Journal of Theoretical and Applied Information Technology
15th September 2020. Vol.98. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DIMENSIONS OF PROTECTION BEHAVIORS: A SYSTEMATIC LITERATURE REVIEW

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 Center, Higher College of Technology, Muscat, 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, Oman

[*] Email: Ibrahim.alharthy@hct.edu.om

ABSTRACT

The term Bring Your Own Device (BYOD) has generated many hopes and fears among many users in this field related to behaviors of information protection. Threats of BYOD include illegal access to policy changes and information, disclosure of confidential details to the public, leakage of organization data and privacy, access control, abuse, and lost of devices. This study examines the existing studies on various dimensions in conceptualizing the behaviors of information protection. Using a systematic method, we analyzed four major databases, including IEEE, Science Direct, SpringerLink, and Taylor & Francis, from which 57 articles were selected from the year 2010 to 2019. In this study, ten (10) dimensions are discussed: protection behaviors and its Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Response Cost, Subjective Norm, Attitude, Security Self-Efficacy, Information Security Awareness and Perceived Behavioral Control.

Keywords: *Bring Your Own Device, BYOD, Protection Behaviors, Systematic Literature Review*

1. INTRODUCTION

Nowadays, information is viewed as a basic need, without which many business organisations cannot properly perform to the fullest. The unavailability of information resources may impact business operations. Due to its importance, it is vital for organisations to protect their information resources to enable continued access [1]. Thus, information security has become a growing concern in organisations whereby the information is protected from authorized access, disclosure, destruction or modification. It means that the information is protected to ensure its availability, integrity, and confidentiality. The report by Verizon Data Breach Investigations Report in 2019 shows that there are 41,686 security incidents in 86 nations worldwide and 2,013 data breaches from 73 data sources, both public and private entities [2]. In addition, It was predicted that overall security expenditure would be increasing to more than USD124 billion in 2019 [3].

Few studies have been conducted to find the reasons for data or information security problems. Among various explanations behind such negligible investigation could be due to the idea that within the data security setting, there are issues related to human behaviour rather than technical [4]. Additionally, [5] in their studies on information security management in Malaysian public sectors mentioned that the human factor is an area that should be given attention when considering information security. The recently accepted norm of allowing personal-owned equipment to be brought into and out of the office that penetrated the office network enables more exposure to privacy and data security threats as the appliances held by employees may not follow the security policies enforced on company machines [6]. This norm which refers to Bring Your Own Device (BYOD) enables employers to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

provide access to organization facilities from appliances possessed by employees; hence, this may lead to compromising the security of the company's information system [7]. Although the issue of BYOD security has raised concerns in organisations, little is known on the determinants of protection behavior. As a result, this study aims to investigate the dimensions of protection behavior of previous studies using a systematic literature review.

During the analysis of 57 articles, there has been an obvious paucity of studies in the extant literature that focus on identifying the dimensions of protection behaviors using a systematic literature review. This paper would definitely fill the knowledge gap in the extant literature as suggested by [8] who urge subsequent action to measure the impact of the factors on user information security behavior because of lack of information security awareness.

This study will contribute to knowing the future suggestions from the previous literature contained in one paper, which will help researchers in the future to study it further. This study will be an addition to an attempt to reduce bias in the summary of evidence for the ten (10) dimensions of protection behaviors. As the protection behaviors, concepts and dimensions are still developing, the results of this paper would open up possibilities for future studies in this area.

The remainders of this paper are organized as follow: the background of the study is introduced followed by the details of the research methodology. The presentation of findings that emerged from the literature review has been clearly stated from which conclusions are drawn. Finally, the authors' recommendations and grounded insights, as well as the roadmap of further research, are mentioned.

2. BACKGROUND OF THE STUDY

Various sectors have reported particular forms of breaches; for instance, information, communications or utility firms are more likely to have breaches related to personally owned devices [9]. The research was in accordance with the prerequisite of the international quality standard for market research. Indeed, organizations that enable their employees to use their personal equipment depend strongly on the correct security settings of their employees' devices [10]. According to [11] several measures are available to help lessen the challenges and risks of BYOD. For example, Mobile Device Management (MDM) is one of the solutions to curtail the proliferation and prevalence of threats of privacy and security in BYOD development. Detection of mobile devices seeking access to the network is possible when MDM is installed in an organization sever. The device's data, applications, and configurations can be controlled and managed.

Privacy-protective behavior could be enhanced by taking advantage on add-on tools such as Privacy-Enhancing Technologies (PETs) to protect data [12] because the end-user behavior plays a profound role in ensuring the security and integrity of the organizational business assets [13]. Protection behaviors in a work environment between colleagues enable an individual to see the performance of his or her colleagues' jobs securely in an equally demanding environment [14]. With a proper security setting, privacy may be protected by preventing unwanted or unintentional information leakage, which can have adverse implications for both people and organizations [15]. In addition, [11] stressed on the worries of legal issues related to data management and device security. Data loss prevention (DLP) software is considered a technical solution that can protect a user's privacy. DLP software can provide access to employees' data to help monitor their activity within the network. Records of the particulars will be updated in the log file. However, any compromise of security will be hard to monitor as personal devices are not fully owned by the organization and accessing them will be difficult. Upon any case of a security breach, notification procedure will be conducted and risk assessment is performed to establish the possibility of data loss.

In an article entitled Best Practices for BYOD Security [7] listed the benefits (e.g. mobility, increase of computing power due to ease of use, and the blend of engaging features) as well as the challenges and risks (e.g. security vulnerabilities) brought about by BYOD adoption. User behavior has become one of the factors of success of security as it is now an essential topic in security [16]. Technological

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and physical security measures are operated by users to safeguard information assets and information systems within their particular territory. Therefore, understanding the effect of behavioral pattern towards the protection of information assets and different types of vulnerabilities, such as leakage of data is crucial. Previous research has agreed that user behaviors result in obvious risk in the protection of information assets [8]. An adequate level of knowledge or capacity to safeguard themselves from online threats may not be possessed by many end-users.

By combining the results of previous studies, new findings can be highlighted by the importance of focusing on the dimensions that play a role in leaking information due to wrong human behaviors. This study will be positive for organizations that are unaware of the importance of looking and focusing on wrong employee behaviors by increasing security awareness spreading and applying regulatory procedures and policies. According to the study by [17] human behavior in complying with security policies is a major contributing factor to security vulnerabilities.

Based on the foregoing, end-users need awareness with regard to protecting information assets [18]. To our knowledge, this factor is currently unavailable in research.

3. METHODOLOGY

The Systematic Literature Review (SLR) approach is adopted in this study and reviewed four (4) online databases, namely: IEEE Xplore, Science Direct, Springer Link, and Taylor and Francis. In particular, these databases were used in the literature search using the keyword "protection behavior" as well as the entire string of keyword. The review included only published articles observing the following guidelines:

a. Publications of original data regarding dimensions contribute to protection behaviors; and
b. Articles published between 2010 and 2019.

According to the presence of a systematic review based on the search keywords, 20 articles were obtained from the IEEE Xplore, 23 articles were drawn from the Science Direct, 2 articles were taken from the Springer Link, and 12 papers were obtained from Taylor & Francis. In total, 57 articles were selected for consideration in this study. Association to the dimensions of protection behaviors can be made through these articles. Table 1 shows the subtleties of the inquiry, as indicated by the above criteria.

Table 1: Selected Articles Related to the Criteria

S/No	Database Name	Total of articles founded	Total of articles excluded	Total of articles selected
1	IEEE	721	701	20
2	Science Direct	183	160	23
3	Springer Link	18	16	2
4	Taylor & Francis	319	307	12
Total	4	1,241	1,184	57

In this study, PICOC [19] is utilized to identify behavioral dimensions, which increase data and information breach. Research Question Population, Intervention, Comparison, Outcomes, and Context (PICOC) structure of questions are shown in Table 2. The primary focus of this review is to identify the dimensions that contribute to protection behavior from various industries.

Table 2: Summary of PICOC

Population	Employees
Intervention	Protection behaviors
Comparison	None
Outcomes	Dimensions of protection behaviors
Context	Review(s) of any conference and journal articles of protection behaviors. There are no restrictions on the type of study applied.

Based on the PICOC structure, the primary questions of this study are as follow:

1. What are the dimensions that contribute to protection behavior?
2. How the dimensions that contribute to protection behavior are recognized in research? What are the demographic profiles of the related studies? What samples and methodologies are used?
3. Is there any evidence regarding dimensions that contribute to protection behavior?

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. What recommendations or future works are suggested from the existing literature?

Therefore, the consequences of the investigation were sorted out and introduced in the following section.

4. ANALYSIS OF THE RESULT

This research shows the variation of dimensions adapted to consider protection behaviors found in previous studies. The main ten (10) dimensions for protection behaviors are also classified by the underlying concepts. This paper is also related to the different concepts of contributing elements including the used criteria of the study, theories and point of view of the paper, the dimensions that contribute to protection behavior from various industries, and recommendations or future works suggested from existing literature.

4.1 What are the Dimensions that Contribute to Protection Behavior?

The first research question of this literature review is aimed to recognize what dimensions are predominantly stated by scholars exploring various dimensions that contribute to protection behavior. The analysis shows different theories, concepts, and approaches are factors that contribute to the variation in protection behavior dimensions. The majority of the existing studies used Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and Organizational Culture (OC) concepts to conceptualize protection behavior. Based on selected articles in this review, most of the primary studies discussed on the PMT and the theory has been adopted in 40 articles. Table 3 summarizes the theories and approaches adopted in the selected articles.

Table 3: Summary of Theories and Approaches

No.	Theories	No. of Articles
1	Protection Motivation Theory	40
2	Theory of Planned Behavior	23
3	Organizational Culture	27

Majority of the selected articles utilized Protection Motivation Theory (PMT) variables such as self-efficacy. This can be seen by the distribution of articles as follows; 34 of the articles used self-efficacy dimension, 27 of the articles used response efficacy dimension, 22 of the studies used perceived severity dimension, 20 of the studies used perceived vulnerability dimension. Another selected studies utilized Theory of Planned Behavior (TPB) variables and this can be seen by the distribution of studies as follows: 18 of the studies used attitude towards dimension, 18 of the studies used response cost dimension, 16 of the studies used subjective norm dimension, 5 of the studies used security self-efficacy dimension and 5 of studies used Perceived behavioral control dimension. Organizational Culture (OC) was utilized in 8 studies by used the information security awareness dimension. This review will explain ten (10) dimensions that contribute to protection behaviors as tabulated in Table 4 and presented in Figure 1.

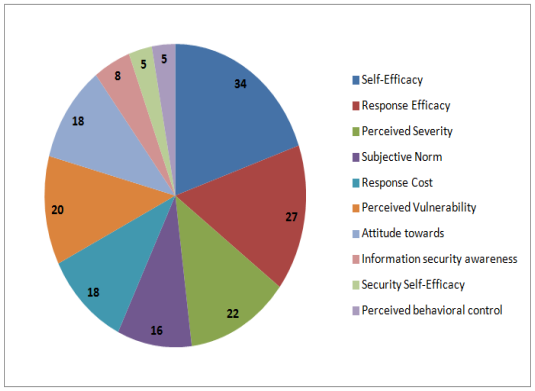


Figure 1: Number of Frequency Articles in Each Dimension

4.2 How the Dimensions that Contribute to Protection Behavior are Recognized in Research? What are the Demographic Profiles of Related Studies? What Samples and Methodologies are Used?

On the other hand, the second research question of this study is to explore the demographic details of similar studies related to year, location, sample, perspectives, theories and methodologies. The findings from the analyses through SLR call for potential further studies. Articles that were published between 2010 and towards the end of 2019 were chosen. Fig. 2 shows the pattern of the chosen articles related to protection behavior issues that reveal about the fluctuating trend from 2010 to 2015 in terms of publications; however, there had been a surge of publications starting from 2016 to 2019.

Journal of Theoretical and Applied Information Technology
15th September 2020. Vol.98. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

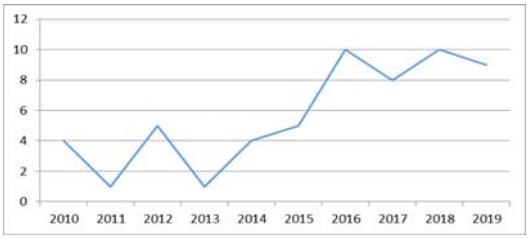


Figure 2: Number of Articles by Year

Most of the articles have focused on protection behavior in the United States and Canada as revealed by 21 articles, followed by Asia Pacific countries in Malaysia, Taiwan, China, Hong Kong, and Indonesia by 13 articles. The number of 14 articles distributed by the number of 7 studies between European countries such as Germany, Sweden, Finland, United Kingdom, Netherlands and Belgium, and the 7 articles between African countries, namely: Nigeria, South Africa and Mauritius. The studies were the least prevalent with 3 articles in the Middle East countries such as Palestine, Iran, and KSA and two studies in Australia. There are 4 articles, the location of which has not been tested and their data collected has not been determined (Figure 3).

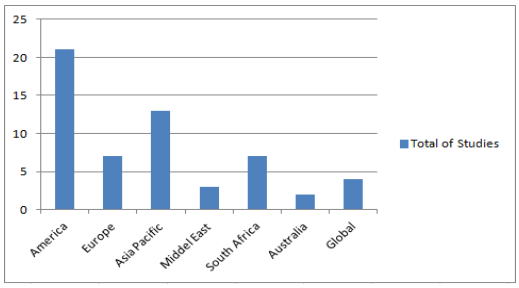


Figure 3: Number of Articles by Region

According to the results of the SLR, most samples were taken by a government or company employees with 31 studies, followed by 14 articles wherein samples were taken from students at the university or college. Six (6) articles took samples from the users of the global social site and 2 articles took samples from customers in banks. There are four (4) studies in which samples were not allocated (Figure 4).

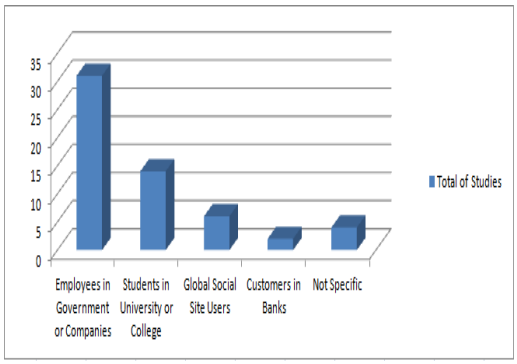


Figure 4: Number of Articles by Respondent Type

Based on the review, most articles on protection behavior adoption concentrated on the individual-level perspective, followed by an organizational-level perspective. Most of the researches on protection behavior focused on individuals and referred to because of the critical role individual beliefs and perceptions play in protection behavior. A broad range of factors associated with individuals like threat assessment, confrontational assessment, and habits have been focused on studies. These factors motivate individuals to conduct protection in conjunction with users' intentions and attitudes based on the theory of motivation to protect. The results of some studies indicate that data breaches due to access to confidential information by unauthorized individuals (Figure 5).

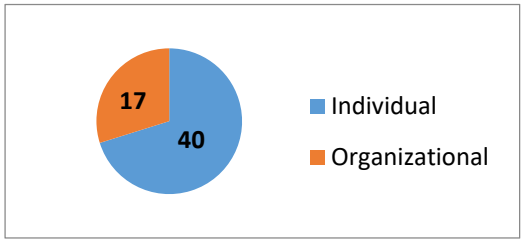


Figure 5: Perspective Level of Protection Behaviors Studies

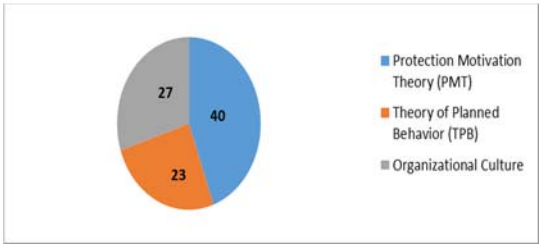
Furthermore, 40 of articles used the Protection Motivation Theory (PMT), 23 of the articles used the Theory of Planned Behavior (TPB) and 27 of the articles used the Organizational Culture approach, as shown in Figure 6. Most studies in the results of this SLR study have focused on adopted the use of PMT theory because protection measures are constructed by intentions or behaviors that show PMT components could be practical for single or community interventions and a model that can be

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

valuable in predicting the adoption of protection techniques. PMT allows plenty of value in recognizing protection intentions and behaviors.

Figure 6: Theories and Approaches used in Protection Behaviors Studies

Figure 7 shows the studies using the quantitative, qualitative, and mixed approach. It



is shown that the most utilized research approach was the quantitative method with 44 articles, followed by 9 articles adopted a qualitative method, while only 4 articles adopted a mixed-methods approach. Most studies in the results of the SLR study focused on quantitative research with a view to identifying the problem of protective behaviors and how to develop an appropriate conceptual model. It was used after an observation that a phenomenon that must be analyzed, studied, and explained by adopting models and statistical numbers.

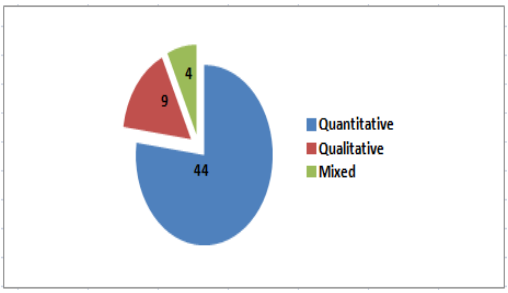


Figure 7: Research Methodologies used in Protection Behaviors Studies

4.3 Is there Any Evidence Regarding Dimensions that Contribute to Protection Behavior?

The third research question aimed at understanding the identified dimensions that contribute to protection behavior.

4.3.1 Self-Efficacy

A study [20] claimed that there exists relative ease when a specific behavior is demonstrated as self-efficacy. Self-efficacy has been utilized in place of perceived behavioral control in the proposed conceptual model because it fits for usage in that it explains the knowledge of cybersecurity that will increase employee compliance to routine security procedures and practices [21].

An individual's capability to manage random security incidents through his/her expertise is described as self-efficacy [22]. The previous encounter of dealing with many computing resources issues was believed to be a contributing factor toward one's self-efficacy. Both IT and security technology usage were notably impacted by self-efficacy, as empirical studies had shown [23].

A proposed framework by [24], self-efficacy was used to identify those types of measures and skills which are required for information protection. Important and positive effects on information security behavior due to self-efficacy were shown in their findings. Another study by [25] found that self-efficacy has a positive connection to an insider's view of security self-efficacy in psychological capital (PsyCap). It was also considered as a construct of role-breadth psychological abilities and resources embodying crucial work-related motivational resources.

An organizational perspective on public universities in Malaysia, employees' self-efficacy towards the conformity of Information Security Policy (ISP) has been positively impacted by Information Security Culture (ISC) [26]. As such, the positive influence of employee intention to comply with ISP was seen with self-efficacy. Based on the study by [27], a model has investigated that Quick Response (QR) codes were used as a measure of the use of new technology and hypothesized that online users' attitudes toward QR codes adoption were positively affected by self-efficacy by student-participants in universities in the US.

Another study by [28] discovered that psychological possession and the intention not to execute secure behaviors were influenced by one's personal orientation toward collectivism. The impact of psychological ownership was seen in the protection motivation constructs and on the intention for the population in US and China. They hypothesized that perceptions of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

self-efficacy would be increased by psychological ownership of the information and the end user's intention of not protecting information will be negatively affected by self-efficacy.

In another research by [29] they hypothesized that someone with high regard of their self-efficacy is less afraid of perceived threats than an individual who has less confidence in his or her ability to handle security threats. Self-efficacy generally appears to be the most effective dimension and important in the PMT for students in a university in US.

Changes in individual behaviors are very much affected by self-efficacy in terms of influencing protection intention and behavior. It has been discovered in this study that an essential effect on protection was due to self-efficacy. Studies should consider the examination of protection behaviors in this regard.

4.3.2 Response Efficacy

Perceived response efficacy has been described as a user belief in technology effectiveness in mitigating the threat to which the user is exposed [12]. Observed by [29] that panic as the central component of the theory growth and presume self-efficacy as a determinant of the extent of fear, which in turn, regulates the course of events moderated by profit and challenges of response efficacy. One's belief in the efficiency of a given behavior on reducing a threat was measured by response efficacy.

A study states that response-efficacy is the ability or capacity to encounter potential threats using efficient resources and is a person's belief in the organizations' capability to handle security violations [22]. Another study by [30] shown that response efficacy is one important element that influenced security behavior. The description stated as users' view of the efficiency of security controls and ISP compliance.

The study by [12] has found that a convincing reaction on individuals' intention to use Privacy Enhancing Technologies (PETs) was seen through perceived response efficacy and they presumed that perceived response efficacy positively influenced the intention to use PETs for German university students. In research by [27], the response efficacy means online users' belief that QR codes can assist them efficiently by protecting their account information. A proposed model of psychological capital (PsyCap) by [25] revealed that one of the residual mechanisms of the surviving appraisal was response efficacy and it regards to the subconstructs of PsyCap. The response efficacy was insiders' confidence that the safety measures they conducted were effective in shielding their organization's information security. The study hypothesized that insider PsyCap is favorable in terms of their views that response efficacy and insiders' perceptions of response efficacy were positively related to their defense motivation.

Another proposed model of BYOD security policies (ISSP) by [31] they observed that security awareness programs might result in employee response efficacy (positively). They planned that high perceived response efficacy might develop users' intention to abide with relevant policies. They hypothesized that perceived response efficacy optimistically affected an employees' intention to obey with BYOD ISSP, the organizational BYOD IT Support positively affected employees perceived response efficacy in demonstrating BYOD compliance behavior and A SETA program positively influenced perceived response efficacy of employees' compliance activities.

Through their research [32] theorized that plans to carry out malware prevention behaviors when using private mobile device were amplified by response efficacy and its effects on intention to perform malware avoidance behaviors vary across the situation. It is established that among the presented PMT variables, the most constant forecaster in contrast to other risk appraisals and other managing appraisals was response efficacy [33]. They hypothesized that response efficacy has positively predicted security intentions.

According to the study by [34], the connection between response efficacy and information security actions was uncertain as well. The authors have hypothesized that a negative affiliation has occurred between apparent response efficacies of taking information security actions with teachers' challenging information security performance. One of the most important predictors of taking precautions was response efficacy and it is able to be applied by researchers and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information-security professionals to develop security teaching, training and awareness movements directed to safe online banking. They hypothesized that response efficacy positively influenced precautionary online behavior [35].

According to a study by [36] the students were more confident about performed protection behavior rather than avoidance behavior. It was pointed out that time and costs to the consumers were the basis of the measures to defend and evade such attacks. They hypothesized that response efficacy has an encouraging outcome on consumers' intention and behavior to use their own device in accessing Universiti Sains Malaysia (USM) proprietary websites in higher education. The amount to which staff suggested a response that will successfully decrease the level of risk of response efficacy. It was found out in a study that staff's response-efficacy, when dealing with cyber security occurrences, was improved by their cyber security familiarity and their cyber security protection behavior was positively influenced by employees' response efficacy [37].

In the study by [38] the response efficacy was among the more dominant predictors of information security-related behavioral products for students university. They hypothesized that perceived response efficacy increases, so too does one's intentions to continue to engage in protective security behaviors. The response efficacy was the idea concerning the consequence of the shielding behavior, if taken [39].

According to a study by [28], they observed that the affected process was related to response efficacy when the elevated intensity of psychological ownership are at hand. Awareness of response efficacy would be raised by the psychological ownership of the information. There have been a wider confirmation in a study [40] projecting that consumers firmly believed in the ability they acquire to look after their devices in order to adopt good security behaviors to guard their smartphones.

There was a significant impact of the response efficacy in removing or preventing possible harm in the protection behavior in the study. The effectiveness of the response was the second most affected dimension in the protection behavior according to the results of this SLR study.

4.3.3 Perceived Severity

Based on the study by [29] it is mentioned the Health Belief Model (HBM) explained perceived susceptibility and perceived severity of the disease affects an individual's healthcare professionals actions in the face of the risk of illness. The moderation test results disclose that self-efficacy extensively decreased the results of awareness and perceived severity in panic. In the threat appraisal, the perceived severity was among the dangers that determine maladaptive behavior. The perceived severity of privacy threats positively influenced the intention to use PETs [12]. On the other hand, a study stated that the severity of the consequences of the incident and the possible amount of threats to the security of one's Institution's information is related to Perceived Severity (PS) [22]. The study by [41], has explained that perceived severity correlates with the original Health Belief Model (HBM) constructs. It is the individual's thought in the severity of the security danger and its effect on lifestyle.

The extent of physical harm, psychological harm, social dangers, and economic threat that is a risk to a person was explained as perceived severity by [42]. In the BYOD solution, staff could react in various ways based on their perceived severity for implementing it. The proposed hypothesis is the idea to implement BYOD is negatively impacted by the perceived severity of negative consequences.

According to the study by [34], they hypothesized that the perceived severity of online information security occurrence has a harmful association with teachers' problematic information security behavior. Another study by [43] uncovered the function of the perceived severity concerning the harmful consequences of IT risks in affecting the motivation of crowd workers to evade suspicious crowdsourcing assignments. They presumed that the possibility of a crowd worker being occupied in a doubtful crowdsourced task amplifies as the perceived severity of being negatively affected by the task reduces.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A consumer's assessment of the severity of the effects of a hostile security incident happening to them has stated a perceived severity. It is hypothesized that perceived severity positively impacts perceived risk and online preventive behavior for banking users [35]. A study applied the PMT model to relate the influence of consumers before computer security understanding of their perceived severity as an overarching theory [37]. They hypothesized that workers' perceived severity of cyber attacks is positively related to their cyber security experience. According to a study by [39] it was claimed that if the population consumers of the US believe that the consequences of threats would be severe, they are more expected to plan to take protective actions with their computing device. It is presumed that personal computing security intentions would positively affect perceived severity.

The perceived severity dimension is one of the most influential dimensions of protection behavior, according to the results of this study. This dimension was used to find out how people view the harmful consequences of an event that may result in neglecting non-compliance with protective behaviors.

4.3.4 Subjective Norm

Subjective norms are described as someone's view of the perceptions of people important to them of given behavior and opinion of top management [22]. Some authors defined subjective norms as behavioral expectations of someone influenced by their view of social pressure led to them by influential figures in their lives [21]. In the security context, workers are more likely to act firmly if those around them behave steadily and require such conduct from them. They have hypothesized that collaborative, competitive, creative, and controlled have a positive outcome on subjective norms.

TPB suggested that influential figures of someone (such as bosses, colleagues, and parents) have a degree of control to influence his/her behaviors by influencing an individual's agreement with a new security policy. They hypothesize that subjective norm has a constructive result on online users' intention to take on [27]. The compelling normative beliefs optimistically inclined motivation to execute the relevant kind of actions for employees in companies. Subjective norms are also allocated to perceived social pressure to perform or not carry out behavior.

The research shows that subjective norms notably affected ISC intention in organizations and they hypothesized that subjective norms positively influenced ISC intention [44]. The study by [30], one of the critical factors that influenced security behavior was subjective norms (or normative beliefs). It described as perceived expectations of colleagues and superiors. Another study by [45] hypothesized that there was a noteworthy variation in the regular level of subjective norms between violators and non-violators for employees of the Midwestern University in the US.

According to a study by [46] it described the subjective norm as someone's view about a certain action influenced by the decision of significant others. In social media, the subjective norm has a significant role in affected users' behavioral intentions. They hypothesized in the model that subjective norm has positively affected WeChat users' intention to share Social Crisis Information (SCI). In the study by [33] they believed that subjective norms were better prepared to seize social power on defensive actions. They hypothesized that subjective norms have positively predicted security intentions. According to a study by [47] the subjective norms were the values, beliefs, and views a worker has in regard to information security and its connected parts. They hypothesized that there was a positive connection between information security policy obedience subjective norms and perceived obedience among EMU staff.

A study observed that the Belgium population influences the subjective norm towards the intention of behavior by following the implementation [48]. They hypothesized that subjective norm was a constructive predictor of a plan in the direction of protective behavior. A study proposed that system quality influenced by subjective norms on how an individual was likely to interact with a system for students in a US university [49]. The system quality also had a constructive effect on subjective norms and it had a positive influence on intentions. They hypothesized that system quality had a positive connection with subjective norms of security and subjective norms of security had a positive influenced behavioral security intention.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Another study by [18] stated that proper information security policies have a crucial impact on the formation of subjective norms towards information security behavior within companies. The subjective norms lead to social pressure for people to execute or not execute a specific action. They hypothesized that organizational policies have a constructive result on subjective norms towards performing Information Security-Conscious Care Behavior (ISCCB). According to a study by [39] the subjective norm had an important impact on security intentions and recommended future research to uncover the function of the descriptive norm. They hypothesized that subjective norm has positively influenced personal computing security intentions.

Some studies in this SLR study have focused on the subjective norm, which is known as the impact of the individual expected behavior through awareness of the social pressure exerted by people in the context of behavior protection. It has been suggested that employees are protected if the people around them behave protectively.

4.3.5 Response Cost

According to a study by [50] the response cost was the social, physical and monetary expenditures of performing the required response. It leads consumers towards maladaptive responses, and even if someone perceives the existence of a strong ability to cope, response costs push that individual far from adoptive responses. It has been mentioned in a study that the response cost calculates any cost related to taking adaptive coping responses [27]. An online consumer may be hesitant to adapt to the current technology which has functions if the response cost is high for using a new one.

A proposed model of psychological capital (PsyCap) by [25], the response cost was the insiders' perceived cost of behavioral security adaptations. The recognized associations between PsyCap and positive organizational behaviors, such as bigger organizational citizenship, usage of a reduced perceived response cost in adapting behavior to guard the institute. In a proposed model of BYOD security policies (ISSP) by [31], they observed that security awareness programs have one of the affected was response costs (negative). The accessibility of an IT support panel for BYOD raises workers' response-efficacy and perceived integrity. Related to the BYOD solution, they suggested that BYOD affected by perceived response cost on obedience will be observed by perceived freedom risk.

In the study by [51], response cost was negatively influenced by the practice of habit of complying with IS security policies. They hypothesized that response cost negatively affected employees' intent to obey with IS security policies and the habit negatively influenced response cost. According to the study by [32], the theoretical contributions included an extended model based on the protection motivation theory that revealed the consumers intention to avoid malware risks in BYOD.

The study by [34] observed that the perceived response expenses of using protective events have a positive connection with undertaking difficult information security actions for teachers in schools. In the study by [35] they explained that response costs were a consumer's viewpoints about how costly managing the coping response will be to them. According to a study by [39] the response cost was seen to have a crucial function in the individual's computing domain, such that amplifies in perceived response cost negatively inclined intentions to carry out security behaviors.

According to a study by [28] they observed that response cost established the only important effect on intention. They hypothesized that psychological ownership of the information had lessened view of response cost and response cost of doing data backups has a negative influence on an end user's intention not to guard information. The study for owners of smartphone devices showed a major negative relationship between response cost and the intention to take on in security behavior. He hypothesized that response costs have negatively influence smartphone security intentions [40].

A large percentage of the results in this SLR study indicated that the protection motivation was negatively influenced by response costs. It has been quoted by staff ignoring security procedures because it limits and deters the routine flow of operational operations, and response costs have a negative effect on the protection driver.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.3.6 Perceived Vulnerability

The behavioral intention has a positive impact on people with knowledge of adaptive responses and recognize it helpful for solving their perceived vulnerability to a risk that causes difficulty [50].

Perceived vulnerability is an individual's evaluation of the likelihood of threatening actions and the option of dangers to the security of a specific organization's information [22]. Another study by [30] one of the critical issues that impact security behavior was perceived vulnerability (or perceived probability of a security violation) and it explained users' opinion of the occurrence's potential of a security risk. The study by [32] as a result, hypothesized that perceived vulnerabilities contributed effected on intention and whereas hypothesized that the contributed effected of perceived vulnerability on the intention for students in the university.

In the study by [34] it explores the relationship between perceived vulnerability and response costs regarding information security behavioral intentions. They hypothesized that the perceived vulnerability of potential victims to online information security occurrences has a negative connection with teachers' problematic information security behavior. According to a study by [35] they explained that perceived vulnerability was a consumer's online banking assessment of the likelihood that an aggressive security incident will occur to them. According to PMT, perceived vulnerability is a main predictor of protection motivation as well. They hypothesized that perceived vulnerability positively affected perceived risk and perceived vulnerability certainly influenced precautionary online performance.

In the study of [37] they explained that perceived vulnerability indicates the degree of which staff senses the risk from a cyber-attack episode and sense preventive ways and actions that are lacking. They hypothesized that employees' cybersecurity experience positively links with their perceived vulnerability because of cybercrimes and employees' perceived vulnerability positively affects their cybersecurity protection behavior. According to a study by [49] one of the threat appraisal dimensions was perceived vulnerability and it has a direct impact on attitudes. It was stated that the perceived vulnerability of students in the university is not affected by the low-quality systems. They hypothesized perceived vulnerability to risk is negatively impacted by system quality but, in contrast, has a positive impact on outlook toward security behaviors. According to a study by [39] perceived vulnerability was known as the degree to which a user thinks they are expected to have security risks to their computing device. The perceived vulnerability to risks means that the population consumers in US individually predicted the likelihood that a security threat will happen.

The perceived vulnerability dimension is among of the constructs of the protection motivation theory, which plays a role and a direct indicator of the motives for protection in this study. The perceived vulnerability was adopted in this study which a notable security vulnerability that did not contribute significantly to the practices of adopting antivirus programs or strengthening the password intensity.

4.3.7 Attitude Towards

The Theory of Reasoned Action (TRA) and the Technology Acceptance Model (TAM) are relied upon to inspect workers' perceived concerns and perceived benefits, and it reflected on their outlook on using BYOD mobile devices [50]. Attitude is defined as a person's positive or negative stance toward having in a specified behavior is defined as attitude [22]. According to a study by [52] the attitude was defined as someone's positive or negative outlook toward engaging in a specified behavior. Another study by [21] mentioned that TPB established that a positive attitude influenced behavioral plans. Hence, staff with a positive view of their organization's cyber security will likely to obey such policy and guidelines. Equally, those with a negative outlook will not voluntarily comply.

The attitude was one of the impacts on gender, age and profession of the social site users' behavior of social network users [53]. They hypothesized that people who were worried more about their privacy and took privacy issues more critically (attitude) are more alert of their online communication than the less concerned persons. In the study by [27] they observed that QR codes are observed as a method to guard account information. They hypothesized that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

outlook toward QR codes has a positive consequence on online users' plans to take up.

The findings in the study by [54] suggested that conscientiousness was crucial in explaining the attitude towards the administration of technical security methods. Besides, the results indicated that when executive managers were tackled with information security standards or guidelines, the personality qualities of conscientiousness and openness have a more dominant impact on attitude towards organizing security measures than without moderators. The results of the study by [44] founded that personal norms, involvement, and commitment to their organization notably affected the workers' outlook towards ISC intention. However, differing from the author's belief, there is no influence of attachment towards the attitude of workers towards ISC. Attitudes towards ISC, perceived behavioral control, and personal norms dominantly influenced the intention of workers towards ISC.

According to a study by [26] they proposed an Information Security Culture (ISC) model through seven newly formulated dimensions to examine its influence on workers' Information Security Policy (ISP) compliance behavior which includes the attitude towards it. They hypothesized that ISC positively affected employees' outlooks towards conformity with ISP and attitude towards ISP compliance positively impacted employees' intention to comply with ISP. According to a study by [46], they described the attitude towards an individual's evaluation of behavior and it was regarding to WeChat users assessment of SCI sharing behavior. They hypothesized that attitude towards SCI sharing behavior has positively influenced WeChat users' intention to share SCI. According to a study by [47] the information system attitudes were that precise outlook concerning information security practices within one's association. They hypothesized that there was a positive correlation between information security policy obedience attitudes and perceived compliance among EMU workers.

According to a study by [49] as explained by TPB, attitudes were a rundown of applicable evaluations of behavioral beliefs and the force of those beliefs and were shaped independently for exact actions for students in the university. They hypothesized that outlook toward security behaviors was positively affected by perceived severity and perceived vulnerability. Security response efficacy and security self-efficacy also have the same effect. A study [18] mentioned that data security readiness modifies the shoppers standpoint performed by Information Security-Conscious Care Behavior (ISCCB). The authors claimed that data security mindfulness has a valuable outcome on attitude towards the ISCCB.

The results of this SLR study states that the user's behavior affects the attitude towards protection behavior because, in the nonexistence of a risk, it is possible that there will be no distinction in the result regardless of protection behavior because it is unlikely that the person who does not see any threat has a particularly strong attitude towards security behavior.

4.3.8 Information Security Awareness

Individual responsibilities of their own individual security which comes with accepting the importance of information security that is suitable to the organization and to operate accordingly were defined as information security awareness by [13]. Organizations are exposed to major threats due to the absence of strong security. This phenomenon has amplified researchers' apprehension of the connection between managerial information security awareness and action [55].

A significant gadget in the protection of information assets was an information security awareness program. According to a study by [30] for employees in Greece, one of the critical factors that influence security behavior was information security awareness and it described facts about information security and the precise ISP of the institute. The study by [56] includes potential cultural factors linking to students from diverse backgrounds as an extension to the traditional advancement of an information security awareness program. The findings recommended that some cultural factors such as mother tongue, neighborhood and the like would have an influence on security awareness levels and should be weighed in when setting up and developing an information security awareness program.

Because of the overwhelming dangers of information security threats, various

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information security awareness approaches were projected in order to help change the user from being ill-informed into a security-minded user by one way to reduce these attacks and their damage by raising the Information Security Awareness (ISA) [8]. The study by [57] revealed that implementing an information security policy does not automatically assure that all workers recognize their responsibility in making sure the security and safeguarding of information assets. It is vital to design and align an information security awareness movement for the information security policies' ultimate goals, objectives, and requirements. The research discussed an information security awareness method that aims to develop positive security behaviors using the behavioral intentions models like the theory of reasoned action and the protection motivation theory.

The study by [58] used the protection motivation theory to research on the impact of information security awareness on desktop security performance for students in US and the importance of it for the global community. According to a study by [59] they hypothesized and predicted that plan to obey to information security policies was enhanced if general information security awareness for staff is included in the prediction model of the TPB. According to the study by [60] the study decomposed information security awareness (ISA) into general information security awareness (GISA) and information security policy awareness (ISPA), and discovered how these aspects influenced knowledge sharing performance for users in social networking sites.

According to a study by [37] they explained the difference among the workers who were alert of cybersecurity policy versus those who do not acknowledge the existence of policies. Management can offer standard in-house information security awareness workshops and training to inculcate a positive mindset of their staff regarding information security issues. As indicated by the investigation conducted by [18] information security awareness changes the workers standpoint towards performed ISCCB. They inferred that data security awareness has an impact on attitude towards the ISCCB.

Information security awareness is among dimensions in this study and its organizational culture. The studies have suggested that the most suitable security awareness theme can be initiated based upon a consumer's personality, thus possibly improving the user's IT security aptitude. The information security awareness dimension also focused on the ways to make the most of this offer end-users with more useful awareness based upon the risks they present to systems.

4.3.9 Security Self-Efficacy

Security self-efficacy was described through PMT that is coping appraisal as one determinant that decides whether a person takes on a specified behavioral reaction. An experimental study concluded that a person's coping appraisal amplified his readiness to execute and the coping behavior also improved [61]. A proposed model of psychological capital (PsyCap) by [25] shows that PsyCap constructs positive resource capabilities to impact the efficacy positively based facets of the coping appraisal (security self-efficacy and response efficacy), while negatively linking to other facets (reducing risk severity by virtue of its hopeful, optimistic, self-efficacious, and resilient qualities). They included security self-efficacy as an antecedent to protection motivation. Insiders' perceptions of security self-efficacy were impacted in a positive manner to their protection motivation.

The study of [41] hypothesized that information security self-efficacy was connected positively to computer security usage. The study by [49] observed that system quality influenced users' security intentions and perceptions of the effectiveness of their measures without utilizing direct messaging to warn, train, or reassure them. Information security self-efficacy is also found as one of the most critical perspectives that extensively prompted ISCCB [18].

The security self-efficacy dimension was one of the items adopted from PMT. In previous PMT studies, strong dependability was seen in the security self-efficacy dimension and it is a precursor to protection motivation.

4.3.10 Perceived Behavioral Control

Theoretically, perceived behavioral control was one of the beliefs that affected a person's volitional behavior by his/her

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

motivation [27]. According to a study by [30] perceived behavioral control is one of the major aspects that influences security behavior and it explained users' judgment on how easy conformity is and the degree of control they have on implementing security tasks. Given that an individual is able to manage his or her actions, the intention will then determine his or her behavior. Although actual behavioral control is what controls the result of intentions, most purpose use perceived behavioral control as a proxy because of the challenges linked to observing actual behavioral control. This may explain the weak influence of perceived behavioral control. The perceived behavioral control had a minor influence on low power distance with workers' influence boosting their behavioral control [59].

According to a study by [46] they described affected behavioral intention as a person's perception of how easy to perform in a behavior called perceived behavioral control. They hypothesized that perceived behavioral control would have a positive impact on WeChat users' intention to share SCI and users Actual behavior (AB) of sharing SCI. It concluded an insignificant link between attitudes, subjective norms, and perceived behavioral control and information security compliance perceptions. They hypothesized that perceived behavioral control concerning compliance and information security policies and perceived compliance is positively connected among EMU staffs [47].

Some of the studies in the SLR result used perceived behavioral control as an alternative because of the challenges linked to measuring actual behavioral control, although actual behavioral control is predominantly moderating the effect of intentions. The perceived behavioral control dimension has a little significant impact, with employees' influence on their behavioral control.

5. RECOMMENDATIONS FOR FURTHER RESEARCH

The fourth and last research question is to synthesize recommendations for further research in the field of protection behaviors. Following a review of the SLR studies conducted on protection behaviors, it was revealed that various researchers individually introduce the impact on protection behaviors by emphasizing different dimensions.

The study of [18] suggested the need to develop the proposed conceptual framework that stresses more on awareness as the determining element in preventing security violations. There are limited studies regarding the field of information security that explains the recommended policies for different users with different situations and personalities. The study of [12] suggested making use of the PMT and its facets. Since privacy threats are of high relevance to individuals, while the application of PETs can directly alleviate these threats and PMT was previously used to discuss information security behavior concerning threats related to IT assets. Another study by [14] advised on exploring PMT facts from a security standpoint related to the function of culture in using protective technologies which could be found in insiders' motivations to protect their companies from security risks. They proposed future researchers to investigate the conceptual model of the recent research by increasing various influential variables for the acceptance of online banking besides the variables used in this study which were perceived security, perceived risk, and trust to improve future research results [62].

The study of [48] advised to consider digital skills and other interpersonal differences as significant differentiators for the PMT model towards the intention to take protective measures. The theoretical model proposed in the study by [50] suggested that future studies focus on developing a technological system that duplicates user behavior using independent variables and calculating them against risky factors to guess behavioral intentions.

According to the study of [63] the researchers advised researching on the impact of BYOD on work-life balance, and issues involving BYOD and its influence on self-perceptions of workload and performance. They suggested considering the varied situation and the intrusiveness of BYOD Information Security Policies (ISSP) [31].

Cyber Security Malaysia has come up with procedures on information security for small and medium-sized enterprises (SMEs) which limited the study to sample size in only one organization. They suggested using the same

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

study for other SMEs. The guideline refers to the important aspects of dealing with information security and the fundamental principle in implementing information security [13]. According to the study by [41] they suggested a reproduction of research using other variety of samples from the target population because numerous the hypotheses used in this study were not supported during the analysis of the data collected. Through replication, the value of these hypotheses to the research model might be fully known and can obtain a sample that is more accurate for the target population, thereby escalating generalizability.

Given the general lack of information security awareness (ISA) for various reasons, it is important to constantly raise ISA standards to change them from uninformed users to security-minded users. In the future, action should be taken to measure the impact of these factors on user information security behavior [8]. According to a study by [61] they suggested the need for more in-depth research to study the relationship of security self-efficacy and the effectiveness of a positive response impact on data support, while threat assessment was negatively connected with this behavior in the context of file backups to defend against file loss.

Studies have suggested focusing on models and theories that help improve an employee's position because the behavioral intention model has proven to be only capable of influencing knowledge and behavior rather than the attitude of employees [57]. According to the study by [64] they suggested that they need to conduct an empirical study, test more key factors, especially those related to the characteristics of mobile devices, and develop the research to different aspects of mobile security behavior studies namely the way to deal with the risk of mobile crime and social engineering. They suggested that future research could investigate ways to develop Person-organization (PO) fit.

The organization's security culture or ethical climate can be good starting points for the next research [65]. In the study by [45] they encouraged other studies to consider testing similar factors in various organizations. It can be possible that more factors might influence workers behavior, such as personal innovativeness and awareness of security measures. Researchers recommended that indirect individual-level measurements or indirect cross-level measurements be used in a future study to extend the existing results [65].

Therefore, through the results of this SLR study, we will suggest that to develop the conceptual model related to protection behaviors through the use of PMT which helps to reduce breaches and information leakage when using BYOD. Because of weak support for hypotheses, while analyzing the collected data in previous studies, we suggest that a larger sample of employees be targeted so that the value of these hypotheses to the research model is well known and can be generalized more broadly and directly on individual-level measurements.

6. CONCLUSION

The main objective of this paper was to conduct SLR and identify dimensions of protection behaviors published between 2010 and 2019. The review disclosed the importance of developing protection behaviors within an institution in order to guard them from within and to influence workers' protection behavior. Another revelation was that useful protection behaviors have the possibility to develop employees' behavior in effect as a 'human firewall' that will assist in guarding organizational information against leakage.

Establishing protection behavior should involve altering the current protection behaviors to make it more effective in regard to managing protection issues. This calls for a switch in the behavior and outlook of workers dealing with information assets. More studies are required to explain the protection behaviors that should be included into organizations and to discover measures of best practice for the implementation of protection behaviors within organizations. The review provided in this paper is hoped to aid researchers who are planning to investigate this field further. The methodology of this systematic literature review can be modified, developed or improved later if it helps to obtain a more useful answer to the future research related to the criteria of the study.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

[1] J.F. Van Niekerk, R. Von Solms, Information security culture: A management perspective, Comput. Secur. 29 (2010) 476–486. https://doi.org/10.1016/j.cose.2009.10.005.

[2] Verizon Business ready, Data Breach Investigations Report, Comput. Fraud Secur. 2019 (2019) 4. https://doi.org/10.1016/s1361-3723(19)30060-0.

[3] Gartner, Newsroom, (2019) 13–16. www.gartner.com.

[4] A. Alhogail, A. Mirza, S.H. Bakry, A comprehensive human factor framework for information security in organizations, J. Theor. Appl. Inf. Technol. 78 (2015) 201–211.

[5] N. Ibrahim, N. Ali, An empirical exploration of information security management system (ISMS) in Malaysian Public Sector: A PLS-SEM method, Test Eng. Manag. 81 (2019) 3266–3275.

[6] D.M. and J.A. Abubakar Garba Bello, A systematic approach to investigating how information security and privacy can be achieved in BYOD environments, Inf. AndComputer Secur. 23 (2017) 450–475. https://doi.org/10.1111/1365-2664.12960.

[7] H. Romer, Best practices for BYOD security, Comput. Fraud Secur. 2014 (2014) 13–15. https://doi.org/10.1016/S1361-3723(14)70007-7.

[8] M. Alohali, N. Clarke, S. Furnell, S. Albakri, Information security behavior: Recognizing the influencers, Proc. Comput. Conf. 2017. 2018-Janua (2018) 844–853. https://doi.org/10.1109/SAI.2017.8252194.

[9] Rishhi Vaidya, Cyber Security Breaches Survey 2018, 2018. https://doi.org/10.13140/RG.2.1.4332.6324.

[10] R.E. Crossler, J.H. Long, T.M. Loraas, B.S. Trinkle, Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap, J. Inf. Syst. 28 (2014) 209–226. https://doi.org/10.2308/isys-50704.

[11] M. Dhingra, Legal Issues in Secure Implementation of Bring Your Own Device (BYOD), Phys. Procedia. 78 (2016) 179–184. https://doi.org/10.1016/j.procs.2016.02.030.

[12] C. Matt, P. Peckelsen, Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior, Proc. Annu. Hawaii Int. Conf. Syst. Sci. 2016-March (2016) 4832–4841. https://doi.org/10.1109/HICSS.2016.599.

[13] J. Kaur, N. Mustafa, Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME, Int. Conf. Res. Innov. Inf. Syst. ICRIIS. 2013 (2013) 286–290. https://doi.org/10.1109/ICRIIS.2013.6716723.

[14] C. Posey, T.L. Roberts, P.B. Lowry, R.T. Hightower, Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders, Inf. Manag. 51 (2014) 551–567. https://doi.org/10.1016/j.im.2014.03.009.

[15] F. Belanger, R.E. Crossler, Dealing with digital traces: Understanding protective behaviors on mobile devices, J. Strateg. Inf. Syst. 28 (2019) 34–49. https://doi.org/10.1016/j.jsis.2018.11.002.

[16] G. Saridakis, V. Benson, J.N. Ezingeard, H. Tennakoon, Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users, Technol. Forecast. Soc. Change. 102 (2016) 320–330. https://doi.org/10.1016/j.techfore.2015.08.012.

[17] R. Palanisamy, A.A. Norman, M.L. Mat Kiah, BYOD Policy Compliance: Risks and Strategies in Organizations, J. Comput. Inf. Syst. 00 (2020) 1–12. https://doi.org/10.1080/08874417.2019.1703225.

[18] N.S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N.A. Ghani, T. Herawan, Information security conscious care behaviour formation in organizations, Comput. Secur. 53 (2015) 65–78. https://doi.org/10.1016/j.cose.2015.05.012.

[19] CEBMA, What is a PICOC?, Cent. Evidence-Based Manag. (2016). http://www.cebma.org/frequently-asked-q

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

uestions/what-is-a-picoc/.

[20] A. Bandura, Self-efficacy -Bandura, Corsini Encycl. Psychol. (2010) 1–3. https://doi.org/10, 9780470479216.

[21] A. Onumo, A. Cullen, I. Awan, Integrating Behavioural Security Factors for Enhanced Protection of Organisational Information Technology Assets, Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud, FiCloud 2018. (2018) 128–135. https://doi.org/10.1109/FiCloud.2018.00026.

[22] S. Hina, D.D. Dominic, Need for information security policies compliance: A perspective in Higher Education Institutions, Int. Conf. Res. Innov. Inf. Syst. ICRIIS. (2017) 1–6. https://doi.org/10.1109/ICRIIS.2017.8002439.

[23] A.J.T. Chang, Understanding organizational information security usage from the risky decision-making perspectives, Proc. - 4th Int. Conf. Interact. Sci. IT, Hum. Digit. Content, ICIS 2011. (2011) 158–164.

[24] H.Y. Bojmaeh, The Main Factors Influencing Information Security Behavior, Int. J. Sci. Eng. Appl. 4 (2015) 353–356. https://doi.org/10.7753/ijsea0406.1004.

[25] A.J. Burns, C. Posey, T.L. Roberts, P. Benjamin Lowry, Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals, Comput. Human Behav. 68 (2017) 190–209. https://doi.org/10.1016/j.chb.2016.11.018.

[26] A. Nasir, R. Abdullah Arshah, M.R. Ab Hamid, A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions, Inf. Secur. J. A Glob. Perspect. 28 (2019) 55–80. https://doi.org/10.1080/19393555.2019.1643956.

[27] J. Yang, Y. Zhang, QR codes and authentication protection, Wirel. Telecommun. Symp. 2015-Janua (2015) 1–7. https://doi.org/10.1109/WTS.2015.7117256.

[28] P. Menard, M. Warkentin, P.B. Lowry, The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination, Comput. Secur. 75 (2018) 147–166. https://doi.org/10.1016/j.cose.2018.01.020.

[29] A. Noushin, L. Daniel, K. Jean-Pierre, S.G. Christoph, An integrated framework to examine mobile users' pathway from threat cognition to action, 7th Int. Symp. Digit. Forensics Secur. ISDFS 2019. (2019). https://doi.org/10.1109/ISDFS.2019.8757556.

[30] I. Topa and M. Karyda, Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance, Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 9264 (2015) 5. https://doi.org/10.1007/978-3-319-22906-5.

[31] A. Hovav, F.F. Putri, This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, Pervasive Mob. Comput. 32 (2016) 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007.

[32] D. Dang-Pham, S. Pittayachawan, Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach, Comput. Secur. 48 (2015) 281–297. https://doi.org/10.1016/j.cose.2014.11.002.

[33] S.R.C. Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, Understanding online safety behaviors: A protection motivation theory perspective, Comput. Secur. 59 (2016) 138–150. https://doi.org/10.1016/j.cose.2016.02.009.

[34] H.L. Chou, C. Chou, An analysis of multiple factors relating to teachers' problematic information security behavior, Comput. Human Behav. 65 (2016) 334–345. https://doi.org/10.1016/j.chb.2016.08.034.

[35] J. Jansen, P. van Schaik, Testing a model

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of precautionary online behaviour: The case of online banking, Comput. Human Behav. 87 (2018) 371–383. https://doi.org/10.1016/j.chb.2018.05.010.

[36] O.U. Franklin, M. Ismail Z., the Future of Byod in Organizations and Higher Institution of Learning, Int. J. Inf. Syst. Eng. 3 (2017) 110–128. https://doi.org/10.24924/ijise/2015.11/v3.iss1/110.128.

[37] L. Li, W. He, L. Xu, I. Ash, M. Anwar, X. Yuan, Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior, Int. J. Inf. Manage. 45 (2019) 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

[38] M. Warkentin, A.C. Johnston, J. Shropshire, W.D. Barnett, Continuance of protective security behavior: A longitudinal study, Decis. Support Syst. 92 (2016) 25–35. https://doi.org/10.1016/j.dss.2016.09.013.

[39] N. Thompson, T.J. McGill, X. Wang, "Security begins at home": Determinants of home computer and mobile device security behavior, Comput. Secur. 70 (2017) 376–391. https://doi.org/10.1016/j.cose.2017.07.003.

[40] S.F. Verkijika, Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret, Comput. Secur. 77 (2018) 860–870. https://doi.org/10.1016/j.cose.2018.03.008.

[41] C.L. Claar, J. Johnson, Analyzing home pc security adoption behavior, J. Comput. Inf. Syst. 52 (2012) 20–29. https://doi.org/10.1080/08874417.2012.11645573.

[42] V. Cho, W.H. Ip, A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy, Enterp. Inf. Syst. 12 (2018) 659–673. https://doi.org/10.1080/17517575.2017.1404132.

[43] N. Alomar, M. Alsaleh, A. Alarifi, Uncovering the predictors of unsafe computing behaviors in online crowdsourcing contexts, Comput. Secur. 85 (2019) 300–312. https://doi.org/10.1016/j.cose.2019.05.001.

[44] N.S. Safa, C. Maple, T. Watson, S. Furnell, Information security collaboration formation in organisations, IET Inf. Secur. 12 (2018) 238–245. https://doi.org/10.1049/iet-ifs.2017.0257.

[45] H.U. Khan, K.A. AlShare, Violators versus non-violators of information security measures in organizations—A study of distinguishing factors, J. Organ. Comput. Electron. Commer. 29 (2019) 4–23. https://doi.org/10.1080/10919392.2019.1552743.

[46] Y. Chen, C. Liang, D. Cai, Understanding WeChat Users' Behavior of Sharing Social Crisis Information, Int. J. Hum. Comput. Interact. 34 (2018) 356–366. https://doi.org/10.1080/10447318.2018.1427826.

[47] M. Rajab, A. Eydgahi, Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education, Comput. Secur. 80 (2019) 211–223. https://doi.org/10.1016/j.cose.2018.09.016.

[48] M. Martens, R. De Wolf, L. De Marez, Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general, Comput. Human Behav. 92 (2019) 139–150. https://doi.org/10.1016/j.chb.2018.11.002.

[49] M. Grimes, J. Marquardson, Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions, Decis. Support Syst. 119 (2019) 23–34. https://doi.org/10.1016/j.dss.2019.02.010.

[50] A. Duke Giwah, User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory, Conf. Proc. - IEEE SOUTHEASTCON. 2018-April (2018) 1–5. https://doi.org/10.1109/SECON.2018.8479178.

[51] A. Vance, M. Siponen, S. Pahnila, Motivating IS security compliance: Insights from Habit and Protection Motivation Theory, Inf. Manag. 49 (2012)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

190–198. https://doi.org/10.1016/j.im.2012.04.002.

[52] P. Ifinedo, Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, Comput. Secur. 31 (2012) 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

[53] S. Dhawan, K. Singh, S. Goel, Impact of privacy attitude, concern and awareness on use of online social networking, Proc. 5th Int. Conf. Conflu. 2014 Next Gener. Inf. Technol. Summit. (2014) 14–17. https://doi.org/10.1109/CONFLUENCE.2014.6949226.

[54] J. Uffen, M.H. Breitner, Management of technical security measures: An empirical examination of personality traits and behavioral intentions, Stand. Stand. Concepts, Methodol. Tools, Appl. (2015) 836–853. https://doi.org/10.4018/978-1-4666-8111-8.ch039.

[55] A.J.T. Chang, Roles of perceived risk and usefulness in information system security adoption, 5th IEEE Int. Conf. Manag. Innov. Technol. ICMIT2010. (2010) 1264–1269. https://doi.org/10.1109/ICMIT.2010.5492818.

[56] H.A. Kruger, L. Drevin, S. Flowerday, T. Steyn, An assessment of the role of cultural factors in information security awareness, 2011 Inf. Secur. South Africa - Proc. ISSA 2011 Conf. (2011) 1–7. https://doi.org/10.1109/ISSA.2011.6027505.

[57] T. Gundu, S. V. Flowerday, The enemy within: A behavioural intention model and an information security awareness process, 2012 Inf. Secur. South Africa - Proc. ISSA 2012 Conf. (2012) 1–8. https://doi.org/10.1109/ISSA.2012.6320437.

[58] B. Hanus, Y. "Andy" Wu, Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective, Inf. Syst. Manag. 33 (2016) 2–16. https://doi.org/10.1080/10580530.2015.1117842.

[59] T. Sommestad, H. Karlzén, J. Hallberg, The Theory of Planned Behavior and Information Security Policy Compliance, J. Comput. Inf. Syst. 59 (2019) 344–353. https://doi.org/10.1080/08874417.2017.1368421.

[60] J. Ortiz, S.H. Chang, W.H. Chih, C.H. Wang, The contradiction between self-protection and self-presentation on knowledge sharing behavior, Comput. Human Behav. 76 (2017) 406–416. https://doi.org/10.1016/j.chb.2017.07.031.

[61] R.E. Crossler, Protection motivation theory: Understanding determinants to backing up personal data, Proc. Annu. Hawaii Int. Conf. Syst. Sci. (2010) 1–10. https://doi.org/10.1109/HICSS.2010.311.

[62] H. Damghanian, A. Zarei, M.A. Siahsarani Kojuri, Impact of Perceived Security on Trust, Perceived Risk, and Acceptance of Online Banking in Iran, J. Internet Commer. 15 (2016) 214–238. https://doi.org/10.1080/15332861.2016.1191052.

[63] M.S. Doargajudhur, P. Dell, The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation, J. Comput. Inf. Syst. 00 (2018) 1–12. https://doi.org/10.1080/08874417.2018.1543001.

[64] Z. Tu, Y. Yuan, Understanding user's behaviors in coping with security threat of mobile devices loss and theft, Proc. Annu. Hawaii Int. Conf. Syst. Sci. (2012) 1393–1402. https://doi.org/10.1109/HICSS.2012.620.

[65] H. Chen, W. Li, Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective, Behav. Inf. Technol. 38 (2019) 454–468. https://doi.org/10.1080/0144929X.2018.1539520.

[66] Y.M. Iriqat, A.R. Ahlan, N.N.A. Molok, Information security policy perceived compliance among staff in palestine universities: An empirical pilot study, 2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc. (2019) 580–585. https://doi.org/10.1109/JEEIT.2019.8717438.

[67] and D.C. Malcolm Pattinson, Marcus Butavicius, Kathryn Parsons, Agata McCormac, Factors that Influence Information Security Behavior: An

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Australian Web-Based Study, Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 9190 (2015) 231–241. https://doi.org/10.1007/978-3-319-20376-8.

[68] X. Chen, L. Chen, D. Wu, Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective, J. Comput. Inf. Syst. 58 (2018) 312–324. https://doi.org/10.1080/08874417.2016.1258679.

[69] B. Hanus, Y. "Andy" Wu, Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective, Inf. Syst. Manag. 33 (2016) 2–16. https://doi.org/10.1080/10580530.2015.1117842.

[70] J. Paliszkiewicz, Information Security Policy Compliance: Leadership and Trust, J. Comput. Inf. Syst. 59 (2019) 211–217. https://doi.org/10.1080/08874417.2019.1571459.

[71] T. Sommestad, H. Karlzén, J. Hallberg, The Theory of Planned Behavior and Information Security Policy Compliance, J. Comput. Inf. Syst. (2017) 1–10. https://doi.org/10.1080/08874417.2017.1368421.

[72] D. Box, D. Pottas, A Model for Information Security Compliant Behaviour in the Healthcare Context, Procedia Technol. 16 (2014) 1462–1470. https://doi.org/10.1016/j.protcy.2014.10.166.

[73] D. Dang-Pham, S. Pittayachawan, Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach, Comput. Secur. 48 (2015) 281–297. https://doi.org/10.1016/j.cose.2014.11.002.

[74] J.M. Blythe, L. Coventry, Costly but effective: Comparing the factors that influence employee anti-malware behaviours, Comput. Human Behav. 87 (2018) 87–97. https://doi.org/10.1016/j.chb.2018.05.023.

[75] K.A. Ismail, M.M. Singh, N. Mustaffa, P. Keikhosrokiani, Z. Zulkefli, Security Strategies for Hindering Watering Hole Cyber Crime Attack, Procedia Comput. Sci. 124 (2017) 656–663. https://doi.org/10.1016/j.procs.2017.12.202.

[76] L. Li, K. Qian, Using Real-Time Fear Appeals to Improve Social Media Security, Proc. - Int. Comput. Softw. Appl. Conf. 2 (2016) 610–611. https://doi.org/10.1109/COMPSAC.2016.217.

[77] P.A. Wang, Information security knowledge and behavior: An adapted model of technology acceptance, ICETC 2010 - 2010 2nd Int. Conf. Educ. Technol. Comput. 2 (2010) V2-364-V2-367. https://doi.org/10.1109/ICETC.2010.5529366.

[78] R.E. Crossler, Protection motivation theory: Understanding determinants to backing up personal data, Proc. Annu. Hawaii Int. Conf. Syst. Sci. (2010) 1–10. https://doi.org/10.1109/HICSS.2010.311.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Dimensions that Contribute to Protection Behaviors

No	Dimensions	Theories and Approaches	Definitions	Relevant Studies	Frequency (studies)
1	Self-Efficacy	PMT	It is the expectation of individuals' ability to perform the behaviors in terms of achieving desired protection outcomes.	[21], [22], [26]	34
2	Response Efficacy	PMT	It is the beliefs of individuals whether a step of protection would avoid the threat.	[29], [25], [35]	27
3	Perceived Severity	PMT	It is the perception of individuals to the results of protection from threats.	[12],[66], [43]	22
4	Perceived Vulnerability	PMT	An individual's belief in the possibility of a threat or breach due to lack of protection	[50], [34], [35]	20
5	Response Cost	PMT	It is a behavioral procedure that involves the loss of protection by individuals that result in unacceptable behavior.	[50], [25], [39]	18
6	Attitude towards	TPB	It is the willingness of individuals to respond positively or negatively to the direction of protection.	[44], [47], [49]	18
7	Subjective Norm	TPB	It is a social condition for individuals to perform or not for protection behaviors.	[21], [27], [46]	16
8	Information security awareness	OC	It is raising awareness about the potential dangers of rapidly evolving forms of information and the rapidly evolving threats to that information that target human behavior.	[8], [59], [60]	8
9	Security Self-Efficacy	PMT	It is the ability of individuals to minimize information system security threats and protect information system assets from security attacks.	[49], [41], [25]	5
10	Perceived behavioral control	TPB	It is the perceptions and intentions of individuals about their ability to protect their data.	[46], [59], [30]	5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Appendix A: List of Reviewed Articles

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
1	Malcolm Pattinson, Marcus Butavicius, Kathryn Parsons, Agata McCormac, and Dragana Calic [67]	2015	**Risks of users security behavior** (employees age, education level, ability to control impulsivity, familiarity with computers, and personality)	Individual	Quantitative	Australia	Employees	Regression Model
2	Ioanna Topa and Maria Karyda [30]	2015	**Protection behavior/ organizational culture** (attitude, subjective norms and perceived behavioral control, which consists of self efficacy , controllability, perceived vulnerability, response efficacy, self-efficacy, attitude towards and security awareness).	Individual	Quantitative	Greece	Employees (security Managers)	Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT)
3	Akhyari Nasir, Ruzaini Abdullah Arshah & Mohd Rashid Ab Hamid [26]	2019	**Protection behavior/ organizational culture** (Procedural Countermeasure, Risk Management, Security Education, Training and Awareness, Top Management Commitment, Security Monitoring, Information Security Knowledge, and Information Security Knowledge Sharing)	Organizational	Qualitative	Malaysia	Employees in government	Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) and Information Security Culture (ISC) model.
4	Vincent Cho & W.H. Ip [42]	2017	**Protection behavior** (Privacy Protection, Perceived Severity, Self-Efficacy, Perceived Cost, Perceived Effectiveness of security policy, perceived usefulness, perceived ease of use, social influence, organizational commitment and job security).	Organizational	Quantitative	Hong Kong	Employees in organizations	Technology Threat Avoidance Theory (TTAT), Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB)
5	Chet L. Claar & Jeffrey Johnson [41]	2012	**Risks of users security behavior** (Perceived Vulnerability , Perceived Severity, Perceived Benefits, Perceived Barriers , Self-Efficacy, Cues to Action, Gender, Age, Education, Prior Experience and Computer Security Usage)	Individual	Mixed	United State	Internet enabled computer owners	Health Belief Model (HBM) and Protection Motivation Theory (PMT)
6	Xiaofeng Chen, Liqiang Chen & Dazhong Wu [68]	2016	**Protection behavior/ organizational culture** (Perceived Penalty, Perceived	Individual	Quantitative	United State	Employees in organizati	Awareness Motivation Capability

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
			Reward, Perceived Self-efficacy, Controllability, Awareness of ISP and Awareness of seriousness of security threat)				ons	framework (AMC), Theory of Planned Behavior (TPB) , Protection Motivation Theory (PMT), Deterrence Theory (DT), and Rational Choice Theory
7	Hossein Damghanian, Azim Zarei & Mohammad Ali Siahsarani Kojuri [62]	2016	**Risks of users behavior** (Perceived security, perceived risk and trust)	Organizational	Quantitative	Iran	Customers of Bank Saderat	Structural Equations Model (SEM) and Perceived Risk Theory (PRT)
8	Bartlomiej Hanus & Yu "Andy" Wu [69]	2016	**Protection behavior** (Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Response Cost, threat Awareness and Countermeasure Awareness)	Organizational	Quantitative	United State	Students in university	Health Belief Model and Protection Motivation Theory (PMT)
9	Joanna Paliszkiewicz [70]	2019	**Trust/ organizational culture** (trust: competence, trust: benevolence, trust: integrity) on leadership regarding the organization's information security policy (ISP).	Organizational	Mixed	United State	Employees in organizations	Protection Motivation Theory (PMT)
10	Melina Seedoyal Doargajudhur & Peter Dell [63]	2018	**Organizational behavior** (technology self-efficacy, perceived workload, perceived job autonomy, perceived job performance and work motivation)	Organizational	Quantitative	Mauritius	Employees in organizations	Job Demands–Resources (JD-R) model
11	Teodor Sommestad, Henrik Karlzén & Jonas Hallberg [71]	2017	**Protection behavior/ organizational culture** (Attitude towards the behavior, perceived norm and perceived behavioral control)	Individual	Quantitative	Sweden	Individual of Employees	Theory of planned behavior (TPB) and Information Security Compliance Behavior
12	Hao Chen & Wenli Li [65]	2018	**Organizational culture** (Perceived demand-ability fit, Perceived need-supply fit, Perceived value fit, Security commitment and Apathy)	Individual	Quantitative	China	Employees in organizations	Person-Organization Fit Theory (POFT)
13	Yang Chen, Chulu Liang & Danqing Cai [46]	2018	**Intention behaviors** (attitude towards, Subjective norm, Perceived behavioral control, Behavioral intention, Getting entertainment, Seeking information, Habitual diversion, Seeking status, Socializing and	Individual	Quantitative	China	Online WeChat users	Theory of Planned Behavior (TPB), the Theory of Use and Gratification

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
			The norm of reciprocity)					(TUG), and the Theory of Prosocial Behavior.
14	Habib Ullah Khan & Khalid A. AlShare [45]	2019	**Protection behavior/ Organizational culture** (perceived privacy, subjective norms, perceived information security policy (ISP) scope, perceived severity of penalty, perceived celerity of penalty, management support, organizational security culture, and perceived organizational IT capability)	Organizational	Quantitative	United State	Employees of the Midwestern University	General Deterrence Theory (GDT), Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA), Protection Motivation Theory (PMT), and Social Cognitive Theory (SCT)
15	Nik Thompson, Tanya Jane McGill b and Xuequn Wang [39]	2017	**Protection behavior** (perceived vulnerability, perceived Severity, self-efficacy, response efficacy, response cost, descriptive norm and psychological ownership and Subjective Norm)	Individual	Quantitative	United State	General population	Protection Motivation Theory (PMT)
16	Debra Box and Dalenca Pottas [72]	2014	**Organizational culture** (misuse of deterrence and compliance promoting)	Organizational	Qualitative	South Afica	Healthcare professionals	General Deterrence Theory (GDT)
17	Hui-Lien Chou and Chien Chou [34]	2016	**Protection behavior** (perceived severity, perceived vulnerability, perceived response-efficacy, self-efficacy, perceived response costs and social norms)	Individual	Quantitative	Taiwan	Teachers in schools	Protection Motivation Theory (PMT)
18	Clay Posey, Tom L. Roberts, Paul Benjamin Lowry and Ross T. Hightower [14]	2014	**Protection behavior/ Organizational culture** (Threat appraisal Maladaptive rewards, Threat severity, Threat vulnerability, Response efficacy, Self-efficacy and Response costs)	Individual	Qualitative	United State	organizational insiders	Protection Motivation Theory (PMT)
19	Duy Dang-Pham andSiddhi Pittayachawan [73]	2014	**Protection behavior** (Vulnerability, Severity, Rewards, self-efficacy, response cost, response efficacy and malware avoidance behaviors (ITA)	Individual	Quantitative	Australia	Students in university	Protection Motivation Theory (PMT)
20	Merrill Warkentin, Allen C. Johnston, Jordan Shropshire and William D. Barnett [38]	2016	**Protection behavior** (perceived threat severity, perceived threat susceptibility, self-efficacy, response efficacy and Perceived extraneous	Individual	Quantitative	United State	Students in university	Protection Motivation Theory (PMT) and Expectation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
			circumstances)					Confirmation Theory (ECT).
21	John M. Blythe and Lynne Coventry [74]	2018	**Protection behavior/ Organizational culture** (Susceptibility, severity, response-efficacy, self-efficacy, response costs and Experience)	Individual	Qualitative	UK	Employees in organizations	Protection Motivation Theory
22	Majed Rajab and Ali Eydgahi [47]	2018	**Protection behavior/ Organizational culture** (Severity, Certainty, Celerity, Threats, Coping, Self-efficacy, Response efficacy, Attitudes, Subjective norms, Perceived behavioral control, Top management, Peers influence, IS climate and Awareness)	Organizational	Qualitative	United State	Employees in organization	Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT), General Deterrence Theory (GDT) and Organizational Theory
23	A.J. Burns, Clay Posey, Tom L. Roberts and Paul Benjamin Lowry [25]	2016	**Protection behavior/ Organizational culture** (threat vulnerability, threat severity, maladaptive rewards, response cost, Security self-efficacy, Security response efficacy, Hope, Optimism, Self-efficacy and Resilience)	Organizational	Quantitative	United State	organizational insiders	Protection Motivation Theory (PMT)
24	Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani and Tutut Herawan [18]	2015	**Protection behavior/ Organizational culture/ Corporate culture** (Information Security Awareness, Information Security Organization Policy, Information Security Experience and Involvement, Attitude towards information security, Subjective Norms, Threat Appraisal, and Information Security Self-efficacy)	Individual	Quantitative	Malaysia	Employees in organizations	Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB)
25	Marijn Martens, Ralf De Wolf and Lieven De Marez [48]	2019	**Protection behavior** (perceived severity, perceived vulnerability, response-efficacy, self-efficacy, Information security awareness, attitude towards behavior and subjective norm)	Individual	Quantitative	Belgium	General population	Protection Motivation Theory (PMT)
26	Ling Li, Wu He, Li Xu, Ivan Ash, Mohd Anwar and Xiaohong Yuan [37]	2019	**Protection behavior** (Perceived vulnerability, Perceived severity, Perceived barrariers, Self-efficacy, Response efficacy, Cybersecurity protection behavior	Individual	Quantitative	United State	Employees in organizations	Protection Motivation Theory (PMT)
27	Anthony Vance, Mikko Siponen and	2012	**Protection behavior** (Vulnerability, Perceived	Individual	Quantitative	Finland	Students in	Protection Motivation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
	Seppo Pahnila [51]		severity, Rewards, Response efficacy, Self-efficacy, Response cost, IS security policies)				university	Theory (PMT) and Habit Theory (HT)
28	Mark Grimes and Jim Marquardson [49]	2019	**Protection behavior** (Perceived vulnerability, Perceived severity, security Self-efficacy, Security Response efficacy, Subjective norms secuirty and Attitude toward security behavior)	Individual	Quantitative	United State	Students in university	Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB)
29	Khairun Ashikin Ismail, Manmeet Mahinderjit Singh, Norlia Mustaffa, Pantea Keikhosrokiani and Zakiah Zulkefli [75]	2017	**Protection behavior** (perceived severity, perceived vulnerability, response-efficacy, self-efficacy and Intention)	Individual	Quantitative	Malaysia	Students in university	Protection Motivation Theory (PMT)
30	Jurjen Jansen and Paul van Schaik [35]	2018	**Protection behavior** (perceived risk, perceived vulnerability, perceived severity, trust, response efficacy, self-efficacy, response costs, internal locus of control, injunctive norms, descriptive norms and Security awareness	Individual	Qualitative	Netherlands	Online banking users	Protection Motivation Theory (PMT)
31	Jaime Ortiz, Shu-Hao Chang, Wen-Hai Chih, and Chia-Hao Wang [60]	2017	**Protection behavior** (information security awareness (ISA) into general information security awareness (GISA), information security policy awareness (ISPA), self-protection and self-presentation perspectives)	Individual	Quantitative	Global	Social Networking Sites (SNSs) Users	Protection Motivation Theory (PMT)
32	Philip Menard, Merrill Warkentin andPaul Benjamin Lowry [28]	2018	**Protection behavior/ Organizational culture** (threat severity, threat susceptibility, response efficacy, self-efficacy, response cost)	Individual	Quantitative	United State & China	General population	Protection Motivation Theory (PMT)
33	Anat Hovav and Frida Ferdani Putri [31]	2016	**Protection behavior/ Organizational culture/ Corporate culture** (Perceived freedom threat, Intention to comply, BYOD IT support, Perceived threat appraisal, Perceived digital mutualism justice, Perceived response cost, Perceived response efficacy and BYOD security awareness)	Individual	Quantitative	Indonesia	Employees in organizations	Protection Motivation Theory(PMT), Reactance Theory (RT) and Organizational Justice Theory (OJT)
34	Noura Alomar, Mansour Alsaleh and Abdulrahman Alarifi [43]	2019	**Protection behavior** (perceived severity, perceived costs, perceived effectiveness, perceived susceptibility, self-efficancy and perceived threat)	Individual	Mixed	Saudi Arabia	Employees in organizations	Technology Threat Avoidance Theory (TTAT) and Theory of Planned Behavior

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
								(TPB)
35	Princely Ifinedo [52]	2012	**Protection behavior/ Organizational culture** (self-efficacy, attitude toward compliance, subjective norms, response efficacy, perceived vulnerability and information systems security policy (ISSP)	Individual	Qualitative	Canada	Employees in organizations	Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT)
36	Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon and Shelia R. Cotton [33]	2016	**Protection behavior/ Organizational culture** (Threat Severity, Threat Susceptibility, Coping self-efficacy, Response efficacy, Subjective norms, Response costs, Safety habit, Personal responsibility and Perceived security)	Individual	Quantitative	United State	Students in university	Protection Motivation Theory (PMT), Unified Theory of Acceptance (UTA) and Use of Technology (UTAUT) Theory and Theory of Planning Behavior (TPB)
37	Silas Formunyuy Verkijika [40]	2018	**Protection behavior** (Perceived vulnerability, Perceived severity, Self-efficacy, Response efficacy and Response cost)	Individual	Quantitative	South Africa	owners of smartphone devices	Protection Motivation Theory (PMT)
38	Anthony Duke Giwah [50]	2018	**Protection behavior** (perceived threat severity, perceived threat susceptibility, and perceived response costs)	Individual	Quantitative	United State	The Fortune 500 individual organization	Protection Motivation Theory (PMT)
39	Aristotle Onumo, Andrea Cullen and Irfan Ullah-Awan [21]	2018	**Protection behavior/ Organizational culture** (attitude, subjective norm, self-efficacy, intention, collaborative, competitive, Creative culture and Controlled culture)	Individual	Quantitative	Nigerian	Employees in Government	Theory of Planned Behavior (TPB), Triandis' Model and Competing Value Framework
40	Arthur Jung-Ting Chang [55]	2010	**Organizational culture** (risk propensity, perceived risk of information system, compatibility, perceived risk of adoption, perceived usefulness, attitude towards and behavioral intention)	Individual	Quantitative	Taiwan	Managers in organizations	Theory of Planned Behavior (TPB) and Technology Acceptance Model
41	Arthur Jung-Ting Chang [23]	2010	**Protection behavior/ Organizational culture** (Subjective Norm, Attitude towards, Perceived Behavioral Control, Compatibility, Perceived Risk, Perceived Usefulness and risky	Individual	Quantitative	Taiwan	Managers in organizations	Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM)

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
			decision-making perspective)					and Protection Motivation Theory (PMT)
42	Ashrafi Noushin, Lee Daniel, Kuilboer Jean-Pierre and Schütz G. Christoph [29]	2019	**Protection behavior/ Organizational culture** (Awareness, Severity, experience, Perceived Barriers, Perceived Benefits, Protective action and Defensive Avoidance)	Individual	Quantitative	United State	Students in university	Protection Motivation Theory (PMT), Health Benefit Model (HBM) and Extended Parallel Processing Model (EPPM)
43	Christian Matt and Philipp Peckelsen [12]	2016	**Privacy Concerns/ Protection behavior** (Perceived severity of privacy threats, Perceived susceptibility of privacy threats, Perceived self-efficacy, Perceived response efficacy, Emotional stability, Agreeableness, Conscientiousness, Extraversion, Openness and Perceived privacy experience)	Individual	Quantitative	Germany	Students in university	Protection Motivation Theory (PMT) and Five-Factor Model (FFM)
44	Dr. Sanjeev Dhawan, Dr. Kulvinder Singh and Ms. Shivi Goel [53]	2014	**Privacy Concerns** (individual's details, privacy concern, attitude, and awareness on their willingness to share personal information in social networking sites)	Individual	Quantitative	Global	Social sites users	Theory of Planned Behavior (TPB)
45	HA Kruger, S Flowerday, L Drevin and T Steyn [56]	2011	**Organizational culture** (information security awareness, security knowledge and behavior)	Individual	Quantitative	South African	Students in university	Security Concepts
46	Jasber Kaur and Norliana Mustafa [13]	2013	**Organizational culture** (knowledge, attitude, behavior, confidentiality, integritym availability and awareness of information security)	Organizational	Quantitative	Malaysia	Employees in a SME	KAB model theory
47	Jing Yang and Yue Zhang [27]	2015	**Protection behavior** (perceived threat severity, perceived threat susceptibility, self-efficacy, response efficacy, response cost, Attitude toward and Subjective Norm)	Organizational	Quantitative	United State	Students in university	Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB)
48	Jörg Uffen and Michael H. Breitner [54]	2015	**Organizational culture** (Conscientiousness, Neuroticism, Openness, Compliance, Attitude towards technical security measures and Intention towards technical security measures	Organizational	Quantitative	German-speaking countries	Managers	Five Factor Model (FFM), Theory of Planned Behavior (TPB) and Technology Acceptance Model (TAM)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
49	Lei Li and Kai Qian [76]	2016	**Protection behavior** (perceived severity, perceived probability, efficiency behavior, self-efficiency and Social Media Users perception of security risks)	Individual	Quantitative	Global	Social media users (College student)	Protection Motivation Theory (PMT)
50	Manal Alohali, Nathan Clarke, Steven Furnell and Saad Albakri [8]	2017	**Protection behavior** (Attitude and Subjective Norm, Past experience, IT Expertise, Risk Communication, Usefulness, Ease of Use and Culture)	Organizational	Quantitative	Global	Undefined	Protection Motivation Theory (PMT), Technology Acceptance Model (TAM) and Automation Approach (AA)
51	Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani and Tutut Herawan [18]	2017	**Organizational culture/protection behavior** (Information Security Awareness, Information Security Organization Policy, Information Security Experience and Involvement, Attitude towards information security, Subjective Norms, Threat Appraisal, and Information Security Self-efficacy)	Organizational	Mixed	South African	Staff in companies	Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB) and Social Bond Theory (SBT)
52	Ping An Wang [77]	2010	**Protection behavior** (actual use, attitude toward using, intention to use, knowledge of information, knowledge of awareness and knowledge of experience)	Individual	Quantitative	United State	Students in university	Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB)
53	Robert E. Crossler [78]	2010	**Protection behavior** (Perceived Security Vulnerabilities, Perceived Security Threats, Security Self-Efficacy, Response Efficacy and Prevention Cost)	Individual	Qualitative	United State	Students in university	Protection Motivation Theory (PMT)
54	Sadaf Hina and Assoc. Prof. Dr. Dhanapal Durai Dominic [22]	2017	**Organizational culture/protection behavior** (Security Education and Training Programs, Provision of Policy, Monitoring, Negative Experience, Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response-Efficacy, Subjective Norms, Attitude and Information Security Policy Compliance)	Individual	Qualitative	Malaysia	Employees in Higher education institutions	Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB) and Cognitive Evaluation Theory (CET)
55	Tapiwa Gundu and Stephen V Flowerday [57]	2012	**Protection behavior** (Subjective Norms, Attitude, Perceived vulnerability, Perceived severity, Response	Organizational	Quantitative	South African	Employees of Engineering SMEs	Behavioral Intentions Models, Theory of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Author	Year	Dimensions/ Issues	Perspective	Method	Location	Sample	Model/ Theory
			efficacy, Response cost, Self-efficacy and Information security awareness)					Reasoned Action (TAM) and Protection Motivation Theory (PMT)
56	Yousef Mohammad Iriqat, Abd Rahman Ahlan and Nurul Nuha Abdul Molok [66]	2019	**Organizational culture/protection behavior** (ISP Awareness, Perceived Sanctions Certainty, Perceived Sanctions Severity, Perceived Rewards, Perceived Self efficacy, Perceived Response efficacy, Perceived Info-Quality, Perceived Info-privacy, Perceived Facilitating Conditions, perceived intention and awareness of Information Security Policies)	Organizational	Quantitative	Palestinian	Academic and administrative staff in University	General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB) and Information Reinforcement
57	Zhiling Tu and Yufei Yuan [64]	2012	**Protection behavior** (Perceived Vulnerability, Perceived Severity, Locus of Control, Self-efficacy, Perceived Cost, Perceived Effectiveness and Social Influences)	Individual	Quantitative	Canada	Online mobile users	Protection Motivation Theory (PMT)