A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy

Vincent Cho, PhD
Associate Professor
Department of Management and Marketing
The Hong Kong Polytechnic University
Hong Kong
Email: vincent.cho@polyu.edu.hk
Tel: (852) 27666339
Fax: (852) 27650611

and

Andrew W.H. Ip, PhD
Associate Professor
Department of Industrial and Systems Engineering
The Hong Kong Polytechnic University
Email: wh.ip@polyu.edu.hk

Please direct all correspondence to Dr V. Cho, whose correspondence address is given above and whose email address is vincent.cho@polyu.edu.hk.

Acknowledgements

We are grateful to two anonymous referees for their constructive comments on an earlier version of this paper.

A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy

Abstract

Why would employees adopt bring your own device (BYOD)? Would employees feel risk-taking to perform their work by using their own devices? Would peer pressure and company policy help encourage their employees to BYOD and how? Using the Technology Threat Avoidance Theory (TTAT), we hypothesize the intention of adopting BYOD is due to the accessing of security policy by threat and coping appraisal. Moreover, we predict perceived usefulness, perceived ease of use, social influence, organizational commitment and job security are essential for formulating the adoption intention. In this study, 450 random employees were surveyed on their adoption perception of BYOD in their respective companies. The results support most of our hypotheses. We uncover perceived cost and privacy protection within the TTAT framework reflect no significance while organizational commitment and job security posit the strongest influences on employees' BYOD adoption intention. This finding suggested that in order to roll out a successful and sustainable adoption intention on BYOD, organizations must consider measurements to build up employees' job security as well as generate a strong sense of organization commitment. Specifically, our analyses show adoption intention is also affected by gender, age, and education level.

Keywords: bring your own device, adoption intention, security policy, job security, organizational commitment.

Introduction

Organizations establish Bring Your Own Device (BYOD) policy to permit employees to use their personal mobile devices to access company information and to perform their jobs. Along with this trend, our commercial world has become a rather mobile worker community. A study by IBM showed the benefits of BYOD include cost savings, increased productivity and employee satisfaction for an organization. For convenience, employees can use their own devices for daily business work. However, there are certain security concerns when using their own devices. For example, if an employee uses his/her own device for work accidentally loses it or the device got stolen, an unauthorized party could access and retrieve company data from the device. Another type of security breach is if an employee leaves the organization, he/she doesn't oblige to return his/her own device. The device may still have the company's proprietary applications and data saved somewhere. Nowadays family members often share electronic devices at home such as tablets and personal computers; a child may play games on the device and accidentally access and expose sensitive data. Furthermore, people sometimes sell their used devices in the second hand market and may forget to wipe out all the sensitive information.

In this regard, an organization should consider how to protect their employee's devices if they can use the device to access sensitive company information and to monitor their usage on work related activities. Security controls on mobile devices are necessary in order to protect involuntary information leaks and unpredictable thefts (Jansen and Grance, 2011). Well-architected back-end services and supports along with appropriate organization security policy are important for building a successful scheme for BYOD.

This study aims to explore the factors affecting employees' adoption intention of BYOD. In addition to the well-established factors such as perceived usefulness, perceived ease of use and social influence as stated in Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB), our framework includes Technology Threat Avoidance Theory (TTAT) as proposed by Liang and Xue (2009) to capture the threat from adopting BYOD and coping assessment of security policy for BYOD. Specifically, perceived severity of losing corporate information from personal devices, privacy protection of using employees' own device for work, perceived costs of following the security policy for BYOD, perceived effectiveness of a company's security policy, and self-efficacy of following the security policy for BYOD are examined to understand whether employees will adopt BYOD. Other concerns are related to employee's organization commitment and job security.

This research has both theoretical and commercial contributions. Our theoretical framework integrates TTAT to assess potential threats due to BYOD and corresponding coping approach of following security policy from an organization to investigate employees' adoption intention of BYOD. This study fills in the gap of how TTAT be applied to investigate adoption of technologies, which are embedded with potential threats. Our findings could help organisations to understand the essential factors, which facilitate or prohibit employees in adopting BYOD. There are also implications for cloud service providers to develop better and safer mobile security applications so they could get more new corporate business.

Literature Review

Past studies of BYOD are mainly focused on four different perspectives (Aaron, et al. 2014; Rose, 2013). First, how were BYOD being applied? Along this vein, a few researchers explored the feasibilities of using BYOD in different business domains (Mitrea, 2014; Tomislav, et al. 2014; Marshall, 2014; Davis, 2013) and education (Song, 2014; Sangani, 2013; Kobus, et al. 2013). From a corporate perspective, both Mitrea (2014) and Leclercq - Vandelannoitte (2015) studied the impact of using mobile devices for the employees. While in the healthcare arena, Marshall (2014) illustrated the practical benefits of a healthcare organization on the implementation of BYOD and Davis (2013) suggested using a patient's own device in global clinical trials. For education, Song (2014) found that students advanced their understanding of the anatomy of fish well beyond what was available in the textbook and they developed positive attitude toward seamless science inquiry supported by their own mobile devices. All in all, these studies help shed light on the stakes involved in BYOD regardless at the organization or individual level.

Second, the technological innovations for BYOD are proposed. Inventors whether from mechanical, electrical or electronics fields were relentlessly inventing new hardware and software in the hope of supplementing and complementing the BYOD environments. For instance, BenQ America developed and introduced a DLP projector specifically addressed the needs for BYOD in 2014. A couple innovations studies included Liagouras et al. (2014) explored the complexity of dynamic calendar based on location-aware technologies for trip planning, and Watts (2014) proposed a two-factor authentication method to access organizational data and application securely.

Third, the policies for security and privacy protection are suggested. Ansaldi (2013) suggested companies should consider various security challenges behind BYOD. This includes how to protect personal privacy and data breaches. Armando et al. (2014) presented a security framework for verifying and enforcing BYOD security policies on Android devices. Garba et al. (2015) reviewed information security and privacy in BYOD environments. They found that the current technologies to manage BYOD are still immature and the risks are perhaps not widely known. It is imperative for organizations to invest time and adequate resources to protect their confidential information resources when implementing BYOD. Holleran (2014) suggested deploying a corporate owned, personally enabled enterprise mobility model that fortify employees with a mobile device that can be used securely for both work and personal communications. Crossler et al. (2014) examined the factors that determine whether employees follow Bring Your Own Device (BYOD) policies through the lens of the Protection Motivation Theory. They found that self-efficacy and perceived threat severity of BYOD are salient factors for adopting BYOD policy. Moreover, Coates (2014) proposed that auditors need to ensure their organization has a map in place for connecting personal devices to corporate networks and data. Along this issue, Fauld et al. (2016) suggested how data to be captured in multicenter for medical audit. Numerous of researches were found focusing on the importance of security and privacy protection policy when BYOD was involved.

Fourth, the acceptance of employee of using BYOD is also an essential concern. Marshall (2014) listed out hurdles that must be overcome when hospital employees begin using consumer IT devices in the workplace. It is crucial to ensure employees develop a sense of personal freedom when deploy BYOD. Weeger et al. (2015) have investigated the factors that determine on employee's intention to participate a BYOD program using the modified technology acceptance model. They showed that performance expectancies have the strongest impact on intention, while perceived threats have the negative impacts. In this regard, our study attempts to investigate the effectiveness of security policy to eliminate the threat of adopting BYOD. This will fill in the research gaps to understand the importance of security policy in BYOD adoption.

An overview of past studies focused on four different perspectives mentioned above in the literature review is captured in the table 1 below.

Table 1: Literature Review

Author	Methodology	Findings
Research Domains		
Mitrea, D.	Survey	Impacts of mobile applications on BYOD.
Tomislav et. al.	Theoretical Paper	Identified new trends in mobile technology and importance in supply chain management.
Song, Y.	Survey	Demonstrated students' improvement in learning and understanding through the use of BYOD.
Sangani, K.	Theoretical Paper	Identified benefits of adopting BYOD in school.
Kobus et. al	Survey	Examined students' position on BYOD implementation in school.
Leclercq-Vandelannoitte, A.	Survey	Identified three organization reactions to incorporate IT innovations and manage BYOD.
Davis, T.	Theoretical Paper	Demonstrated device independence in medical field.
Technological Innovations		
Liagouras et. al.	Theoretical Paper	Explored the complexity of dynamic calendar from trip planning.
Watts, S.	Theoretical Paper	Proposed a two-factor authentication method to access organizational data and application securely.
Company Privacy Protection		
Ansaldi, H.	Theoretical Paper	Explored security challenges on persoanl privacy protection and data breaches.
Armando et. al.	Theoretical Paper	Presented a security framework to verify and enforce BYOD security policy on Android devices.
Garba et. al.	Survey	Examined different dynamics relating to security and privacy in BYOD environments.
Holleran, J.	Theoretical Paper	Proposed using a COPE based approach to build a better BYOD strategy.
Crossler et. al.	Survey	Leveraged Protection Motivation Theory (PMT) to examine factors that employees to follow BYOD policies.
Coates	Theoretical Paper	Addressed BYOD issues among internal auditors.
Fauld et. al.	Survey	Assessment of data protection and accuracy during data collection for medical audit.
Employee Psychological Status		
Marshall, S.	Theoretical Paper	Identified challenges of BYOD implementation in medical setting.
Weeger et. al.	Survey	Identified determining factors on employees' participation intention on BYOD.

Theoretical Framework

From the review of the extant literature, we understand that security policy is essential but there is lack of understanding on how does BYOD policy affect employees' adoption of BYOD. Figure 1 depicts our framework, which is based on Technology Acceptance Model – TAM (Venkatesh & Davis, 2000), Theory of Planned Behavior (Ajzen, 1985), and Technology Threat Avoidance Theory – TTAT (Liang and Xue, 2009). In particular, our framework investigates risk assessment and avoidance for adopting BYOD. The following elaborate the details of our hypotheses.

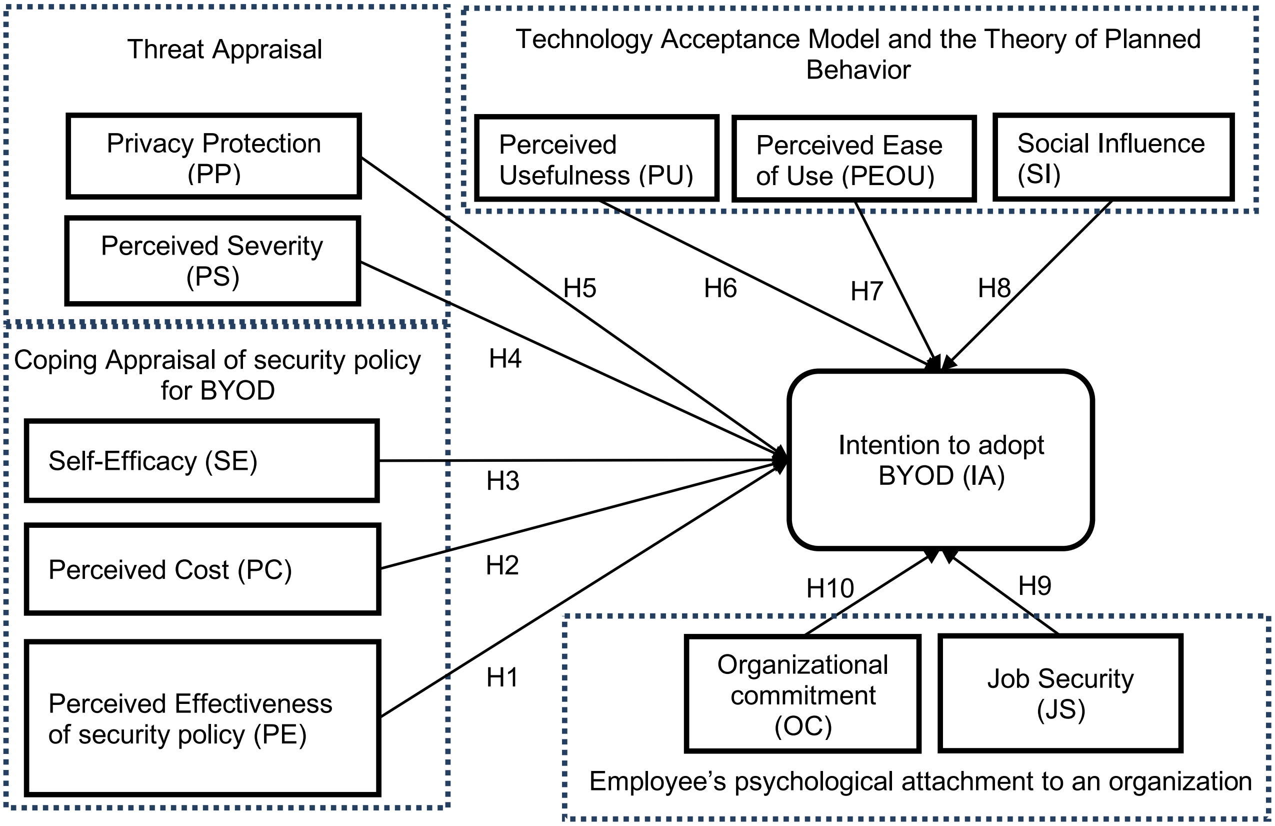
Threat Appraisal
Privacy Protection (PP)
Perceived Severity (PS)
Technology Acceptance Model and the Theory of Planned Behavior
Perceived Usefulness (PU)
Perceived Ease of Use (PEOU)
Social Influence (SI)
H5
H6
H7
H8
H4
Coping Appraisal of security policy for BYOD
Self-Efficacy (SE)
Perceived Cost (PC)
Perceived Effectiveness of security policy (PE)
H3
H2
H1
Intention to adopt BYOD (IA)
H10
H9
Organizational commitment (OC)
Job Security (JS)
Employee's psychological attachment to an organization

Figure 1: Theoretical Model

Perceived effectiveness (PE) refers to how effective a security policy is on threat avoidance when adopting BYOD. A study by the Information Security Forum (2000) suggested that as high as 80% of major security failures were due to human error rather than system malfunction. In order to better governance employees' work activities when using their own devices, the company relies on its security policy. A BYOD policy could help reduce the severity of any unpredictable incidents (Leach, 2003). Without an effective security policy, allowing employees to access organization resources from their personal devices could be detrimental. For this reason, we suggest the following hypothesis.

H1: Perceived effectiveness of security policy relating to BYOD has positive influence on intention to adopt BYOD.

Perceived cost (PC) refers to an individual's physical and cognitive efforts that are required to carry out a safeguard measure under a security policy (Liang and Xue, 2009). It includes any costs that are associated with taking the adaptive coping actions, such as money, time, effort, inconvenience, unpleasantness, difficulty, comprehension, or any negative effects for adopting the BYOD security policy (Lee and Larsen 2009). Normally, a user would weigh the threat avoidance if to cope with the security policy against its expected costs. If the costs exceed the benefits, the user is likely not taking the coping actions (Tu and Yuan, 2012). For example, periodic data backup of a mobile device is regulated by a security policy so as to cope with potential loss of data. However, the backup action takes time and could cause inconvenience. If the user believes the data in his/her mobile devices is not that important compare with the backup efforts spent, he/she may not do the regular backup activity as instructed. Moreover, some companies may require the employees to turn on the GPS of their devices to as to trace the location of the devices. This helps to find the device in case it is being lost. However, employees may have concerns about their personal privacy as well as the battery consumption of the GPS. Hence, when people perceive the costs of implementing protections of information and following through the policy exceed its corresponding benefits, they are likely not adopting BYOD.

H2: Perceived cost of adopting a security policy for BYOD has negative influence on intention to adopt BYOD.

Self-efficacy (SE) is a person's self-confidence in his ability to perform a behavior (Bandura, 1977). The origin of self-efficacy came from the social cognitive theory and is refer to an individual's self-confidence in his ability to perform a response action. According to the social cognitive theory, individuals with greater confidence in their abilities are more likely to initiate challenging behaviors such as smoking cessation. In this study, self-efficacy refers to one's ability to apply security control as indicated by security policy to overcome the threat from adopting BYOD. Hence, one's self-efficacy will affect his/her willingness to adopt BYOD.

H3: Perceived self-efficacy of apply security control has positive influence on intention to adopt BYOD.

Perceived severity (PS) is described as the degree of physical harm, psychological harm, social threats, and/or economic harm that is endanger to an individual (Lee and Larsen 2009). When an organization allows its employees using their own mobile devices to perform work instead of giving them an assigned company computer, security threat could be a big issue to both the company and the users. Perceived severity of negative consequences is not limited to the damage or loss of the employees' device and data, but also on the company. In general, employees may respond differently based on their perceived severity for adopting BYOD (Workman et al., 2008). Consequently, we propose the following hypothesis.

H4: Perceived severity of negative consequences has negative influence on intention to adopt BYOD.

Employees are cautious about whether their personal data are protected especially when using their own devices for work activities. Privacy protection (PP) and data confidentiality are major concerns. Some organizations have the rights to access their employees' mobile devices where activities are being tracked. Hence, personal privacy for using his/her own mobile device is a concern. Moreover, some organizations rely on their cloud service providers to provide security protection. In this regard, the exposure of employees' personal information to an unauthorized party is possible. If the employees feel their personal data protection are not guarantee, it will hinder them to adopt BYOD. Hence, we have the following hypothesis.

H5: Privacy protection for employees' personal data when using their personal devices for work activities has positive influence on intention to adopt BYOD.

The Technology Acceptance Model posits that perceived ease of use (PEOU) and perceived usefulness (PU) has a direct effect on the intention adoption towards using a new technology (Venkatesh & Davis, 2000; Ajzen & Fishbein, 1980). In literature, both PU and PEOU are found to be significant determinants of behavioral intention to adopt. In this regard, the following hypotheses based on the TAM-relationship are proposed.

H6: Perceived Usefulness will have a positive effect on intention to adopt BYOD.

H7: Perceived Ease of Use will have a positive effect on intention to adopt BYOD.

According to the Theory of Planned Behaviour (TPB) (Ajzen, 1985), social influence (SI) is related to an individual's emotions, opinions, and/or behaviors that are affected by others. It is a social pressure that drives an individual to comply. Social influence also affects an individual to adopt a socially desirable behavior (Lee and Larsen, 2009). Hence, we expect that an employee will adopt BYOD if he/she perceives other employees in the organization are doing the same.

H8: Social influence has positive influence on intention to adopt BYOD.

Job security (JS) exerts a positive influence on employees' psychological well-being and work behavior (Ashford, Lee, and Bobko, 1989; De Witte, 1999; Sverke, Hellgren and Nässwall, 2002). Research has shown that the greater job satisfaction and job security the employees feel, the higher their job performance they have (Yousef, 1998). The present paper operationalizes job security as job stability, commonly found in research on stress and health-related outcomes (Godin and Kittel, 2004).

According to the psychological contract literature, employers are expected to provide job security in order to receive loyalty and commitment in return from their employees (Kalleberg, Rognes, 2000; McDonald & Makin, 2000). Psychological contracts refer to "the idiosyncratic set of reciprocal expectations held by employees concerning their obligations and their entitlements" (McLean Parks, Kidder and Gallagher, 1998, p. 698). However, the rapidly changing organization environment has produced increase feelings of insecurity among employees (Sverke *et al.*, 2002). Mergers, acquisitions, downsizing and the recent economic crisis all pose threats to employees' job security (Ashford *et al.*, 1989; Van Gyes & Szekér, 2013). When employees experience danger to their perceived entitlement of job security, they may perceive a breach of the psychological contract against their organization (King, 2000; Pearce, 1998), which lead to a sense of betrayal (De Cuyper, Notelaers and De Witte, 2009). If employees experience low job security, they are more worry about BYOD and are afraid of any mistakes from using their own device could lose their jobs. In contrast, we hypothesized that employees who are experiencing better job security would positively sync up with the organizational policy, and are more comfortable with BYOD (Ashford *et al.* 1989; Bhuian and Islam, 1996).

H9: Job security posits a positive influence on intention to adopt BYOD.

Organizational commitment (OC) is defined as "a state in which an employee identifies with a particular organization and its goal" (Blau and Boal, 1987, p. 290). We hypothesize that committed employees are more likely to adopt BYOD, because of their commitment; they are more engaged to follow and execute organization policies.

H10: Organizational commitment has a positive influence on intention to adopt BYOD.

Methodology

Measurements

In terms of coping appraisal, we adapted the constructs (perceived effectiveness, perceived cost and self-efficacy) and the items as suggested by Liang and Xue (2010). The respondents were asked to complete four items (e.g. Security policy would be useful for protecting my mobile device) on perceived effectiveness of security policy for BYOD. Three items on the perceived cost (e.g.

following security policy is too much trouble); and four items on self-efficacy (e.g. I am able to apply security control on my mobile device without much effort).

We also followed the five items on perceived severity for appraising threat of adopting BYOD suggested by Liang and Xue (2010). For example, “Having mobile devices infected by a virus as a result of opening a suspicious file is a serious problem for me.”

For privacy protection, we applied the three items from Bucanan et al. (2007) as follows: “My company will not collect the personal data from my mobile device,” “this security policy will not use my personal information in device to any purpose unless I authorize it to do so,” and “when running business application, the personal information in my mobile device will not be used for any purpose.”

The items used to measure perceived usefulness and perceived ease of use, each having four items, are based on the scale of Davis (1989) with appropriate modifications pertinent to BYOD adoption. For instance, “BYOD enables me to accomplish tasks more quickly” is an item of perceived usefulness and “I have no trouble in using BYOD” is an item of perceived ease of use.

To measure social influence, three items were extracted from Taylor and Todd (1995) and Rucker and Petty (2006). For instance, “Colleagues who influence my behavior think that I should adopt BYOD”.

Three items were selected from van Quaquebeke et al.’s (2008) on work values for accessing job security. They were “I feel that I am respected by administrators,” “senior executives appreciate my work to the organization,” “most of colleagues feel that whether or not the job gets done right is clearly their own responsibility.”

Another three items were extracted from Angle and Perry's (1981) to measure commitment. They were "I am willing to put in a great deal of effort beyond that normally expected in order to help this organization be successful," "I talk up this organization to my friends as a great organization to work for," "I would accept almost any type of job assignment in order to keep working for this organization."

For adoption intention of BYOD, we adapted three items from Liang and Xue (2010). For instance, "I tend to bring my own device for work," is an item of this construct. All items were measured using a 7-point Likert-type scale with 1 standing for "strongly disagree" and 7 standing for "strongly agree".

Survey procedure

BYOD is making significant inroads in the business world, with about 75% of employees in high growth markets including India and Malaysia and 44% in developed markets are already using their own technology at work. 78.6% of employees in high growth markets enjoy the flexibility of being able to access mobile enterprise applications outside office hours, versus 55.1% in mature markets. However, only 20.1% of employees on an average who use their personal devices signed a policy governing that behaviour (CXO Unplugged, 2012).

This study was conducted to assess the coping and threat appraisals of employees in adopting the security policies for BYOD. The survey was started on 1st July, 2016 through 31st July, 2016. Our target population included employees who were thinking to adopt BYOD for their work, and their companies had a BYOD security policy in place already. In order to reach a wide range of potential candidates, we picked some densely populated areas in Hong Kong after office hours and distributed the questionnaires. First, we asked if the candidates were BYOD users and if their companies have a security policy for BYOD. This was to make sure we were selecting the right samples. At last after intensive efforts, we reached 450 candidates who met our criteria. Thirty-two questionnaires were void because we found plenty missing data. The remaining four hundred and eighteen questionnaires were used for subsequent analyses. Table 2 below shows the descriptive statistics of their profiles and organizations.

Table 2: descriptive statistics of the respondents and their negative life events

<table>
<tr><td colspan="2"><i>Respondent profile</i></td></tr>
<tr><td><b>Gender:</b> Male (215, 51.4%),
Female (203, 48.6%)</td><td><b>Age</b>: 16-20 (51, 12.2%), 21-25 (78, 18.6%), 26-30 (83, 20.0%), 31-40 (76, 18.2%), 41-45 (62, 14.8%), 46-50 (52, 12.4%), 50 or above (16, 3.8%)</td></tr>
<tr><td colspan="2"><b>Education:</b> Secondary School (85, 20.3%), Diploma/Higher diploma (105, 25.1%), Graduate (152, 36.4%), Post graduate (76, 18.2%)</td></tr>
<tr><td colspan="2"><i>Organization profile of the respondents</i></td></tr>
<tr><td colspan="2"><b>Number of employees:</b> less than 50 (98, 23.4%), between 51 and 200 (86, 20.6%), between 201 and 500 (83, 19.9%), between 501 and 1000 (92, 22.0%), more than 1000 (59, 14.1%)</td></tr>
<tr><td colspan="2"><b>Business nature:</b> Financial sector (72, 17.2%), Retailing and trading (53, 12.7%), Hotel and tourism (69, 16.5%), Logistics and transportation (76, 18.2%), Public utilities (79, 18.9%), Government and Non-profit Organizations (69, 16.5%)</td></tr>
<tr><td colspan="2"><b>Business application:</b> Customer relationship management (70, 16.7%), Enterprise resources planning (56, 13.4%), Financial applications (62, 14.8%), Sales and marketing (83, 19.9%), Human resources management (69, 16.5%), logistic management (62, 14.8%), Others (16, 3.8%)</td></tr>
</table>

Analyses and Findings

We used the means, standard deviations, and bivariate correlations to analyze predictions of all variables. We also checked for multivariate normality of the data and were fairly normally distributed.

We tested sample bias by comparing key constructs from the earlier respondents and the later respondents using the Kolmogorov-Smirnov two-sample test (Siegel and Castellan, 1988). This test assesses whether significant differences exist in the distribution of respondents and non-respondents for a given variable, includes differences in central tendency, dispersion, skewness, and so forth. The results showed the data from both group of respondents were fairly equal.

Judging from the standard deviations of all the items, the sampled data had enough variations to represent the population. The means of the items, as shown in Table 3, suggest that the respondents tended to adopt BYOD with the mean(IA) equal to 4.18. On the one hand, they thought it was serious if they lost company data with the mean(PS) equal to 5.36 and they were confident that their companies would not retrieve their personal data (mean(PP)=4.95). On the other hand, they agreed that the security policy was effective (mean(PE)=4.82), it was easy to adopt the security policy (mean(PC)=4.72) and they felt they were capable to adopt the security policy without much help from others (mean(SE)=4.55). With respect to perceived usefulness and perceived ease of use, both constructs are of high levels (mean(PU)=4.43 and mean(PEOU)=4.34) indicating that the respondents thought that BYOD was useful and was easy to use for their work. They were also influenced by their peers in BYOD adoption (SI)=4.71). Moreover, their organization commitment and job security were rather high with the mean(OC) and mean(JS) at 4.72 and 5.20 respectively.

Table 3: Descriptive statistics, validity and reliability of the constructs

Constructs	Mean*	Std. Dev.	Factor Loading
Perceived Effectiveness of BYOD security policy - PE (Cronbach's alpha = 0.769)	4.82	1.11	
Security policy would be useful for protecting my mobile device	4.85	1.28	.751
Security policy would increase the protection of my mobile devices	4.68	1.26	.762
Security policy would enable me to protect my mobile device	4.92	1.35	.758
Security policy would enhance the effectiveness in protecting my mobile devices	4.82	1.31	.702
Perceived cost of following BYOD security policy – PC (Cronbach's alpha = 0.822)	4.72	1.25	
Security policy may cause problems to other programs on my mobile devices	4.68	1.46	.781
Following security policy is too much trouble	4.76	1.39	.793
PC3: I don't know how to follow the security policy	4.72	1.48	.761
Self-efficacy – SE (Cronbach's alpha = 0.813)	4.55	1.27	
I am able to apply security control on my mobile device without much effort	4.46	1.48	.801
I could follow security policy on my mobile device even if there was no-one around instructing me as I go along	4.38	1.51	.748
Applying security control on my mobile device is easy for me	4.66	1.43	.790
Applying security control on my mobile device is not difficult	4.71	1.40	.780
Perceived severity – PS (Cronbach's alpha = 0.799)	5.36	.902	
Having mobile device infected by a virus as a result of opening a suspicious file is a serious problem for me	5.12	1.11	.812
Losing organizational data as a result of opening a suspicious file is a serious problem to me	5.20	1.22	.803
Having my online identity stolen as a result of mobile hacking is a serious problem for me	5.38	1.05	.755
Spyware could record my internet activities and send it to unknown parties	5.50	1.11	.769
Spyware would invade my privacy data	5.61	1.03	.785
Privacy protection – PP (Cronbach's alpha = 0.785)	4.95	1.12	
My company will not collect the personal data from my mobile device	5.01	1.25	.751
The security policy of my organization will not use the personal information in my device for any purpose unless I authorize it to do so	4.95	1.31	.762
When running business application, my organization will not use my personal information for any purpose	4.88	1.29	.793
Perceived usefulness – PU (Cronbach's alpha = 0.851)	4.43	0.96	
BYOD enables me to accomplish tasks more quickly	4.38	1.11	.795
BYOD improves the quality of my tasks	4.35	1.21	.762
BYOD enhances the effectiveness of my tasks	4.51	1.18	.803
BYOD is useful to me	4.48	1.23	.815
Perceived ease of use – PEOU (Cronbach's alpha – 0.783)	4.34	1.01	
Use of my own device for work is simple	4.29	1.51	.780
I have no trouble in using my device for work	4.31	1.32	.756
My device provides information that is easy to comprehend for my work	4.51	1.26	.749
My device is easy to use	4.26	1.16	.792
Social influence – SI (Cronbach's alpha = 0.811)	4.71	1.15	
People who influence my behaviour think that I should use my own device for work	4.85	1.43	.801
People who bring their own device for work have a high profile	4.62	1.47	.753
My colleague thinks that I should bring my own device for work	4.66	1.39	.723
Job security – JS (Cronbach's alpha = 0.761)	5.20	0.96	
I feel that I am respected by administrators	5.23	1.01	.764
My supervisor appreciates my work to the organization	5.15	1.25	.798
Most of colleagues feel that whether or not the job gets done right is clearly their own responsibility	5.21	1.06	.756
Organizational commitment – OC (Cronbach's alpha = 0.768)	4.72	0.96	
I put in much effort beyond that normally expected in order to help this organization be successful	4.56	1.25	.788
I promote this organization to my friends as a great organization to work for	4.91	1.33	.791
I would accept almost any type of job assignment in order to keep working for this organization	4.69	1.29	.761
Adoption intention of BYOD – AI (Cronbach's alpha = 0.852)	4.18	1.01	
I tend to bring my own device for my work	4.21	1.12	.850
I predict I would bring my own device to facilitate my job	4.32	1.11	.825
I plan to bring my own device for work in coming six month	4.01	1.32	.768

* 1- strongly disagree and 7 – strongly agree. The factor loadings are all on their respective constructs.

To check the existence of common method bias, we conducted the Harmon one-factor analysis suggested by Podsakoff and Organ (1986). A factor analysis combining every variable in the research framework did not detect a single factor explaining the majority of covariance. In addition, the results of the regression analysis showed different degrees of significance for the regression coefficients. The above evidence collectively suggested that common method bias was not a serious concern in this study.

Reliability refers to a construct that is free from errors and yields consistent results. Cronbach's alpha was used to measure the internal consistency of the multi-item scales which was used in this study. Since the Cronbach's alpha values of all of the constructs were over 0.7, we claimed that they were all reliable. Moreover, all of the measures of the constructs were used in past studies, and the questionnaire was validated by experts in the fields of IT and behavioral science before it was administered, the content validity of all the constructs were deemed acceptable.

Convergent validity of the measurement scales was evaluated using the two criteria suggested by Fornell and Larcker (1981), namely (1) all the indicator factor loadings should be significant and exceed 0.70, and (2) the average variance extracted (AVE) for each construct should exceed the variance due to measurement errors for that construct (i.e., should exceed 0.5). The factor loadings of the items are shown in Table 3. All items exhibited a loading value higher than 0.7 on their respective constructs. Thus, acceptable item convergence on the intended constructs was achieved.

Table 4: correlation matrix

	AVE	1	2	3	4	5	6	7	8	9	10	11
1. PE	.553	.743										
2. PC	.606	.087	.778									
3. SE	.608	.137*	.154*	.780								
4. PS	.616	.155*	.025	.166*	.785							
5. PP	.591	.204**	.112*	.182**	.121**	.769						
6. PU	.630	.128*	.067	.156*	.069	.038	.794					
7. PEOU	.592	.098*	.028	.123*	.092	.086	.269**	.769				
8. SI	.577	.053	-.062	-.012	.081	.029	.086	.035	.760			
9. JS	.597	.069	.012	.060	.087	.120*	.102*	.085	.174*	.773		
10. OC	.609	.181*	-.057	.129*	.095	.052	.127*	.092	.175*	.218**	.780	
11. IA	.664	.331**	.033	.265*	-.110*	.142*	.118*	.105*	.060	.359***	.262**	.815

*, **, *** significant level with p-value less than 0.05, 0.01, and 0.001 (2-tailed).
the diagonal elements reporting the square root of the variance shared

Table 4 demonstrates the correlation matrix of the constructs, verifies whether the constructs potentially overlap by their correlations and helps to analyze whether the constructs are independent. This table consists of three pieces of information: 1) correlation coefficients among all constructs (PE, PC, …), 2) the average explained variance (AVE), which indicate the explained variance of the measurements of related construct, 3) the square root of AVE as stated on the diagonal in the matrix. If the correlation coefficients between two constructs are below 0.7, then they are deemed to be independent. As indicated in table 4, all correlation coefficients are less than 0.7 which indicate they are independent to each other. Moreover, according to Fornell and Larcker (1981), if the square root of the AVE is all higher than the correlations between constructs, then discriminant validity of all the constructs are guaranteed. The diagonal elements shown in Table 4 (reporting the square root of the variance shared between a construct and its measures) are higher than the correlations between the target constructs without exception. Hence, the discriminant validity of all of the constructs in this research are considered acceptable and both conditions for convergent validity are satisfied.

The results of the regression analyses on the adoption intention of BYOD are presented in Table 5. The R^2 of model one (just the control variables) and model two (including the main effects) were .131, and .368 respectively. The control variables had significant impacts on the adoption intention of security policy for BYOD. Our findings showed that males had a higher tendency to adopt security policy for BYOD ($\beta = .135^*$), it was also valid for young people ($\beta = -.175^{**}$), and for highly educated people ($\beta = .167^{**}$). It is reasonable to say young people are more confident in adopting BYOD than the mature ones. Moreover, educated people are likely to adopt BYOD. In terms of organization size, employees in large organizations are more willing to adopt BYOD ($\beta = .175^{**}$). It is properly because large organizations would have more resources and expertise in protecting intellectual property and their security policies are likely more comprehensive.

Table 5: Regression analyses on adoption intention of BYOD

	Model 1 Control Variables	Model 2 Main Effects
Control Variables		
Gender	$.148^*$	$.135^*$
Age	$-.192^{**}$	$-.175^{**}$
Education	$.187^{**}$	$.167^{**}$
Number of employees	$.182^{**}$	$.175^{**}$
Main Effects		
Perceived effectiveness of BYOD security policy (PE)		$.216^{**}$
Perceived cost of following BYOD security policy (PC)		.065
Self-efficacy of following BYOD security policy (SE)		$.187^{**}$
Perceived severity of negative consequence from adopting BYOD (PS)		$-.118^*$
Privacy protection of personal data (PP)		.035
Perceived usefulness (PU)		$.135^*$
Perceived ease of use (PEOU)		$.101^*$
Social Influence (SI)		$.126^*$
Job security (JS)		$.265^{***}$
Organizational commitment (OC)		$.237^{***}$
Model Information		
R^2	.131	.368
Change in R^2		.237

Our findings, as indicated in Table 5, showed that the PE, SE, PS, PU, PEOU, SI, JS and OC are significant factors to predict adoption intention of BYOD. Hence, H1, H3, H4, H6, H7, H8, H9 and H10 were supported. However, H2 and H5 were not supported. The R^2, being .368, was increased by .237, which was a big increment from the explained variance among the control variables. This indicated the variables PE, SE, PS, PU, PEOU, SI, JS and OC were all dominant factors to explain adoption intention. To compare their influence, JS and OC (β = .265*** and .237*** respectively) were of greater impact on adoption intention than that of PE, SE, PS, PU, PEOU and SI (β = .216**, .187**, -.118*, .135*, .101*, and .126* respectively). Perhaps it is because both job security and organization commitment have more important influence on an employee than the other factors. Hence, if employees think they are secure in their jobs and are committed to their organizations, they will adopt BYOD.

In terms of coping appraisal, perceived effectiveness of security policy for BYOD and self-efficacy were considered significant factors, while perceived cost of adopting security policy for BYOD was not. This would be because the perceived cost was not regarded as an essential concern. If an employee thinks he/she can adopt the security policy, which is effective, then he/she will adopt it. For threat appraisal, our findings showed that employees whose perceived severity of negative consequences would have negative impact on BYOD adoption (β = -.118*). However, they are not much worried on their personal data protection. Besides perceived usefulness (β = .135*) and perceived ease of use (β = .101*), employees will also be influenced by their friends and colleagues in BYOD adoption (β = .126*).

Implications on commercial practice

In this study, we conclude that coping appraisal in terms of perceived effectiveness, self-efficacy and threat appraisal in terms of perceived severity were significant factors to force employees to adopt BYOD. In addition, both organizational commitment and job security are also crucial to BYOD adoption intention. In practice, more and more organizations are promoting and allowing their employees to use their own devices to get the work done; more employees also start adopting this trend with the convenience of using their own devices. Because of that, effective security policy on avoiding information leaks and preventing unpredictable privacy thefts and its execution become essential. On the one hand, organizations must continue develop robust data protection and security software applications as information leaks could be costly and serious. On the other hand, organizations should enhance its BYOD security policy and to ensure easy execution according to the latest and safest technologies in the rising use of cloud computing. For instance, Basu, Sengupta and Mazumdar (2016) proposed to resolve the conflict of simultaneous access to the cloud using the Chinese Wall security policy (Brewer and Nash, 1989). Feng, Wu, Li, Wu, Chen and Tian (2016) attempted to assess the risk level of allied organization's information systems and support proactive security treatment. Curiac and Pachia (2015) introduced a procedure to destruct sensitive data that are no longer needed for the organization's future process. The scope of information removal covers all splinters spread throughout the cloud.

In order to encourage more employees to adopt BYOD at ease, an organization not only may consider running vigorous promotions and schemes to educate and train their employees on the benefits and safety of adopting BYOD, but also finding ways to gain employees' loyalty and commitment. Organizations may emphasize their allowing employees to BYOD because they are trust worthy staffs. When the employees' works are more productive and efficient because of doing BYOD, the company can become more successful and profitable and the employees' contributions should be awarded and recognized. There are many affordable measurements and incentive programs an organization can do to gain employees' commitments and to build a sense of job security. Once employees' loyalties are established, the employees would highly likely follow and support the company policy and engage in further BYOD deployment by all means.

In this study, we found that male, young, and higher educated employees are more willing to adopt BYOD than their counterparts. Hence, an organization could consider using these groups of employees as a pilot trial to plan for a successful full launch for BYOD.

Limitations and Conclusion

As of the case for all empirical researches, this investigation too has several limitations. A notable weakness lied in the cross-sectional research design, where all measurement items were collected at the same point in time from the employees' perspectives. Given that the investigated constructs could change over time, this research method might not fully capture the dynamics of adoption intention of BYOD. This constraint could lead same-source bias and inaccuracy, which fortunately is not a serious concern as confirmed in our analysis. To address the above issues, future research should consider employing multi-methods and longitudinal research designs. A longitudinal study combining qualitative and quantitative data would enable a process-oriented perspective that cannot be achieved by using a variance-based approach, such as the one employed here.

Furthermore, security policy in general is a valid concern for senior management; however, only employees' perspectives were collected and examined in this study. Hence, future research should also consider collecting inputs from senior management.

Effective management and coping with the BYOD security policy can enable an employee's work flexibility and efficiency. One way to reduce security risk is to learn to expect the unexpected. Be prepared for the incidents you planned for, but also for the ones you don't. Always have backup as contingency plans and alternative solution are no doubt good ideas. Many employees waste so much time stressing about things that may go wrong, things that are not expected; instead of utilize the time on a wisely and constructive way to come up with solution and options.

In general, employees who are limited to work within their cubicles are rather isolated. Bring your own device (BYOD) allows employees to use their own notebooks and mobile devices to conduct their work. This approach gives flexibility to mobile workers who need to interact with clients and complete tasks outside their offices and office hours. Many businesses rely on short turnaround times and seamless interaction. BYOD allows employees to be more productive regardless of when and where. Whether they are travelling, on vacation, on sick leave or just out to lunch, employees can stay connected and remain productive. Not only do they feel a sense of empowerment on the devices they can choose to use to perform their duties best, but also the freedom on when and where they do their jobs.

We argue that mobile devices, which become more and more popular, facilitate people to communicate at anytime and anywhere. From time to time, this is also true and applicable to work life. Our findings have shown that BYOD adoption is mainly affected by threat and coping appraisal; while organization commitment and job security are also essential supporting factors. Similar to other studies in technology adoption, perceived usefulness, perceived ease of use, social influence are also found significant.

Reference

Aaron, F., Guo, C., and Shim, J.P. (2014). Current status, issues, and future of bring your own device. *Communication of the Association for Information Systems*. 35, 191 – 205.

Ajzen, I. (1985). From intentions to actions: a theory of planned behavior. In: J. Kuhl & J. Beckman, Editors, *Action-Control: From Cognition to Behavior*, Springer-Verlag, 11–39.

Angle, H.L. and Perry, J.L. (1981). An empirical assessment of organizational commitment and organizational effectiveness. *Administrative Science Quarterly*, 26, 1, 1 – 14.

Ansaldi, H. (2013). Addressing the challenges of the "bring your own device" opportunity. *The CPA Journal*, 83, 11, 63 – 65.

Armando, A., Costa, G., Merlo, A., and Verderame, L. (2014). Formal modelling and automatic enforcement of bring your own device policies. *International Journal of Information Security*, 14, 2, 123 – 140.

Ashford, S.J., Lee, C. and Bobko, P. (1989). Content, causes and consequences of job insecurity: a theory-based measure and substantive test. *Academy of Management Journal,* 32, 4, 803 – 829.

Ajzen, I. and Fishbein, M. (1980) *Understanding Attitudes and Predicting Social Behaviour*, NJ: Prentice-Hall.

Bandura, A. (1977). Self-efficacy: towards a unifying theory of behavioral change. *Psychological Review* 84, 2, 191 – 215.

Basu, S., Sengupta, A. and Mazumdar, C. (2016). Modelling operations and security of cloud systems using Z-notation and Chinese Wall security policy. *Enterprise Information Systems*, 10, 9, 1024 – 1046.

Bhuian, S.N. and Islam, M.S. (1996). Continuance commitment and extrinsic job satisfaction among a novel multiculture expatriate work force. *Mid-Atlantic Journal of Business,* 32, 1, 35 – 46.

Blau, G.J. and Boal, K.B. (1987). Conceptualizing how job involvement and organizational commitment affect turnover and absenteeism. *The Academy of Management Review*, 12, 2, 288 – 300.

Brewer, D.F.C., and Nash, M.J. (1989). The Chinese Wall Security Policy. *IEEE Symposium on Security and Privacy*, Oakland, CA, May 1–3, 206–214.

Buchanan, T., Paine, C., Joinson, A.N. and Peips, U.D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58, 2, 157 – 165.

Coates, S. (2014). BYOD business issues: Auditors need to ensure their organization has a map in place for connecting personal devices to corporate networks and data. *Internal Auditor*, 71(1), 21(2).

Crossler, R.E., Long, J.H., Loraas, T.M. and Trinkle, B.S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: bridging the intention behaviour gap. *Journal of Information Systems*, 28, 1, 209 – 226.

Curiac, D. and Pachia, M. (2015). Controlled information destruction: the final frontier in preserving information security for every organization. *Enterprise Information Systems*, 9, 4, 384 – 400.

CXO Unplugged (2012). *BYOD research findings*. http://cxounplugged.com/2012/11/ovum_byod_research-findings-released/

Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340

Davis, T. (2013). Device independence is the future of clinical trials. *Applied Clinical Trials*, 22, 11, 34 – 35.

De Cuyper, N., Notelaer, G., and de Witte, H. (2009). Job insecurity and employability in fixed-term contractors, agency workers, and permanent workers: associations with job satisfaction and affective organisational commitment. *Journal of Occupational Health Psychology*, 14, 2, 193 – 205.

De Witte, H. (1999). Job insecurity and psychological well-being: review of the literature and exploration of some unresolved issues. *European Journal of Work and Organizational Psychology*, 8, 2, 155 – 177.

Faulds, M. C. ; Bauchmuller, K. ; Miller, D. ; Rosser, J. H. ; Shuker, K. ; Wrench, I. ; Wilson, P. ; Mills, G. H. (2016). The feasibility of using ‘bring your own device’ (BYOD) technology for electronic data capture in multicentre medical audit and research. *Anaesthesia*, 71, 1, 58 – 66.

Feng, N., Wu, H., Li, M., Wu, D., Chen, F. and Tian, J. (2016). Managing security risks for inter-organisational information systems: a multiagent collaborative model. *Enterprise Information Systems*, 10, 7, 751 – 770.

Fornell, G., Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18, 39 – 50.

Garba, A.B., Armarego, J., Murray, D., Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device environments. *Journal of Information Privacy and Security*, 11(1), 38-54.

Godin, I., and Kittel, F. (2004). Differential economic stability and psychosocial stress at work: associations with psychosomatic complaints and absenteeism. *Social Science & Medicine*, 58, 1543 – 1553.

Holleran, J. (2014). Building a better BYOD strategy. *Risk Management*, 61, 7, 12 – 13.

Information Security Forum. (2000). *Information Security Culture – A preliminary investigation*, s.l.

Jansen, W., and Grance, T. (2012). *Guidelines on security and privacy in public cloud computing*. National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication, 800-144.

Kalleberg, A. L., and Rognes, J. (2000). Employment relations in Norway: Some dimensions and correlates. *Journal of Organizational Behavior*, 21, 315–335.

Kobus, M.B.W., Rietveld, P., and van Ommeren, J.N. (2013). Ownership versus on-campus use of mobile IT devices by university students. *Computer & Education*, 68, 29 – 41.

Leach, J. (2003). Improving user security behavior. *Computers & Security*, 22, 8, 685 – 692.

Leclercq - Vandelannoitte A., (2015), Managing BYOD: How do organizations incorporate user-driven IT innovations? *Information Technology & People*, 28, 1, 2 – 33.

Lee, Y. and Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18, 2, 177 – 187.

Liagouras, G.A., Sayegh, A.A. and Koutsakis, P. (2014). A new location-aware calendar-based application for dynamic minimum path trip planning. *Wireless Personal Communications*, 78, 29 – 44.

Liang, H. and Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective, *MIS Quarterly*, 2009, 33, 1, 71 – 90.

Liang, H. and Xue, Y. (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective, *Journal of the Association for Information Systems*, 11, 7, 394 – 413.

Marshall, S. (2014). IT consumerization: A case study of BYOD in a healthcare setting. *Technology Innovation Management Review*, 4(3), 14-18.

McDonald, D.J., and Makin, P.J. (2000). The psychological contract, organizational commitment and job satisfaction of temporary staff. *Leadership and Organizational Development Journal*, 21, 84 –91.

McLean Parks, J., Kidder, D. L., & Gallagher, D. G. (1998). Fitting square pegs into round holes: Mapping the domain of contingent work arrangements onto the psychological contract. *Journal of Organizational Behavior*, 19, 697–730.

Mitrea, D. (2014). Impact of mobile application on smartphones for European employees. *Bulletin of the Translivania University of Brasov. Economic Sciences*, 7, 2, 31 – 38.

Podsakoff, P.M., Organ, D.W. (1986). Self-reports in organizational research: problems and prospects. *Journal of Management*, 12 (4), 531 – 544.

Rose, C. (2013). BYOD: an examination of bring your own device in business. *The Review of Business Information Systems*, 17, 2, 65 – 69.

Sangani, K., (2013). BYOD to the classroom. *Engineering & Technology*, 8, 3, 42 – 45.

Siegel, S., Castellan, N.J. (1988). *Nonparametric statistics for the behavioral sciences* 2nd edition, New York: McGraw-Hill.

Song, Y., (2014). "Bring Your Own Device (BYOD)" for seamless science inquiry in a primary school. *Computers & Education*, 74, 50 – 60.

Sverke, M., Hellgren, J. and Naswall, K. (2002). No security: a meta-analysis and review of job insecurity and its consequences. *Journal of Occupational Health Psychology*, 7, 3, 242 – 264.

Taylor, S. and Todd, P. (2006). Understanding the determinants of consumer composting behavior. *Journal of Applied Social Psychology*, 27, 7, 602 – 628.

Tomislav, C., Ljubica, P., and Mislav, S. (2014). Mobile technologies and supply chain management – lessons for the hospitality industry. *Tourism and Hospitality Management*, 20, 2, 207 – 219.

Tu, Z. and Yuan, Y. (2012) Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft. *Proceedings of the 45th Hawaii International Conference on System Sciences*, 1393 – 1402.

Van Gyes, G. and Szekér, L. (2013), *Impact of the Crisis on European Working Conditions: Assembling National Trends and Reports*, Eurofound, Dublin.

Van Quaquebeke, N. Zenker, S. and Eckloff, T. (2008). Find out how much it means to me! The importance of interpersonal respect in work values compared with perceived organizational practices. *Journal of Business Ethics*, 89, 423 – 431.

Venkatesh, V. and Davis, F.D. (2000) "A Theoretical Extension of the Technology Adoption Model: Four Longitudinal Field Studies," *Management Science*, (46), pp.186-204.

Watts, S. (2014). Intelligent combination – the benefits of tokenless two-factor authentication. *Network Security*, 8, 17 – 20.

Weeger, A., Wang, X., and Gewald, H. (2015). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems*, 56, 1, 1 – 10.

Workman, M., Bommer, W.H., and Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, 24, 18, 2799 – 2816.

Yousef, D., (1998). Satisfaction with job security as a predictor of organizational commitment and job performance in a multicultural environment. *International Journal of Manpower*, 19, 3, 184 – 194.