusting privacy settings and watching videos [72]. Without operational skills, it would be difficult to operate on the internet, and people would not be able to use privacy settings and other online privacy protection behavior.

b) Information Navigation Skill: Information navigation skill refers to the ability of individuals to search the Internet and/or the ability to navigate the Internet to find the most appropriate information using the right keywords, verifying the reliability of the information, and the ability of not getting lost on websites [72], [71].

c) Social Skill: Social skill refers to the ability of an individual to filter information that is shareable and those that are not. It may also mean the ability to apply the art of giving feedback and comments. Keeping in touch with friends online and the ability to unfriend online are specific examples of social skills [72], [71]. It has been regarded that once a user is more aware of the appropriateness and audiences of their online content, there is a tendency that he/she is also more aware of the privacy issues around social network sites.

d) Creative skill: This refers to the technical know-how of the user to fix and match, edit or create content from scratch to form pictures, videos, and websites and publishing them online [72], [71]. People who exchange content frequently are most likely aware that they are sharing the

same in the right setting. They may also confident to accept comments and reactions (either favorable or unfavorable) which would give them the touch-and-feel of how their privacy has been unnecessarily invaded. Thus, it has been argued that if a person has high creative skills then there is a great chance that he is using online privacy protection behavior. On the other hand, if people carelessly share content with the world, this implies a decrease in their online privacy protection behavior. Hence, a supporting claim is that people who share content do not absolutely mean that they wanted to divulge and give up their privacy instead they still do protect their personal information.

A study by [68] created a framework that contains five digital skills, such as Operational skill, Information Navigation skill, Social skill, Creative skill, and Mobile skill. This study adopts four internet skills, which are: Operational skill, Information Navigation skill, Social skill, and Creative skill as shown in Fig. 7.

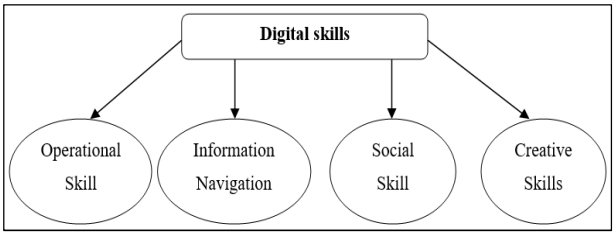

Fig. 7. Adapted Digital Skills

C. *Determinants of Protection Intentions Towards BYOD*

Based on the foregoing sections, Fig. 8 presents the different determinants of BYOD protection intentions such as Perceived Vulnerability, Perceived Severity, Self-Efficacy, Response Efficacy, Attitudes, Behavior Control, Operational Skill, Information Navigation Skill, Social Skill, and Creative Skill. It can be hypothesized that:

- H1: Perceived Vulnerability has a positive influence on Protection intention
- H2: Perceived Severity has a positive influence on Protection intention
- H3: Self-efficacy has a positive influence on Protection intention.
- H4: Response efficacy has a positive influence on Protection intention.
- H5: Attitude towards having a positive influence on Protection intention.
- H6: Behavior Control has a positive influence on Protection intention.
- H7: Operational skill has a positive influence on Protection intention.
- H8: Information navigation skill has a positive influence on Protection intention.
- H9: Social skill has a positive influence on Protection intention.
- H10: Creative skill has a positive influence on Protection intention.
- H11: Protection intentions having a positive influence on protection behaviors.

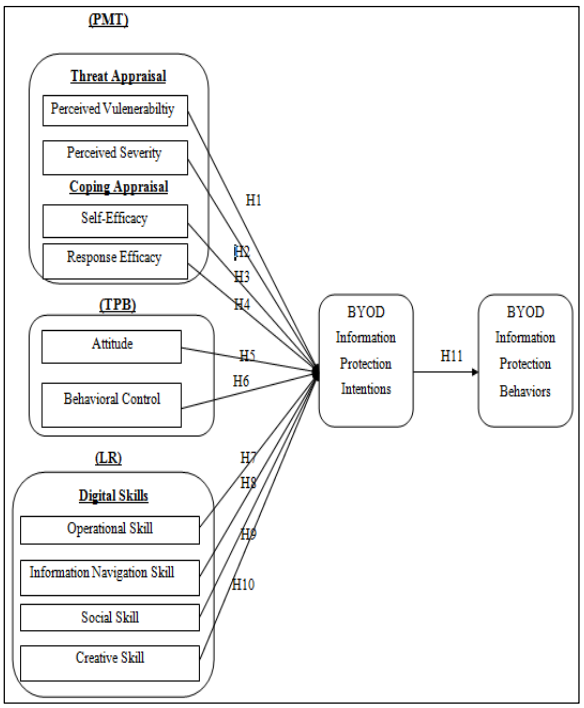

Fig. 8. Determinants of Protection Intentions towards the protection behaviors of BYOD

V. Conclusion and Future Works

This is an initial yet ongoing study that introduces the various determinants of protection intentions towards protection behaviors of BYOD. Utilizing the available secondary data resources, this study was able to successfully identify the determinants that influence protection intentions towards protection behaviors of BYOD, namely: Perceived Vulnerability, Perceived Severity, Self-Efficacy, Response Efficacy, Attitudes, Behavior Control, Operational Skill, Information Navigation Skill, Social Skill, and Creative Skill.

The related literature provided the content validity that these determinants have an association with protection intentions. In view of the foregoing context, a proposed model hypothesizes the ten determinants that would influence protection intentions. Hence, the succeeding testing stage of the proposed conceptual model would help to determine the underlying influencing relationship and interrelationship among the aforementioned determinants. The unit of analysis for this study would be the employees from various types of organizations across the Sultanate of Oman.

References

[1] J. Thielens, "Why APIs are central to a BYOD security strategy," *Network Security,* 2013.

[2] C. C. S. I. Systems, "2012 Annual Report," 2012.

[3] H. Romer, "Best practices for BYOD security. Computer Fraud and Security," p. 13–15, 2014.

[4] Antonopoulos, "IT security's scariest acronym: BYOD, bring your own device," 2011. [Online]. Available: https://www.networkworld.com/article/2179632/it-security-s-scariest-acronym--byod--bring-your-own-device.html. [Accessed 21 November 2019].

[5] V. &. M. H. Omwenga, "Towards the adoption of bring your own device concept in an organization," *International Journal of Social Sciences and Entrepreneurship,* no. 1(11), p. 1–12, 2014.

[6] G. Thomson, "BYOD: Enabling the chaos," *Network Security,* vol. (2), p. 5–8, 2012.

[7] S. Johnson, "Bringing IT out of the shadows," *Network Security,* vol. 12, p. 5–6, 2013.

[8] G. &. K. C. Disterer, "BYOD Bring Your Own Device," *Procedia Technology,* vol. 9, p. 43–53, 2013.

[9] J. Tavangar, "Big Data Means Big Jobs: 4 Areas to Specialize In for Career Success," 2015. [Online]. Available: https://www.thearmadagroup.com/blog?cat=1&limit=10&start=600. [Accessed 21 November 2019].

[10] J. Yap, "BYOD boosts staff ' s productivity , job satisfaction," 2012. [Online]. Available: https://www.zdnet.com/article/byod-boosts-staffs-productivity-job-satisfaction. [Accessed 21 November 2019].

[11] P. Voica, "BYOD ' linked to increased productivity ' Summary : BYOD policies can help boost employee satisfaction and improve productivity," 2016. [Online]. Available: http://www.employeechoice.co.uk/byod-linked-to-increased-productivity/. [Accessed 21 November 2019].

[12] M. &. K. E. Keshavarz, "Farmers' pro-environmental behavior under drought: Application of protection motivation theory," *Journal of Arid Environments,* vol. 127, p. 128–136, 2016.

[13] M. Turek, "Employees Say Smartphones Boost Productivity by 34 Percent," *Insights in Frost & Sullivan Research,* 2016.

[14] Ericsson, "Executive Enterprise Mobility Report: White Paper," 2016.

[15] S. Blizzard, "Coming full circle: Are there benefits to BYOD?," *Computer Fraud and Security,* vol. 2, p. 18–20, 2015.

[16] O. U. &. I. Z. M. Franklin, "The Future of Byod in Organizations and Higher Institution of Learning," *International Journal of Information Systems and Engineering,* vol. 3, no. 1, p. 110–128, 2017.

[17] R. A. Siddiqui, "Bring Your Own Device (BYOD) in Higher Education," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS).*

[18] P. &. Y. S. Hynes, "Bring your own device?," *Debates in Computing and ICT Education,* p. 153–166, 2018.

[19] M. W. C. &. Z. Z. Mahinderjit, "Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm," *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 2, p. 53–62, 2017.

[20] M. Dawson, "Hyper-connectivity : Intricacies of national and international cyber securities.," 2017.

[21] M. Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)," *Physics Procedia,* vol. 78(December 2015), p. 179–184, 2016.

[22] F. P. W. H. C. T. &. Z. X. Li, "Smartphone strategic sampling in defending enterprise network security," *IEEE International Conference on Communications,* vol. (June 2013), p. 2155–2159, 2013.

[23] H. Romer, "Best practices for BYOD security," *Computer Fraud and Security,* vol. 2014(1), p. 13–15, 2014.

[24] H. Romer, "Best practices for BYOD security," *Computer Fraud and Security,* vol. 2014(1), p. 13–15, 2014.

[25] K. Olivieri, *How to Permanently Secure Mobile Temp Workers,* 2015.

[26] J. Neuner, "40% of America's workforce will be freelancers by 2020," *Quartz,* 2013.

[27] P. Beauchamp, "BYOD in the Workplace: Benefits, Risks and Insurance Implications," *HuffPost,* 2016.

[28] B. Zalud, "Minimizing Risks from Contractors and Temporary Employees," 2015.

[29] J. Pochepan, "Employees Working On Their Personal Devices? Here's How You Can Protect Your Business Data," 2019.

[30] G. Hollander, "The Top 7 Risks Involved With Bring Your Own Device (BYOD)," 2019. [Online]. Available: https://www.m-files.com/blog/top-7-risks-involved-bring-device-byod/. [Accessed 21 November 2019].

[31] R. &. T. Astani, "Issues in information systems planning," *Information & Management,* vol. 10(5), p. 245–254.

[32] D. A. M. S. B. &. A. A. Arregui, "Mitigating BYOD Information Security Risks," *Australasian Conference on Information Systems,* p. 1–11, 2016.

[33] D. f. D. C. M. a. S. HM Government, "Cyber Security Breaches Survey 2018: Statistical Release," *Cyber Security Breaches Survey,* 2018.

[34] U. o. Edinburgh, "BYOD Policy: Use of Personally Owned Devices for University Work," 2015.

[35] A. C. G. M. A. &. V. L. Armando, "Formal modeling and automatic enforcement of Bring Your Own Device policies," *International Journal of Information Security,* vol. 14(2), p. 123–140.

[36] S. Johnson, "Bringing IT out of the shadows," *Network Security,* vol. 2013(12), p. 5–6, 2013.

[37] G. B. V. E. J. N. &. T. H. Saridakis, "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users.," *Technological Forecasting and Social Change,* vol. 102, p. 320–330, 2016.

[38] N. C. F. L. S. F. Manal Alohali, "Information & Computer Security Article information," *Information & Computer Security,* vol. 24(4), p. 348–371, 2018.

[39] N. S. S. M. V. S. R. F. S. G. N. A. &. H. T. Safa, "Information security conscious care behaviour formation in organizations," *Computers and Security,* vol. 53, p. 65–78, 2015.

[40] S. R. G. D. F. L. P. B. M. G. D. &. P. P. Boss, "What Do Systems Users Have to Fear? Using Fear Appeals To Engender Threats and Fear that Motivate Protective Security Behaviours," *MIS Quarterly (MISQ), 39(4), 837–864,* 2015.

[41] F. &. T. A. Hassandoust, "Understanding Users ' Information Security Awareness and Intentions : A full Nomology of Protection Motivation Theory," in *PACIS 2018 Proceedings*, 2018.

[42] B. &. W. Y. A. Hanus, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Information Systems Management,* vol. 33(1), p. 2–16, 2016.

[43] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," 1975. [Online]. Available: https://www-tandfonline-com.ezproxy.uniten.edu.my/doi/abs/10.1080/00223980.1975.9915803. [Accessed 21 November 2019].

[44] D. &. P. S. Dang-Pham, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," *Computers and Security,* vol. 48, p. 281–297.

[45] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers and Security,* vol. 31(1), p. 83–95, 2012.

[46] S. S. P. &. O. S. Milne, "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *Journal of Applied Social Psychology,* vol. 30(1), p. 106–143, 2000.

[47] N. S. D. &. R. J. G. Kurt, "Protection motivation and risk communication," *Risk Analysis,* vol. 20(5), p. 721–734, 2000.

[48] I. Ajzen, "Behavioral Interventions Based on the Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes,* vol. 50(2), p. 179–211, 1996.

[49] N. D. A. N. &. A. N. Oye, "The history of UTAUT model and its impact on ICT acceptance and usage by academicians," *Education and Information Technologies,* vol. 19(1), p. 251–270, 2014.

[50] N. &. G. A. Marangunić, "Technology acceptance model: a literature review from 1986 to 2013," *Universal Access in the Information Society,* vol. 14(1), p. 81–95, 2015.

[51] B. D. K. &. B. M. Lebek, "Discussion of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices," in *AMCIS 2013 Proceedings*, 2008.

[52] O. C. L. S. O. B. C. A. S. &. O. S. Otieno, "Validation of Extended Theory of Reasoned Action to Predict Mobile Phone Money Usage," *World Journal of Computer Application and Technology,* vol. 6(1), p. 1–13.

[53] R. S. Lazarus, "Stress, Appraisal, and Coping," 1984.

[54] B. Han, "User's Information Security Awareness in BYOD Programs: A Theoretical Model," 2017.

[55] G. Harris, "Contextual Difference and Intention to Perform Information Security Behaviours Against Malware in a BYOD Environment: a Protection Motivation Theory Approach," p. 4–6, 2013.

[56] C. B. Ageneau, "Bring your own device," *Le Nouvel Economiste,* vol. 10(2), p. 117–122, 2012.

[57] B. D. P. T. J. V. B. J. D. W. &. D. P. Pynoo, "Predicting secondary school teachers' acceptance and use of a digital learning environment: A cross-sectional study," *Computers in Human Behavior,* vol. 27(1) , p. 568–575.

[58] F. Davis, "A Combined Phase and Force Compensation Method for Real-time Hybrid Testing," in *15th World Conference on Earthquake Engineering (15WCEE)*, 1989.

[59] M. G. H. M. D. G. B. D. F. D. &. W. S. M. V. e. a. Morris, "User acceptance of information technology," vol. 27(3), p. 425–478, 2003.

[60] A. M. A. C. G. &. M. G. L. de Vargas Pinto, "Workaround behaviour in information systems research," *Revista de Gestão,* vol. 25(4), p. 430–446, 2018.

[61] Y. B. Paméla Baillette, *BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs,* 2018.

[62] A. M. D. a. A. J. Bello, "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments," *Information & Computer Security,* vol. 25(4), pp. 475-492, 2017.

[63] A. S. J. B. L. C. T. X. a. G. J. Aldini, "Design and validation of a trust-based opportunity-enabled risk management system," *Information & Computer Security,* vol. 25(1), pp. 2-25, 2017.

[64] C. Scogings, *Understanding Learning Outcome Divide in the Learning Process,* 2016.

[65] P. S. E. V. K. L. M. Matina Tsavli, "Reengineering the user: privacy concerns about personal data on smartphones," *Information & Computer Security,* vol. 24(4), p. 348–371, 2016.

[66] J. &. L. R. C. Williams, "Unified communications as an enabler of workplace redesign," *Measuring Business Excellence,* vol. 19(1), p. 81–91, 2015.

[67] K. a. R. D. Cousins, "Managing work-life boundaries with mobile technologies: An interpretive study of mobile work practices," *Information Technology & People,* vol. 28(1), pp. 34-71, 2015.

[68] L. A. Vandelannoitte, "Information Technology & People Article information ," *Information Technology & People,* vol. 28(1), p. 2–33, 2015.

[69] I. &. S. S. Ajzen, "Action versus inaction: Anticipated affect in the theory of planned behavior," *Journal of Applied Social Psychology,* vol. 43(1), p. 155–162, 2013.

[70] S. Youn, "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *The Journal of Consumer Affairs,* vol. 43(3), p. 389–418, 2009.

[71] A. J. A. M. H. E. J. &. E. R. van Deursen, "Measuring digital skills. From digital skills to tangible outcomes project Report," 2014. [Online]. Available: http://www.oii.ox.ac.uk/research/projects/?id=112. [Accessed 21 November 2019].

[72] M. Kamp, "Determinants of privacy protection behavior on social network sites," 2016. [Online]. Available: http://essay.utwente.nl/69826. [Accessed 21 November 2019].

[73] S. Blizzard, "Coming full circle: Are there benefits to BYOD?," *Computer Fraud and Security,* vol. 2015(2), p. 18–20, 2015.