International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.3 (May-2020)
http://dx.doi.org/10.12785/ijcds/090310

The Direct and Indirect Effects of Personality on Data Breach in Education Through the Task-Related Compulsive Technology use: M-Learning Perspective

Basil John Thomas[1] and Jeyhun Hajiyev[2]

[1] Department of Business Administration, Sur University College, Sur, Sultanate of Oman
[2] Department of Information Management, Chang Gung University, Taiwan, R.O.C

Received 7 Jul. 2019, Revised 8 Mar. 2020, Accepted 13 Apr. 2020, Published 1 May 2020

Abstract: Literature is lack of understanding the negative outcome of compulsive technology use (CTU) and security/data breach in virtual learning environment. This research employs task-related CTU with consideration of university students' use of mobile devices in m-learning environment and investigates the impact of personality diversity on task-related CTU. It is also tested whether task-related CTU increases the likelihood of data breach. Medium of access (mobile devices) is tested as moderating variable. Agreeableness, conscientiousness, openness, extraversion, and external locus of control significantly influences task-related CTU, while agreeableness and conscientiousness also impact the likelihood of data breach. Task-related CTU significantly leads to likelihood of data breach and medium of access moderates this relationship. This research is one of the few studies addressing data breach in education and role of excessive technology use on risky cyber-security behavior of students, which can guide m-learning system designers to take safety measures against data and privacy theft.

Keywords: M-Learning, Task-Related Compulsive Technology Use, Data Breach, Education

1. Introduction

It is reported that in 2018, average total cost of data breach grew from US$ 3.62 to $3.86 million (6.4%) (Ponemon Institute LLC, 2018). There are several factors that mainly increase the cost of data breaches, such as extensive use of Internet of things (IoT) devices, mobile devices, and compliance failures. Recently, Internet use in school campuses as well as in society has drastically increased (Marahatta et al., 2015). The use of Internet is beneficial for learning and research purposes, as it becomes an integral part of academic life. Mobile learning (m-learning) is denoted as a learning technology that is accessed through mobile device, which provides teachers and students with the aptitude to get connected to local wireless network (Mobile Learning, 2016). Yet, it is reported that mobile education apps are one of the 10 most malicious apps with 3.9% malware. As mentioned above, extensive use of mobile devices is one of the factors that affect the data breach. However, majority of technologies are used outside the harsh organizational boundaries, while they are not compulsory (Clements & Boyle, 2018). The identification of the factors eliciting technology usage in personal settings has yet to be fully comprehended (Ang, 2017). As such, human factors in respect with information security have gained immense attention, while the security technologies usage fails to prevent cyber-attacks in organizations (Anwar et al., 2016). It happens when employees fail to conform to cyber security protocols and further place their organizations at risk. According to Clements (2015), human behavior is often automatic and non-rational, indicating that technology engagement might be an outcome of technology features that lead to certain behavior independent from self-awareness. Since studies identifying the source and consequence of unplanned and uncontrollable automatic behavior referred as compulsive technology use (CTU) (Clements & Boyle, 2018), the major aim of this research is to address the gap in understanding how CTU leads to the likelihood of data breach (DB) in m-learning setting. Unlike the majority of former studies, this research employs the idea of "task-related CTU" following the suggestions of De Guinea and Markus (2009) that goal-oriented intentional habits can generate far more automatic and unintentional behavior. Although individuals might consciously plan to perform a task, they might not need to formulate a conscious behavioral intention to use information technology (IT), because the goal of IT usage and plan towards to it is automatically activated by the task performing goal. Initiation to habitual behavior might be intentional, while the further implementation of this behavior might be unintentional (Verplanken & Aarts, 1999). In the context of education, we can assume that instigation of effective learning by students might be intentional, while further actions (e.g., seeking for Internet resources related to study, educational forums, looking at social media or YouTube for learning materials or videos) might be unintentional, which could ultimately lead to the

E-mail address: basil@suc.edu.om, ceyhunhajiyev@gmail.com

compulsive use of Internet on the purpose of achieving learning task. Moreover, in the recent study, the term "task-related CTU" is utilized. Hence, in m-learning context, task-oriented intention to use mobile devices might lead to compulsive usage behavior.

Human error is one of the essential causes of the data breach following malicious and/or criminal attach (Ponemon Institute LLC, 2018). In organizational context, employees underestimate the probability of being victim of cybersecurity breach that is influenced by organizational, behavioral, and environmental factors (Herath & Rao, 2009). Regarding the personality factors, McBride et al. (2012) found that those who are more extraverted are prone to violate cybersecurity policy in comparison with individual with higher neuroticism and conscientiousness. Hadlington (2017) revealed that Internet addiction is significantly related to cybersecurity behaviors. To tackle the human factor in data breach and excessive use of Internet, this study relies on Big-five personality traits model. The five traits of personality, namely agreeableness, conscientiousness, extraversion, openness, and neuroticism are employed.

2. RESEARCH PROBLEM

The current study explores the potential for individual differences in risky Internet usage behavior to act as predictors for CTU and likelihood of DB in m-learning setting. Because each individual with different personality might be affected by the elements of technology design compare to others, suggesting the further investigation of individual characteristics that could potentially inhibit or contribute to the CTU (Clements & Boyle, 2018).

With the access to m-learning on portable devices at any time and any place, students can remain focused that can potentially result in less academic failures (Laskaris, 2015). The number of students using mobile applications and devices is greater than non-students, which is accounted for 79%. However, more than 90% of incidents related to security breach during the technology usage in schools are because of human error (Wagner, 2016). Mobile devices and software currently made identity theft and security breach prevalent, particularly in big universities and colleges (Battle, 2018). Hence, the convenience of the visibility to see other students' personal information has become a key concern owing to the higher accessibility of mobile devices to Internet and applications. Therefore, it can be assumed that the medium of access used in a learning process may also have an impact in likelihood of DB. Besides the technology features, individual's internal force, as well as personal efforts, may also affect the behavioral consequences (Lefcourt, 1991), or the behavior may be shaped out of the individual's control (Lee et al., 2014). These two tendencies are explained by internal locus of control (ILOC) and external locus of control (ELOC), respectively. Individuals with ELOC are more likely to show more Internet addiction and compulsive behavior compare to those with ILOC, which can also be reflected in smartphone use. Hence, it is also worthy to investigate whether ILOC or ELOC would lead to task-related CTU in educational setting. Drawing from the discussion, this research addresses the following questions:

RQ1: Is there a relationship between personality diversity and task-related CTU in m-learning environment?

RQ2: Is there a relationship between locus of control and task-related CTU in m-learning environment?

RQ3: Is there a relationship between task-related CTU and the likelihood of DB in m-learning environment?

RQ4: Is the medium of access used for m-learning moderates the relationship between task-related CTU and likelihood of DB?

3. LITERATURE REVIEW

A. *Task-related compulsive technology use*

The social network feature and content of Internet as well as it social platforms do not always lead to positive outcomes such as learning, but also problematic usage behavior (Hsiao et al., 2017). This problematic Internet use is discussed in literature as compulsive use and/or addiction (Klobas et al., 2018). The compulsive use is closely aligned with Internet addiction, whereas it can exist on its own too if Internet users do not have a negative experience or threat in their life (Griffiths, 2013).

Compulsive technology is viewed as unplanned interaction with technology that is unintended, uncontrollable, efficient, and requires fewer efforts. CTU can be classified on the scale of behavioral addictions related to engagement with specific technology for comfort or encouragement, which triggers discomfort when discontinued (Porter & Kakabadse, 2006). In their study, Clements & Boyle (2018) explored non-work related CTU in educational context. However, De Guinea and Markus (2009) suggested that goal-oriented intentional behavior could result in more automatic and unplanned behavior. Even though individuals might plan to perform a task on purpose, they might not need to form a conscious behavioral intention to use IT, because of the automatic activation of goal of IT usage and plan towards to it by the task performing aim. It can be assumed that task-related learning on academic purpose can lead to an excessive CTU in m-learning environment. In this regard, unlike the majority of former studies, this research employs task-related CTU and tests whether personality diversity affects it and whether it increases the likelihood of DB in education.

Former studies mainly explored the negative outcomes of CTU as being emotional and physical ill-being (Panda & Jain, 2018), technostress (Hsiao et al., 2017), problematic learning outcome (Aladwani &

Almarzouq, 2016), compulsive working (Quinones et al., 2016), and social connectedness (McIntyre et al., 2015). The literature is lack of understanding the negative outcome of task-related CTU and security/data breach, particularly in virtual learning environment (VLE), which denotes the system delivering the learning materials to students with the means of Internet (Oxford University Press, 2015). In this study, VLE is referred as m-learning.

Several studies explored the impact of personality diversity on the individual's obedience to cybersecurity process. It was found that extraverted individuals are more tended to violate cybersecurity rules in comparison with their conscientious and neurotic counterparts (McBride et al., 2012). Another study linked personality traits with susceptibility to cyber-attacks (Uebelacker & Quiel, 2014). People with higher impulsiveness would be highly affected by technology compare to people with more conscientious personality (Clements & Boyle, 2018). Although the characteristics that affect the CTU are well addressed, it is still worthy to investigate whether personality characteristics would change the task-related CTU in m-learning environment.

4. Hypotheses Development

A. Personality traits and task-related compulsive technology use

Studies related to compulsive Internet usage identified that the personality has an immense role in the compulsive social network service (SNS) usage (Klobas et al., 2018; De Cock et al., 2014). Majority of the studies employed the Five-Factor Model, so-called Big Five personality traits framework suggested by (McCrae & John, 1992) that evaluates the personality with five dimensions: (1) agreeableness; (2) conscientiousness; (3) extraversion; (4) openness; and (5) neuroticism. Former studies found that neuroticism is positively associated with the use of personalization and photography mobile apps, whereas extraversion has a negative impact on mobile games usage (Xu et al., 2016), conscientiousness is positively connected with SNS usage and cloud services (Kim & Jeong, 2015), and extraversion is likely to lead to online transaction and financial services (Tan & Yang, 2014). Hence, the Big Five personality traits can be used as key determinants of compulsive usage of mobile social apps.

Academic sites including online courses are mostly well-organized (e.g., exams, material presentation) and involve a degree of commitment that could be connected with various personalities. For instance, extraversion was significantly associated with using the Internet for research-specific purpose (Amiel & Sargent, 2004), whereas conscientiousness was positively associated with percent of time for Internet use on academic purpose (Landers & Lounsbury, 2006). Conversely, neuroticism was found to be negatively related with the use of Internet for educational and learning purpose.

Costa & McCrae (1992) described agreeableness as being tolerant, thoughtful, and polite. It was found to be highly related to SNS behaviors, such as messaging and commenting (Wang et al., 2012). Conscientiousness is defined as "*a person's self-discipline and focus on achievement.*" (Klobas et al., 2018, p. 131). This personality is characterized as being responsible and ordered (Baumeister, 2002). It is added that individuals with this personality trait are likely to spend less time on mobile devices, while they are more productive at work or school. Courneya and Hellsten (1998) emphasized that while Facebook and video game addiction is negatively influenced by conscientiousness, studying and exercise addiction is positively influenced by conscientiousness. Extraversion characterizes enthusiasm, social interaction, energetic behavior (Klobas et al., 2018; Costa & McCrae, 1992), while introversion reflects Internet addiction in university students (Servidio, 2014). However, the relationship between extroversion and compulsive use is bidirectional. Such that, Gosling et al. (2011) found that extroverted people have a higher online social presence. McIntyre et al. (2015) found that introversion is negatively related to compulsive Internet use. Openness is characterized as being independent, adventurous, and curious about and open to new ideas (Costa & McCrae, 1992). It has been found to be positively related to SNS usage and compulsive SNS usage on mobile devices (Correa et al., 2010), while Hsiao et al. (2017) found no relationship between openness and compulsive use. Neuroticism is defined as negative emotion and higher anxiety (Roberts et al., 2015). It has been identified that individuals with a higher neuroticism are tended to use SNS for social purposes more persistently (Hughes et al., 2012). Drawing from the discussion above, the following hypotheses are proposed:

H1a: Agreeableness positively affects task-related CTU

H1b: Conscientiousness positively affects task-related CTU

H1c: Extraversion negatively affects task-related CTU

H1d: Openness positively affects task-related CTU

H1e: Neuroticism positively affects task-related CTU

B. Task-related compulsive technology use and likelihood of data breach

To date there have not been strong initiatives to investigate the association between Internet addiction and likelihood to engage with risky cybersecurity behavior (Hadlington, 2017). Majority of the studies have concentrated on excessive Internet usage with a negative outcome of being productivity loss at the workplace (Young & Case, 2004). According to Chen et al. (2008), inappropriate use of Internet in the working environment could lead to growing cybercrime, intellectual asset theft, and online piracy. In addition, unconscious or careless download of malicious code or visit the compromised websites could create serious issues for organizations (Panko, 2010). Therefore, the hypothesis is proposed as following:

H2: Task-related CTU positively affects likelihood of DB

C. Personality traits and likelihood of data breach

Several studies investigated the impact of personality differences on obedience to cybersecurity rules (Hadlington, 2017; McBride et al., 2012; Shropshire et al., 2006). One of them found that individuals with higher agreeableness and conscientiousness are tended to comply with security protocols (Shropshire et al., 2006). On the contrary, more extraverted individuals are less likely to comply with cybersecurity procedure compare to those with higher neuroticism and conscientiousness (McBride et al., 2012). Another research linked the Big Five traits with susceptibility to manipulation and persuasion by cybersecurity attackers (Uebelacker & Quiel, 2014). Hence, extraverted and conscientious individuals with a higher level of openness and agreeableness are more vulnerable to cyber-attacks. However, McCormac et al. (2016) proposed that openness, agreeableness, and conscientiousness create more awareness on information security and cybersecurity rules in individuals. The inconsistency in findings of former studies highlights the further perspective to investigate the connection between personality traits and likelihood of DB in different domains. Drawing from literature, the following hypotheses are proposed:

H3a: Agreeableness positively affects likelihood of DB

H3b: Conscientiousness positively affects likelihood of DB

H3c: Extraversion positively affects likelihood of DB

H3d: Openness positively affects likelihood of DB

H3e: Neuroticism positively affects likelihood of DB

D. Locus of control and task-related compulsive technology use

Locus of control is referred to a perception on the ability to influence the outcome of events with own actions (Rotter, 1966). There are two types of locus of control (LOC): (1) internal locus of control (ILOC); (2) external locus of control (ELOC). In terms of ILOC, the cause of events or personal behavior heavily rely on individual's internal force and decisions as well as personal efforts that can potentially affect what will happen next (Lefcourt, 1991). Conversely, individuals with higher ELOC perceive that the events are out of their control (Lee et al., 2014). Smartphone users with higher ELOC are more tended to compulsively use smartphones (Lee et al., 2014). Therefore, it is expected that in m-learning environment through mobile devices, students with ELOC are more tended to experience task-related CTU compare to their counterparts with ILOC. Therefore, it is hypothesized that:

H4a: Students with ELOC are likely to show higher task-related CTU

H4b: Students with ILOC are likely to show lower task-related CTU

E. Moderating role of the medium of access

Lee et al. (2014) emphasized that the growing adoption of mobile devices to keep up with the trends with growing acceptance of smartphone as a major IT device leads to overdependence on mobile devices, which leads to compulsive use and technostress. De Guinea and Markus (2009) added that IT in the form of device or feature might serve as a significant factor for task-related use of IT. For instance, a plain sight of computers on a desk might prompt working on a paper, whereas a sight on a mobile device might trigger making a call to a friend. Moreover, with good design, we can be guided interactively by signs of technology without distracting our attention from what we are doing. Therefore, it can be assumed that the medium of access used for m-learning process at the universities could potentially increase the CTU and impact each personality type differently. Moreover, it is hypothesized that:

H5a: The medium of access used for m-learning strongly moderates the relationship between personality traits and task-related CTU

H5b: The medium of access used for m-learning strongly moderates the relationship between task-related CTU and likelihood of DB

In the current study, the conceptual model (see Figure 1) is based on related theories reflected in former literature and explains the hypothesized relationships as follows:

Figure 1. The proposed conceptual model

5. METHODOLOGY

A. Measurement development

This research employed an online survey method for collecting data as it reduces the cost and increases efficiency of the geographical dissemination of the questionnaire (Chang et al., 2019; Kurfali et al., 2017).

The constructs of the current research were taken from former studies and were measured with multiple items. The instruments were designed to weigh the Big Five traits, LOC, task-related CTU, and likelihood of DB. In addition, the questionnaire is comprised of demographic variables, namely gender, age, education grade, mobile device type, and frequency of mobile devices usage in respect of for educational and non-educational purposes.

The Mini-IPIP scales were used (Donnellan et al., 2006). Each of them consists of four items and are measured on a 5-point Likert scale ranging from 1 being "strongly disagree" to 5 being "strongly agree." The Mini-IPIP is confirmed as the brief measurement of the Big Five traits with 20 items, compare to the IPIP-FFM scale with 50 items. LOC was assessed with 6 items set by Lee et al. (2014) and Sapp and Harrod (1993). The items of the CIUS are taken from Meerkerk et al. (2009). Task-related CTU was measured with the compulsive Internet use scale (CIUS), which consists of 14 items on a 5-point Likert scale (1 being "strongly disagree" to 5 being "strongly agree"). The CIUS is believed to have a high internal consistency (Meerkerk et al., 2010). Being related to the SeBIS proposed by (Egelman & Peer, 2015) and risky cybersecurity behaviors scale (RScB) by Hadlington (2017), 8-item questionnaire based on 5-point Likert scale was developed to measure the likelihood of DB in m-learning setting at the universities. The items consisted of questions, such as "Using the similar password for multiple websites", "Using an online storage system to keep or exchange educational and personal data", "Downloading data and study materials from websites without checking their authenticity." Finally, the medium of access as a moderating variable was measured with multiple items related to functions, usability, applications, and design (Kim et al., 2016).

B. Participants

The current empirical research is conducted in Oman for several reasons. Oman has over 70% smartphone penetration rate along with Kuwait and Israel in the Middle East region (GSMA, 2016). One of the studies reveal that in the Gulf region, 58% of instructors and 99% of students have smart phones (Al Emran et al., 2016), which can ultimately increase the effectiveness of m-learning adoption, while it may also raise the concern about the data security of students. Because, Al Khawaldi (2000) emphasized that the educational technology in Oman higher education is still in infancy of utilization of advanced technology, meaning that the drawbacks in technology infrastructure may lead to data leakage in universities.

C. Pre-test

As suggested by Van De Vijver and Leung (1997), translation and back-translation technique were used to ensure the practicality of the survey questionnaire. Initially, the questionnaire was translated into Arabic with the help of bilingual assistant because of the target respondents being mostly local students at the Oman universities. Then, it was translated back to English in order to confirm that the meanings are not lost during the translation process.

The survey was pre-tested with 11 respondents (7 undergraduate students, 4 IT department staff experienced with the campus data management) with a convenience sampling technique. 5 items signifying task-related CTU and LOC were rephrased following the respondent feedbacks. The ultimate survey has 59 items along with the demographic variables. The reliability of the study constructs was tested with Cronbach's alpha (α) and α scores exceeded 0.7 (Nunnally, 1978), showing that the final questionnaire assures reliability. (We re-ran reliability test with Cronbach's α following the data collection process, while the results are provided in Measurement model section)

AMOS v.24 software was employed to analyze data with structural equation modeling (SEM) technique. Measurement model was primarily assessed, followed by the structural model test (Hair et al., 1998). The analysis section contained construct validity including convergent and discriminant validity, and model testing including model fitting and hypothesis testing.

6. ANALYSIS AND RESULTS

A. Demographic profile

328 completed and valid questionnaires were returned (13th April to 29th June) from the total of 413 questionnaires. The 85 responses (20.5%) were discarded due to incompleteness. Demographic distribution of the respondents (see Table 1) shows that male students constitute 58.2% of overall respondents, while their female counterparts are 41.8%. Regarding the age distribution, majority of the students are between 20-22 years old (36.0%) with undergraduate grade (59.8%). In addition, the students mostly use their smartphones to access m-learning materials, and class-related content (55.8%). Finally, it is found that about 29% of them use mobile devices for 3-4 hours, followed by over 4 hours (27.1%) for educational purpose, while less than 2 hours are spent for non-educational purposes (35.4%) on mobile devices. Hence, it can be assumed that compulsive use of mobile devices is mostly related to accomplishing academic tasks in m-learning setting.

TABLE I. STUDY RESPONDENTS' PROFILE

Demographic variable (N=328)	Items	Frequency	%
Gender	Male	191	58.2
	Female	137	41.8
Age	<20	65	19.8
	20-22	118	36.0
	22-24	96	29.3
	>24	49	14.9
Education grade	Undergraduate	196	59.8
	Postgraduate	132	40.2

Mobile device used for m-learning	Smartphone	183	55.8
	Tablet	145	44.2
Mobile device usage frequency-education purpose	<1 hour	21	6.4
	1-2 hours	78	13.7
	2-3 hours	95	23.8
	3-4 hours	89	29.0
	>4 hour	103	27.1
Mobile device usage frequency-non-educational purpose	<1 hour	116	31.4
	1-2 hours	48	35.4
	2-3 hours	27	14.6
	3-4 hours	34	8.2
	>4 hour		10.4

B. Measurement model

In a measurement model, the study constructs were initially assessed for reliability, as well as convergent and discriminant validity. Then, internal consistency (construct reliability) of the study variables was assessed with Cronbach's α, as suggested by Nunnally (1978). Three variables, namely OPEN (0.81), LOC (0.78), and AGR (0.73) have high reliability, while six variables have moderate reliability. The results of the Cronbach's α values are presented in Table 2. The study variables are internally consistent when Cronbach's α values are high. Following that, item reliability was assessed with the use of standardized factor loadings, as recommended by Shih (2004). It is revealed that item loadings are over 0.66, by considering that 0.5 is a threshold value.

Confirmatory factor analysis (CFA) was run for assessing scale validity (Anderson & Gerbing, 1988). The indicator loadings must be over 0.7, while composite reliability (CR) value must exceed 0.7, and finally average variance extracted (AVE) value of each construct must be higher than 0.5, recommended by (Hair et al., 2006). Based on Table 2, CR values range between 0.84 and 0.93, task-related CTU having the highest CR value. In addition, NEU (0.66), AGR (0.63), and OPEN (0.61) have the highest AVE values.

Discriminant validity is explained by the empirical difference between two different constructs. Henseler et al. (2015) proposed and Heterotrait-monotrait (HTMT) ratio of correlation. $HTMT_{.85}$, $HTMT_{.90}$, and $HTMT_{inference}$ yield higher sensitivity levels at the rate of 90% or above. Lack of discriminant validity is observed when HTMT values reach to 1. Even though $HTMT_{.85}$ is considered as threshold, $HTMT_{.90}$ is also accepted. Some earlier studies recommended 0.85 as the threshold rate (Kline, 2011), while others recommended 0.90 (Teo et al., 2008).

In the current research, $HTMT_{.90}$ criterion indicates that discriminant validity is established among all the variables (see Table 3). Only the correlation between EXT and AM slightly exceeds 0.85 level. However, discriminant validity is established based on $HTMT_{.90}$ and $HTMT_{inference}$ criteria.

According to Hair et al. (2006), there are several model-fit measures used to estimate the measurement model, which are Chi-square/degree of freedom (χ^2/df), Tucker-Lewis index (TLI), root mean square error for approximation (RMSEA), comparative fix index (CFI), and standard root mean residual (SRMR). This study also used model-fit indices in measurement model testing. Table 4 shows the findings, showing that measurement model has a satisfactory fit.

TABLE II. MEASUREMENT MODEL

Variable/item	Mean	SD	Factor loading	Cronbach α	CR	AVE
Task-related				0.68	0.93	0.60
CTU	2.51	1.08	0.73			
CTU1	2.32	1.14	0.76			
CTU2	2.09	1.31	0.74			
CTU3	3.12	0.99	0.73			
CTU4	2.24	0.97	0.72			
CTU5	2.56	1.53	0.80			
CTU6	2.43	1.64	0.77			
CTU7	2.11	1.12	0.76			
CTU8	2.05	1.04	0.81			
CTU9	2.01	0.93	0.72			
CTU10	2.22	1.42	0.71			
CTU11	3.06	1.54	0.78			
CTU12	2.49	1.87	0.74			
CTU13	2.38	1.45	0.71			
CTU14						
EXT				0.65	0.85	0.59
EXT1	2.59	1.64	0.79			
EXT2	2.81	1.28	0.82			
EXT3	3.13	0.89	0.81			
EXT4	2.29	1.11	0.75			
AGR				0.73	0.89	0.63
AGR1	3.20	0.82	0.81			
AGR2	0.07	1.05	0.86			
AGR3	3.45	1.25	0.82			
AGR4	2.28	1.08	0.79			
CON				0.69	0.84	0.57
CON1	3.13	1.06	0.81			
CON2	3.24	0.97	0.73			
CON3	2.19	0.73	0.75			
CON4	2.74	1.43	0.71			
NEU				0.67	0.89	0.66
NEU1	2.97	0.84	0.80			
NEU2	3.10	0.96	0.84			
NEU3	2.46	1.32	0.79			
NEU4	2.86	1.75	0.83			
OPEN				0.81	0.86	0.61
OPEN1	2.84	1.05	0.77			
OPEN2	2.79	1.04	0.81			
OPEN3	2.34	1.49	0.79			
OPEN4	3.05	0.93	0.74			
LOC				0.78	0.89	0.57
LOC1	2.34	0.98	0.72			
LOC2	2.46	1.73	0.73			
LOC3	2.67	1.14	0.75			
LOC4	2.13	1.02	0.82			
LOC5	2.87	0.83	0.79			

LOC6	2.54	1.43	0.71			
DB				0.70	0.89	0.51
DB1	3.29	0.97	0.73			
DB2	2.23	1.47	0.67			
DB3	2.29	0.83	0.69			
DB4	2.14	1.83	0.72			
DB5	2.06	1.14	0.69			
DB6	2.21	0.97	0.78			
DB7	2.84	0.99	0.74			
DB8	3.03	0.84	0.66			
MA				0.69	0.87	0.53
MA1	2.71	1.38	0.71			
MA2	3.06	0.85	0.79			
MA3	3.25	1.62	0.69			
MA4	2.09	0.93	0.74			
MA5	2.45	1.32	0.73			
MA6	2.33	1.76	0.71			

(EXT=Extraversion, AGR=Agreeableness, CON=Conscientiousness, NEU=Neuroticism, OPEN=Openness, LOC=Locus of control, DB=Likelihood of data breach, MA=Medium of access)

TABLE III. DISCRIMINANT VALIDITY RESULTS

	1	2	3	4	5	6	7	8	9
Task-related CTU	-								
EXT	0.535	-							
AGR	0.624	0.538	-						
CON	0.722	0.741	0.673	-					
NEU	0.630	0.659	0.741	0.741	-				
OPEN	0.306	0.427	0.843	0.566	0.643	-			
LOC	0.419	0.566	0.771	0.438	0.456	0.357	-		
DB	0.801	0.768	0.619	0.441	0.451	0.672	0.822	-	
MA	0.793	**0.853**	0.485	0.549	0.567	0.487	0.786	0.765	-

Note: The value market in bold refers to problematic discriminant validity in terms of $HTMT_{.85}$ level, while $HTMT_{.90}$ and $HTMT_{inference}$ have no problematic discriminant validity

TABLE IV. MODEL-FIT INDICES OF MEASUREMENT MODEL

Model-fit index	Value	Recommended value
$\chi2/df$	1.864	<3.00
TLI	0.918	≥0.90
RMSEA	0.067	<0.08
CFI	0.937	≥0.90
SRMR	0.041	<0.05

Source: Kline (2005); McDonald and Ho (2002)

C. *Testing structural model*

The hypotheses were tested with the use of AMOS v.24 software. Initially the relationships of personality traits with task-related CTU were tested. It was found that AGR ($\beta = 0.414$, $p < 0.001$), CON ($\beta = 0.337$, $p < 0.001$), and OPEN ($\beta = 0.198$, $p < 0.05$), are positively and significantly related to the task-related CTU, while EXT ($\beta = -0.196$, $p < 0.01$) and NEU ($\beta = -0.131$, $p < 0.05$) have negative and slightly significant impact on the task-related CTU among the university students. Thus, **H1a**, **H1b**, **H1c,** and **H1d** are supported, whereas **H1e** is not supported.

Task-related CTU is positively and significantly related to the likelihood of DB at the universities ($\beta = 0.247$, $p < 0.01$), meaning that **H2** is supported.

Personality traits were also hypothesized to have an impact on likelihood of DB at the universities. Testing the structural model discovered that AGR ($\beta = 0.223$, $p < 0.01$) and CON ($\beta = 0.301$, $p < 0.001$) are positively and significantly associated with DB at the universities, while EXT ($\beta = -0.118$, $p < 0.05$) has a negative and slight influence on the DB. OPEN ($\beta = 0.082$, $p = 0.643$) and NEU ($\beta = -0.018$, $p = 0.215$) do not have an impact on the DB. Hence, **H3a** and **H3b** are supported, while **H3c** and **H3e** are not supported. EXT was expected to have a positive impact on the DB, but testing it in an m-learning setting at the universities revealed that higher extraverted students do not lead to the potential of likelihood of DB. Hence, higher extraversion is equal to higher awareness of security and privacy procedures. Conversely, **H3d** is not supported, indicating that openness cannot lead to the likelihood of DB at the universities ($\beta = 0.082$, $p = 0.319$).

By testing the effect of two types of LOC, this study found that ELOC positively and significantly impacts task-related CTU ($\beta = 0.221$, $p < 0.01$), while ILOC does not affect task-related CTU among the students ($\beta = 0.014$, $p = 0.661$). Hence, **H4a** is supported, while **H4b** is rejected.

D. *Moderation analysis*

Multiplicative approach is one of the techniques to test moderation effect in SEM analysis (Anning-Dorson, 2016; Boso et al., 2013). Moderator is referred as a quantitative or qualitative variable, which impacts the strength of the relationship between independent and dependent variables (Baron & Kenny, 1986). Unlike the majority of former studies, this research used the medium of access as a moderator to test whether it will have an influence on the relationship of personality traits with task-related CTU, and the relationship of task-related CTU with DB. It was found that the medium of access does not moderate the relationships between personality traits and task-related CTU, while it strongly moderates the relationship between task-related CTU and likelihood of DB in education (Task-related CTU * Medium of access) ($\beta = 0.264$, $p < 0.01$). Hence, **H5a** is rejected, while **H5b** is confirmed.

7. DISCUSSION AND IMPLICATIONS

Testing the relationship between personality traits and task-related compulsive technology use showed that agreeableness is positively and significantly related to the students' compulsive use of mobile devices for academic purposes. It seems that the majority of students who are involved in group discussions through mobile devices do not skip messages coming from classmates, or the active use of mobile devices during learning process is highly related to willingness to help classmates by answering their questions posted in group chats. However, Servidio (2014) had found that agreeableness is negatively related to compulsive Internet use. As non-task related compulsive use Internet or SNS (Hsiao et al., 2017), students with a high level of agreeableness enjoy using Internet to chat with classmates. Conscientiousness is also positively and significantly linked to task-related compulsive technology use among the students. It was hypothesized that students with a high conscientiousness might be more likely to use mobile devices for academic more than non-academic purposes. While Hsiao et al. (2017) found a negative relationship between this personality trait and compulsive use of social apps with a consideration of academic self-perception and emphasized that individuals with a high conscientiousness spend less time on mobile devices due to its impact on productivity at the workplace, our finding can be explained by the idea that mobile devices and Internet is the core of m-learning process at the universities. Mark and Ganzach (2014) found that conscientiousness does not have an influence on Internet use for academic activities. Instead, it is positively related to Internet use for leisure and economic purposes. In addition, it was also found that higher agreeableness and conscientiousness create a likelihood of data breach at the universities, which conforms to the findings of Uebelacker and Quiel (2014) that conscientious individuals with higher openness and agreeableness are more vulnerable to cyber-attacks. In this study, openness does not impact the likelihood of DB at the universities. One explanation for our findings could be related to the Internet usage settings and age of users. For instance, Hadlington (2017) investigated human factors in Internet addiction and risky cybersecurity behavior in a business environment. However, our study involved university students, who might not be well-aware of cybersecurity rules and potential outcome of their personality and Internet behavior. It was also found that openness is positively and significantly related to task-related compulsive technology use, which is different from the findings of several studies (Hsiao et al., 2017; Correa et al., 2010). It can be underlined that the student with this personality trait might seek for expanding their interests via online courses, materials, and easy access to the content (Mark & Ganzach, 2014).

Extraversion was found to have a negative and significant influence on the task-related compulsive technology use. The findings are not coherent with that of Klobas et al. (2018), Mark and Ganzach (2014), and Gosling et al. (2011). It seems that students with higher extraversion are not tended to put more efforts on task-related use of Internet for communication or learning activities instead of real interaction with instructors and/or classmates. In several previous studies, it has been found that neuroticism is positively linked to compulsive use of SNS and social apps (Hughes et al., 2012), which can be explained to the extent that individuals with higher neuroticism seek for social interaction online, even though they feel stressful and anxious in real interaction. It can be suggested that task-related use of Internet and mobile devices is not same as non-task related use for making friendships and interacting with other people in virtual environment. Extraversion was found to be negatively linked to the likelihood of data breach at the universities. McBride et al. (2012) emphasized that individuals with higher extraversion are less likely to comply with cybersecurity procedure. Neuroticism was not found to have any impact on the likelihood of data breach. It can be related to the findings of hypothesis between neuroticism and task-related compulsive technology use.

Internal locus of control and external locus of control were added as external variables due to the findings of previous studies that individuals with internal locus of control try to control their actions, by reducing the stress and making plans, while those with external locus of control express more Internet addiction and credit card misuse (Chak & Leung, 2004). Accompanying the findings of Lee et al. (2014) that smartphone users with higher external locus of control are more tended to compulsively use smartphones, this study expected that in m-learning context through mobile portable devices, students with external locus of control could be more tended to experience task-related compulsive technology use compare to those with higher internal locus of control. There is a possibility that students who are aware of their behavior and able to plan their learning activities are less dependents on the mobile devices as parts of m-learning environment. Hence, they show less Internet addiction, particularly in educational context.

This study also found that students' excessive use of mobile devices and Internet for educational purposes by downloading materials from Internet, sending documents through network and other kind of activities could potentially result in a breach of privacy and personal information.

Another interesting finding is related to the moderating effect of the medium of access between task-related compulsive technology use and likelihood of data breach (see Fig. 2). Students might think that personal data can be stolen or lost on mobile devices easily compared to other devices. In addition, it was hypothesized that the medium of access might also have a moderating effect between personality diversity and task-related compulsive technology use. Opposing to Lee et al. (2014), the excessive of Internet on mobile devices does not differ for students with different personalities. However, extreme use of mobile devices by the students could potentially lead to the DB.

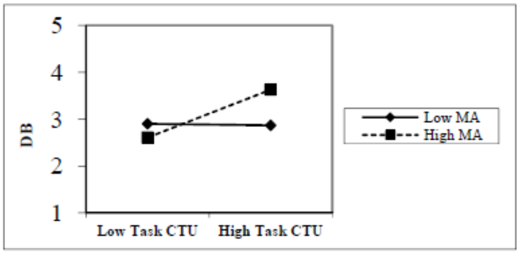

Figure 2. Graphical representation of moderation effect of MA between Task CTU and DB

8. CONCLUSION, IMPLICATIONS AND FUTURE WORK

This study has several contributions. In light of theoretical contribution, this research explores task-related compulsive technology use in an educational context. As Human errors surpass the technology errors, this study focuses on the relationship between personality diversity of university students and their compulsive use of Internet on mobile devices for academic purposes. Following the suggestions of Clements and Boyle (2018), this study also addresses the potential consequences of excessive use of Internet on mobile devices in line with the data breach.

Hence, it is highlighted that mobile devices used in m-learning process can produce the breach of data and privacy of university students. In practice, this finding can urge the system designers to purposefully design m-learning system with certain features that can prohibit the data and privacy loss but provide students and instructors with safe and efficient learning tools.

M-learning environment provides students and instructors with the opportunity to engage in an experience of creative learning with resources that can be accessed at anywhere and anytime. The current study attempted to investigate the m-learning process with the consideration of personality, Internet behavior, and cybersecurity risk factors. Personality was assessed with the Big Five traits, while Internet behavior was assessed with the task-related compulsive technology use to see whether students are excessively engaged in using mobile devices and Internet in m-learning process or not. In addition, cybersecurity risk such as data breach was considered due to the growing potential of identity and personal data theft on mobile devices in the recent years. As the strict measure against vulnerability to cyber-attacks and data loss puts an emphasis towards human factors, research in this nature becomes highly necessary.

As personality diversity of students shapes their compulsive use of Internet, which in its turn leads to the likelihood of data breach, it is necessary to promote the security awareness in m-learning environment. They must be instructed to use mobile devices proportionately to reach maximum academic goals and minimum privacy loss. The susceptibility of the types of devices used in m-learning environment must be assessed and students must be encouraged to use less-vulnerable devices.

A potential limitation of this study can be regarded as a subject being students without inclusion of their awareness level with potentially negative outcomes of excessive reliance on Internet and mobile devices. Younger Internet users, particularly students might not be well-aware of potential risky outcomes of compulsive use, which can be assessed with their knowledge and expertise with data breach and cybersecurity rules.

Non-task-related use of Internet by users with different personalities might lead to the breach of privacy and personal data outside of educational setting too. Hence, it creates the potential for future investigation of task-related vs. non-task-related use of Internet by individuals with different personalities and DB, particularly in business environment, due to the opportunity for corporate date theft and irresponsible Internet behavior of employees at the workplace. Finally, the types of devices can be differentiated such as mobile vs. desktop devices to assess the vulnerability against data breach.

ACKNOWLEDGMENT

The author is thankful to the management and staff of Sur University College for their full support and cooperation in getting this research work accomplished in time.

REFERENCES

[1] Al-Emran, M., Esherif, H. M., & Shaalan, K. (2016). Investigating attitudes towards the use of mobile learning in higher education. *Computers in Human Behavior*, 56, 93-102.

[2] Al Khawaldi, H. (2000). Faculty perceptions toward ET status at Omani colleges of education. Unpublished MA thesis, Yarmouk University, Jordan.

[3] Aladwani, A. M., & Almarzouq, M. (2016). Understanding compulsive social media use: The premise of complementing self-conceptions mismatch with technology. *Computers in Human Behavior*, 60, 575-581.

[4] Amiel, T., & Sargent, S. L. (2004). Individual differences in internet usage motives. *Computers in Human Behavior*, 20, 711–726.

[5] Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 10(3), 411-423.

[6] Ang, C. (2017). Internet habit strength and online communication: Exploring gender differences. *Computers in Human Behavior*, 66, 1–6.

[7] Anning-Dorson, T., Kastner, A., & Mahmoud. (2013). Investigation into mall visitation motivation and demographic idiosyncrasies in Ghana. *Management Science Letters*, 3(2), 367-384.

[8] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2016). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443.

[9] Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51, 1173–1182.

[10] Barrick, M. R., & Mount, M. K. (1991). The Big Five personality dimensions and job performance: A meta-analysis. *Personnel Psychology*, 44, 1–26.

[11] Thomas, B. J. (2020). Personality traits and work-related compulsive technology use: An organizational perspective. *International Journal of Psychosocial Rehabilitation*, 24(6), 2624-2645.

[12] Battle, K. (2018). Security management for mobile devices of higher education. Mathematics and Computer Capstones, 37. https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1036&context=mathcompcapstones.

[13] Baumeister, R. F. (2002). Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior. *Journal of Consumer Research*, 28 (4), 670–676.

[14] Boso, N., Story, V. M., & Cadogan, J. W. (2013). Entrepreneurial orientation, market orientation, network ties, and performance: Study of entrepreneurial firms in a developing country. *Journal of Business Venturing*, 28, 708-727.

[15] Chak, K., & Leung, L. (2004). Shyness and locus of control as predictors of internet addiction and internet use. *Cyber Psychology & Behavior*, 7(5), 559–570.

[16] Chang, C.-T., Tu, C.-S., & Hajiyev, J., (2019). Integrating academic type of social media activity with perceived academic performance: A role of task-related and non-task-related compulsive Internet use. *Computers & Education*, 139, 157-172.

[17] Chen, J. V., Chen, C. C., & Yang, H.-H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management & Data Systems*, 108 (1), 87–106.

[18] Clements, A. J., & Boyle, R. (2018). Compulsive technology use: Compulsive use of mobile applications. *Computers in Human behavior*, 87, 34-48.

[19] Clements, J. A. (2015). Beyond Habit: The role of sunk costs on developing automatic is use behaviors. *Journal of the Southern Association for Information Systems*, 3(1).

[20] Correa, T., Hinsley, A. W., & De Zuniga, H. G. (2010). Who interacts on the Web?: The intersection of users' personality and social media use. *Computers in Human Behavior*, 26 (2), 247–253.

[21] Costa, P. T., & McCrae, R. R. (1992). Normal personality assessment in clinical practice: the NEO Personality Inventory. *Psychological Assessment*, 4 (1), 5–13.

[22] Courneya, K. S., & Hellsten, L-A. M. (1998). Personality correlates of exercise behavior, motives, barriers and preferences: An application of the five-factor model. *Personality & Individual Differences*, 24(5), 625-633.

[23] De Cock, R., Vangeel, J., Klein, A., Minotte, P., Rosas, O., & Meerkerk, G.-J. (2014). Compulsive use of social networking sites in Belgium: Prevalence, profile, and the role of attitude toward work and school. *Cyberpsychology, Behavior, and Social Networking*, 17(3), 166–171.

[24] De Guinea, A. O., & Markus, M. L. (2009). Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing Information Technology use. *MIS Quarterly*, 33(3), 433-444.

[25] Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The mini-IPIP scales: tiny-yet-effective measures of the Big Five factors of personality. *Psychological Assessment*, 18, 192-203.

[26] Egelman, S., & Peer, E. (2015). Predicting Privacy and Security Attitudes. *Computers and Society: The Newletter of ACM SIGCAS*, 45 (1), 22–28.

[27] Gosling, S. D., Augustine, A. A., Vazire, S., Holtzman, N., & Gaddis, S. (2011). Manifestations of personality in online social networks: self-reported Facebook-related behaviors and observable profile information. *Cyberpsychology, Behavior, and Social Networking*, 14 (9), 483–488.

[28] Griffiths, M. D. (2013). Internet addiction in adolescence: Challenges, prevention and intervention. In M. Kim (Ed.), *Saving children from the Internet* (pp. 19-45). Seoul: Kachi Books.

[29] GSMA. (2016). The Mobile Economy Middle East and North Africa. https://www.gsmaintelligence.com/research/?file=9246bbe14813f73dd85b97a90738c860&download.

[30] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3.

[31] Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate data analysis. Upper Saddle River, NJ: Prentice Hall.

[32] Hair, J. R., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). Multivariate data anlysis (6th ed.). Upper Saddle River, NJ: Pearson-Prentice Hall

[33] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support System*, 47(2), 154–165.

[34] Hsiao, K.-L., Shu, Y., & Huang, T.-C. (2017). Exploring the effect of compulsive social app usage on technostress and academic performance: Perspectives from personality traits. *Telematics and Informatics*, 34, 679-690.

[35] Hughes, D. J., Rowe, M., Batey, M., & Lee, A. (2012). A tale of two sites: Twitter vs. Facebook and personality factors of social media use. *Computers in Human Behavior*, 28, 561-569.

[36] Kim, M.-K., Wong, S. F., Chang, Y., & Park, J.-H. (2016). Determinants of customer loyalty in the Korean smartphone market: Moderating effects of usage characteristics. *Telematics and Informatics*, 33, 936-949.

[37] Kim, Y., & Jeong, J. S. (2015). Personality predictors for the use of multiple internet functions. *Internet Research*, 25 (3), 399–415.

[38] Klobas, J. E., McGill, T. J., Moghavvemi, S., & Paramanathan, T. (2018). Compulsive YouTube usage: A comparison of use motivation and personality effects. *Computers in Human Behavior*, 87, 129-139.

[39] Kurfali, M., Arifoğlu, A., Tokdemir, G., & Pacin, Y. (2017). Adoption of e-government services in Turkey. *Computers in Human Behavior*, 66, 168-178.

[40] Landers, R. N., & Lounsbury, J. W. L. (2006). An investigation of Big Five and narrow personality traits in relation to Internet usage. *Computers in Human Behavior*, 22(2), 283-293.

[41] Laskaris, J. (2018). 7 Awesome Advantages of Mobile Learning. https://www.talentlms.com/blog/7-awesome-mlearning-benefits/.

[42] Lee, Y. K., Chang, C. T., Lin, Y., & Cheng, Z. H. (2014). The dark side of smartphone usage: psychological traits, compulsive behavior and technostress. *Computers in Human Behavior*, 31, 373-283.

[43] Lefcourt, H. M. (1991). Locus of control. In J. P. Robinson, P. R. Shaver, & L. S. Wrightsman (Eds.), Measures of personality and social psychological attitudes (pp. 413–499). San Diego: Academic Press.

[44] Mamaonov, S., & Benbunan-Fich, R. (2015). An empirical investigation of privacy breach perceptions among smartphone application users. *Computers in Human Behavior*, 49, 427-436.

[45] Marahatta, S. B., Adhikari, B., Aryal, N., & Regmi R. (2015). Internet addition and associated factors among health science students in Nepal. *Journal of Community Medicine & Health Education*, 5(4).

[46] Mark, G., & Ganzach, Y. (2014). Personality and internet usage: a large-scale representative study of young adults. *Computers in Human Behavior*, 36, 274–281.

[47] McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International–Institute of Homeland Security Solutions, North Carolina.

[48] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016). Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156.

[49] McCrae, R. R., & John, O. P. (1992). An introduction to the five-factor model and its applications. *Journal of Personality*, 60 (2), 175–215.

[50] McIntyre, E., Wiener, K. K. K., & Saliba, A. J. (2015). Compulsive Internet use and relations between social connectedness, and introversion. *Computers in Human Behavior*, 48, 569-574.

[51] Meerkerk, G. J., Van Den Eijnden, R. J. J. M., Vermulst, A. A., & Garretsen, H. F. L. (2009). The compulsive internet use scale (CIUS): Some psychometric properties. *Cyber Psychology & Behavior*, 12(1), 1–6.

[52] Nunnally, J. C. (1978). Psychometric theory (2nd ed.). New York, NY: McGraw-Hill.

[53] Oxford University Press. (2015). *Learn about virtual learning environment/Course Management System content*. http://tinyrul.com/o54enla

[54] Panda, A., & Jain, N. K. (2018). Compulsive smartphone usage and users' ill-being among young Indians: Does personality matter? *Telematics and Informatics*, 35, 1355-1372.

[55] Panko, R. (2010). *Corporate Computer and Network Security*, second ed. Prentice Hall, Upper Saddle River, NJ.

[56] Ponemon Institute LLC. (2018). 2018 cost of a data breach study: Global overview. https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

[57] Porter, G., & Kakabadse, N. K. (2006). HRM perspectives on addiction to technology and work. *Journal of Management Development*, 25, 535-560.

[58] Quinones, C., Griffiths, M. D., & Kakabadse, N. K. (2016). Compulsive Internet use and workaholism: An exploratory two-wave longtitudinal study. *Computers in Human Behavior*, 60, 492-499.

[59] Roberts, J. A., Pullig, C., & Manolis, C. (2015). I need my smartphone: a hierarchical model of personality and cell-phone addiction. *Personality and Individual Differences*, 79, 13–19.

[60] Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. Psychological Monographs: *General and Applied*, 80(1), 1–28.

[61] Sapp, S. G., & Harrod, W. J. (1993). Reliability and validity of a brief version of Levenson's locus of control scale. *Psychological Reports*, 72(2), 539–550.

[62] Servidio, R. (2014). Exploring the effects of demographic factors, Internet usage and personality traits on Internet addiction in a sample of Italian university students. *Computers in Human Behavior*, 35, 85–92.

[63] Shih, H.-P. (2004). An empirical study on predicting user acceptance of e-shopping on the Web. *Information & Management*, 41, 351-368.

[64] Shropshire, J., Warkentin, M., Johnston, A. C., & Schmidt, M. B. (2006). Personality and IT security: An application of the five-factor model. *Americas Conference on Information Systems (AMCIS)*, 3443–3449.

[65] Tan, W. K., & Yang, C. Y. (2014). Internet applications use and personality. *Telematics & Informatics*, 31 (1), 27–38.

[66] Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. Workshop on Socio-Technical Aspects in Security and Trust, 24–30.

[67] Van De Vijver, F. J. R., & Leung, K. (1997). Methods and data analysis for cross-cultural research. CA: Sage Publications.

[68] Verplanken, B., & Aarts, H. (1999). Habit, attitude, and planned behavior: Is habit an empty construct or an interesting case of goal-directed automaticity? *European Review of Social Psychology*, 10(1), 101-134.

[69] Wagner, M. (2017). 95% of All Security Incidents Involve Human Error – Insider Threat. https://edwps.com/cyber-the-insider-threat-by-melissa-wagner/.

[70] Wang, J. L., Jackson, L. A., Zhang, D. J., & Su, Z. Q. (2012). The relationships among the Big Five Personality factors, self-esteem, narcissism, and sensation-seeking to Chinese University students' uses of social networking sites (SNSs). *Computers in Human Behavior*, 28 (6), 2313–2319.

[71] Wu, K., Lindsted, K. D., Tsai, S-Y., & Lee, J. W. (2008). Chinese NEO-PI-R in Taiwanese adolescents. *Personality and Individual Differences*, 44, 656-667.

[72] Xu, R., Frey, R. M., Fleisch, E., & Ilic, A. (2016). Understanding the impact of personality traits on mobile app adoption–Insights from a large-scale field study. *Computers in Human Behavior*, 62, 244–256.

[73] Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: new trends in risk management. *Cyber Psychology Behaviors*, 7 (1), 105–111.

BASIL JOHN THOMAS, is an Assistant Professor in Human Resources at Sur University College affiliated to Bond University Australia and University of Sunderland, UK. He is the recipient of GCC Educational Leadership Award for the 'Best Professor in HR and Organizational Studies' honored by the World Federation of Academic & Educational Institutions Jury in 2019 March. Later he was honored with the Global Outreach Research and education Award too in 2019 April for the Outstanding teacher in Management followed by the Hundred talented professors in the world, the Asian Leadership Award and finally the Oman education leadership Award. His research interests include Organizational Behavior, Innovation and Creativity, Employee Stress Analysis, Work life balance, ICT in Education and Investor's Behavior.

JEYHUN HAJIYEV received the Ph.D. degree from the Department of Information Management, Graduate Institute of Business and Management, Chang Gung University, Taiwan, in 2018, where he is currently a Postdoctoral Fellow. His major research interests include digital marketing technologies, e-learning, e-banking, and mobile technologies.