Bring Your Own Device (BYOD) Security Policy Compliance Framework

Research-in-Progress

Rathika Palanisamy **Azah Anir Norman**

Miss Laiha Mat Kiah

Abstract

Bring Your Own Device (BYOD) is an environment that allows employees to use their own personal device to access organisation's resources to perform their work, but it has raised some security concerns as with BYOD, organisations face bigger challenges to safeguard their information assets. Compliance with ISP is a key factor in reducing organisation's information security risks, as such, understanding employees' compliance behaviour and other relevant factors that influence compliance with ISP is crucial. Hence, this study aims to explore this phenomenon by investigating the factors influencing employees in complying with BYOD Information Security Policy (ISP) in Malaysian public sector. A mixed method study on five (5) ministries in the public sector is proposed for the study. The understanding of these factors would assist in systematically developing a BYOD compliance framework for the public sector. This is critical as this trend is here to stay or even expand rapidly as employees carry more than one device to the workplace. The proposed framework will help improve ISP compliance to ensure organisational information assets are well protected.

Keywords: Bring Your Own Device, BYOD, Information Security Policy, Compliance, Social Cognitive Theory

Introduction

The significance of BYOD has increased exponentially in recent years due to the expansion of mobile device consumerisation. This movement has become a standard practice as more mobile devices are being used in the workplace by most employees ranging from the top management, executives right to the supporting staffs. The BYOD trend is inevitable as today, government agencies are tasked to cut costs, increase transparencies, employees are required to work and respond anytime, anywhere and this practice is considered as an important strategy to improve service delivery to the citizens.

On a positive note, with BYOD, employees are able to perform their tasks with the comfort of their own devices leading to an increase in productivity and boost their morale. Though BYOD practice promises lots of benefits to those who embrace them, there is a range of security risks such as device

loss, data contamination and data leakage that can detriment organisations financially and tarnish their reputation.

A recent industry survey by Fortinet (2018) has revealed that about 65 percent of organisations are now allowing personal devices to connect to corporate networks, with 95 percent of CIOs stating concern over emails being stored on personal devices, and 94 percent being worried about organisational information stored in mobile applications. While there may be similarities in security settings for traditional and BYOD, security concerns are much more amplified with BYOD. In a traditional corporate scenario, the organisation had complete security control over the assets and if a security attack happens; the suspect would be most likely to originate from an outsider unlike in the BYOD environment, the attacks can possible be from the trusted insider. With BYOD, the confidential organisational information resides in personal devices that moves around on a daily basis and lies at risk of loss or theft (Miller et al. 2012). Additionally, there are also concerns about the traversal of data from various environments and employees having multiple devices assessing the corporate network (Thomson 2012).

Problem Background

Employee's strong dependence on technologies with the rapid expansion of powerful devices and explosive growth of social media has brought new work behaviours that may jeopardise the organisation's information security landscape. Though most organisations implement security policies to help prevent against BYOD security risks, in reality this is often ignored by employees (Timms 2017). A study from Kaspersky (2018) found that only one in ten employees is aware of the security policy in the organisation. Security policies are far less likely to be enforced on devices that are not owned by the organisation (Miller et al. 2012), neither would the employee be obliged to comply to the policy as their freedom of using their own device is being threatened (Hovav and Putri 2016). Employees may perceive the security policy as a hindrance; which will be most likely be overlooked leading to exposure of IT systems to various risks and other implications. In the BYOD environment, the users are required to play an active role in protecting valuable assets of the organisation (e.g. locking device, password management, cautious use of email and Internet, being tactful when handling organisational assets and information out of organisation and reporting security breaches) (Zahadat et al. 2015). Adherence to security policy is critical in a BYOD environment because employees' activities on their devices has a tremendous impact on the organisation's performance (Staglianos et al. 2013).

Prior studies in this particular area are limited to using traditional PMT and TPB as the underlying psychological process that motivates users to comply with BYOD ISP (Crossler et al. 2014; Dang-Pham and Pittayachawan 2015; Hovav and Putri 2016; Thompson et al. 2017; Tu et al. 2018). Balozian and Leidner (2017) suggested that future studies should incorporate other theories from psychology and management besides PMT and GDT. Besides, most of these early studies used students as their sample data, which may not represent the employee in the BYOD environment. Tu et al. (2019) also recommended that future study should be extended to other countries as individuals with different cultures may have different perceptions and thus different motivations. Previous research has not looked into influence of environment, social elements and the mandoriness of the security policy in shaping an employees' behaviour in a BYOD environment. Therefore, it is valuable to study factors influencing compliance from various perspectives and provide understanding of the issues. Below are the research objective (RO) and questions (RQ) that this research seeks to answer;

RO1: To identify factors that influence BYOD security policy compliance behaviour among employees.

RQ1a: What are the factors that influence BYOD security policy compliance?

RQ1b: How do the identified factors improve employees' compliance behaviour towards BYOD security policy?

The remaining of the paper is structured to discuss on the theoretical perspective, conceptual framework formation, research design, potentials and implications.

Theoretical Background

Social Cognitive Theory (SCT) posits that individual behaviour is part of a triadic structure in which behaviour, personal factors and environmental factors constantly influence each other, mutually determining each other (Bandura 1989; Carillo 2010). This theory explains that the interaction between the employee and their behaviour is influenced by their thoughts and actions. Similarly, the interaction between the employee and their environment involves cognitive competencies and beliefs influenced by their environment. The interaction between their environment and behaviour involves the employee's behaviour determining the environment and vice versa.

The second theory chosen is Organisational Control Theory (OCT), derived from the study of Boss et al.(2009). This theory uses the concept of mandatory controls, where participation towards compliance is not optional. This is very similar set up in the public sector, as security policy and guidelines are mandates from the central agencies that are supposed to be compulsory and adhered to by the employees. OCT is appropriate for this context as it explains whether the perception of mandatoriness affects compliance behaviour. In this current research, controls of international standard ISO27001/2013 relevant to BYOD; 'Mobile Devices' and 'Teleworking' (Hajdarevic et al. 2017) will be used to measure the construct of employee security policy compliant behaviour.

Finally, the research model includes Security Culture, as it addresses the call to include the presence of security culture (Boss et al. 2009) to effectively understand the effects of control on security policy compliance. Research has shown that security culture is an important factor in increasing compliant behaviour (Stanton et al. 2005).

As such, the conceptual model is designed based on factors gathered from review of literature by integrating Compeau (2013), Boss et al., (2009), D'Arcy and Greene (2009) using SCT and Control Theory to examine its influence on the employee BYOD security policy compliance behaviour which will be based on ISO27001/2013. The conceptual research model is depicted in Figure 1.

Social Cognitive Theory

Variables adopted in this study are from Compeau and Higgins (1995) and Galvez et al. (2015). Among those are self-efficacy, which plays an important role in SCT whereby when a person believes that his/her capability to use certain system influences his/her performance (Carillo 2010) and predicted that self-efficacy will influence individuals' actual ability to perform the behaviour (Bandura 1977; Workman et al. 2008). This prediction is consistent with Protection Motivation Theory studies (Herath and Rao 2009; Ifinedo 2012; Pahnila et al. 2007) which also found that complying security policies have been influenced by self-efficacy. Additionally, people with higher self-efficacy in the use of technology tend to use the technology more than those with lower self-efficacy (Compeau and Higgins 1995). There is a call to study the relationship between self-efficacy and compliance as research has produced contradicting results (Hovav and Putri 2016). SCT also posits that self-efficacy influences an individual's outcome expectations (Bandura 1978). Therefore:

> **H1a:** Employees' self-efficacy in information security (SEIS) is positively associated with employees' outcome expectations in information security.
>
> **H1b:** Employees' self-efficacy in information security (SEIS) is positively associated with employee BYOD security policy compliance behaviour.

The encouragement of others is when an individual look to find guidance on behavioural expectations and might influence both self-efficacy and outcome expectations (Compeau and Higgins 1995). In this study, it is expected that encouragement from peers and superiors may influence self-efficacy and outcome expectation in information security and hence contribute to BYOD security compliance behaviour.

H2a: The higher the encouragements by others in the use of information security tools, the higher the employees' self-efficacy in information security (SEIS).

H2b: The higher the encouragements by others in the use of information security tools, the higher the employees' outcome expectations in information security

SCT posits that instrumental support as one of the factors that positively influence self-efficacy (Compeau and Higgins 1995; Galvez et al. 2015). In the Compeau and Higgins (1995) study, when organisations give computer support to individuals who need it, it enhances their ability and their perception of their ability to perform a specific task. In this context, the availability of Information Technology (IT) support team to deal with technical issues related to employees' personal devices may influence self-efficacy and outcome expectations and thus contribute to their compliance behaviour. IT support is a norm in a traditional environment where the resources are fully owned by the organisation, the same may not be applicable in a BYOD environment (Hovav and Putri 2016).

H3a: The higher the instrumental support for information security in the organisation, the higher the employees' outcome expectations in information security.

H3b: The higher the instrumental support to employees for information security in the organisation, the higher the employees' self-efficacy in information security (SEIS).

According to Bandura (1977), individuals learn new information and behaviour by watching other individuals. Similarly, Compeau & Higgins, (1995) stated that the use of technology by others can be applied in forming self-efficacy. In the context of this study, it is expected that when peers and superiors practice information security behaviour, it may influence self-efficacy and outcome expectations.

H4a: The higher the Information Security Practices by others in one's reference group, the higher the employees' outcome expectations in information security.
H4b: The more frequent the Information Security Practices by others in one's reference group is, the higher the employees' Self-efficacy in information security (SEIS) will become.

An outcome expectation is an important construct that is used to explain and predict human behaviour. Hence, it motivates one to perform behaviour over time if they believe their actions will produce wanted results (Galvez et al. 2015).

H5: Employees' outcome expectations in information security are positively associated with employees' BYOD security policy compliance behaviour.

Organisational Control Theory

Boss et al., (2009) in their study defined mandatoriness as the "degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organisational management".

H6: The higher the employees' perceived mandatoriness of compliance with existing security policies and procedures, the higher employee BYOD security policy compliance behaviour

In order to practice control, the specification of desired behaviour should be documented as part of procedures (Eisenhardt 1985; Kirsch 2004). Understandable policies give clear direction to the employees to achieve the desired behaviour. This study will include this as the specification of security policy may be seen as mandatory by employees.

H7: The higher the specification of security policy is, the higher the perceived mandatoriness in information security will be.

Evaluation is important to assess an individual's compliance with specific behaviour or outcomes (Kirsch 2004). Boss et al., (2009) stated that employees will ignore or overlook policies if management fails to evaluate policies.

> **H8:** The higher the employees' evaluation of security policy, the higher the perceived mandatoriness of compliance with existing security policies and procedures.

Security Culture

Security Culture is able to minimise the risks to IT assets as well as employees' interactions with the assets whether intentional or unintentional (Hina and Dominic 2018). Security culture is a multi-dimensional concept whereby it comprises three main concepts which are top management support, security communication and computer monitoring (Greene and D'Arcy 2010).

> **H9:** Security culture is positively associated with BYOD security compliance behaviour.

BYOD Awareness

BYOD awareness is crucial to alert the employees on the cyber threats that lurk within the mobile devices. Besides, a recent study showed that there is a lack of awareness among smartphone users about the security and privacy risks associated with downloading smartphone apps (Mylonas et al. 2013). Hovav and Putri (2016) raised a question whether there is a relationship between security training and awareness and self-efficacy which brings to the next two hypotheses;

> **H10:** BYOD security awareness program is positively associated with self-efficacy of information security.

Technical Skills Training

Technical skills training is included as an antecedent to the construct of self- efficacy as by empowering the employees with adequate technical skills it improves self-efficacy and hence, enable employees to adhere to BYOD ISP and procedures. These skills are also essential in training the employees to be alert of threats and also being able to mitigate the threats. It is needed to foster the necessary knowledge and skills for employees to successfully protect information assets (Furnell and Thomson 2009). Besides, many organisations are concerned about their own limited resources and lack of capabilities and expertise. IT departments fear the thought of supporting the entire universe of possible devices (Cisco Systems 2012).

H11: Technical skill training is positively associated with employees' BYOD security policy compliance behaviour.

Conceptual Research Framework of the Factors Influencing BYOD Security Policy Compliance

Figure 1 depicts plausible factors that may influence employee adherence towards the BYOD security policy from the analysis of literature. This conceptual framework shows factors from various aspects which serve as a fundamental idea and knowledge acquired of the current study. Table 1 provides brief summary of the constructs and related theories considered in this study.

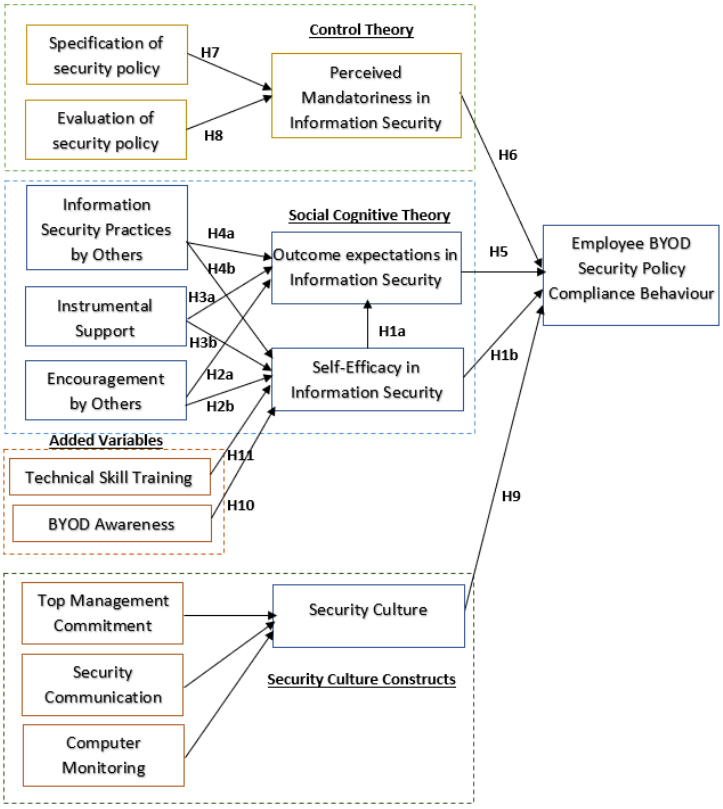

Figure 1. Conceptual Research Framework

Table 1. Main Constructs and Related Theories

Theory	**Construct Name**	**Adapted From**
Social Cognitive Theory (SCT)	Self-Efficacy in Information Security	(Compeau and Higgins 1995; Galvez et al. 2015)
	Outcome expectations in Information Security	(Compeau and Higgins 1995; Galvez et al. 2015)
	Encouragement by Others	(Compeau and Higgins 1995; Galvez et al. 2015)
	Information Security Practices by Others	(Compeau and Higgins 1995; Galvez et al. 2015)
	Instrumental Support	(Compeau and Higgins 1995; Galvez et al. 2015; Hovav and Putri 2016)
Control Theory	Perceived Mandatoriness in Information Security	(Boss et al. 2009)
	Specification of security policy	(Boss et al. 2009)
	Evaluation of security policy	(Boss et al. 2009)
Security Culture	Top Management Commitment	(Greene and D'Arcy 2010)
	Security Communication	(Greene and D'Arcy 2010)
	Computer Monitoring	(Greene and D'Arcy 2010)
-	Technical Skill Training	Added Variable
	BYOD Awareness	(Putri and Hovav 2014)

Proposed Research Design

This study will adopt a mixed method research approach. Table 2 shows the proposed research design which intends to answer the rest of research questions.

Table 2. Research Design

Phases	Research Process	Method	Activity	Expected Outcome
Phase 1 Background Study (RQ1a)	Contextual definition Review of literature	-	• Seek definition • Understand concept • Gather plausible factors	• Conceptual Research Framework
Phase 2 Empirical Study (RQ1a)	Data Collection Data Analysis	Expert Interview	• To interview at least 5 senior managers.	• BYOD Risk Factors • Compliance Factors Identification and Verification
Phase 3 Empirical Study (RQ1b)	Data Collection Data Analysis	Survey	• To conduct online / face to face survey to 350 employees.	• BYOD Security Policy Compliance Factors Relationship • Proposed BYOD Security Policy Compliance Framework
Phase 4 Development and Findings Validation	Final Result	Focus Group Discussion	• To validate findings by at least 5 experts • To propose framework for the public sector	• Validated BYOD Security Policy Compliance Framework

Potential Academic and Practical Implications

This research offers several contributions to the literature. Firstly, it studies an area that is under-researched; which is the behavioural study in a BYOD environment. Acknowledging the fact that there are risks surrounding the BYOD practice, findings of this research is both important and timely. Second, security is studied from the management perspective, different from previous research of BYOD which is from a technical perspective. This study will develop a theoretical model to identify factors affecting employees' compliance with organisation's BYOD security policies, which is still scarce. It extends and enriches the SCT and OCT to new contexts of BYOD security policy compliance, besides offering a new insight into a different security culture. It extends the study of compliance behaviour in a BYOD context away from the traditional PMT.

The findings will be beneficial to organisations which practise BYOD or planning to embark on one. BYOD trend is inevitable and it is no longer an option. The findings will provide a better understanding on employee work behaviour in adherence to BYOD ISP. It is even more crucial now that employees carry more than one mobile device with them for both work and personal usage. The research findings will strengthen the most important pillar of an organisation which is the 'People' by assisting policy makers to craft BYOD security policies and programs that will be most likely be adhered by the employees leading to a better protection of organisational information assets.

Acknowledgement

We would like to express gratitude to the Public Service Department of Malaysia for the sponsorship of this study under the Federal Training Award. We sincerely appreciate the valuable and constructive comments by the reviewers in helping us to improve this paper.

References

Balozian, P., and Leidner, D. 2017. "Review of IS Security Policy Compliance," *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* (48:3), pp. 11–43. (https://doi.org/10.1145/3130515.3130518).

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84:2), pp. 191–215. (https://doi.org/10.1037/0033-295X.84.2.191).

Bandura, A. 1978. "Reflections on Self-Efficacy," *Advances in Behaviour Research and Therapy* (1:4), pp. 237–269. (https://doi.org/10.1016/0146-6402(78)90012-7).

Bandura, A. 1989. "Social Cognitive Theory," in *Annals of Child Development.* (Vol. 6), R. Vasta (ed.), Greenwich, CT: JAI Press, pp. 1–60. (https://doi.org/10.1111/1467-839X.00024).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151–164. (https://doi.org/10.1057/ejis.2009.8).

Carillo, K. D. A. 2010. "Social Cognitive Theory in IS Research – Literature Review, Criticism, and Research Agenda," *Communications in Computer and Information Science* (March). (https://doi.org/10.1007/978-3-642-29166-1).

Cisco Systems. 2012. "BYOD In Government: Prepare For The Rising Tide," *Forrester Consulting* (10), pp. 1–13. (http://www.cisco.com/web/strategy/docs/gov/cisco_forrester_byod_government.pdf).

Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), p. 189. (https://doi.org/10.2307/249688).

Compeau, R. 2013. *Application of Social Cognitive Theory to Training for Computer Skills Author (s): Deborah R . Compeau and Christopher A . Higgins Published by : INFORMS Stable URL : Http://Www.Jstor.Org/Stable/23011006 . Application of Social Cognitive Training for Co*, (6:2), pp. 118–143.

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-Behavior Gap," *Journal of Information Systems* (28:1), pp. 209–226. (https://doi.org/10.2308/isys-50704).

D'Arcy, J., and Greene, G. 2009. "The Multifaceted Nature of Security Culture and Its Influence on End User Behavior," *IFIP TC 8 International Workshop on Information Systems Security Research* (2005), pp. 145–157.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98. (https://doi.org/10.1287/isre.1070.0160).

Dang-Pham, D., and Pittayachawan, S. 2015. "Comparing Intention to Avoid Malware across Contexts in a BYOD-Enabled Australian University: A Protection Motivation Theory Approach," *Computers and Security* (48), Elsevier Ltd, pp. 281–297. (https://doi.org/10.1016/j.cose.2014.11.002).

Eisenhardt, K. M. 1985. *Control: Organizational and Economic Approaches*, (31:2), pp. 134–149.

Furnell, S., and Thomson, K. L. 2009. "From Culture to Disobedience: Recognising the Varying User

Acceptance of IT Security," *Computer Fraud and Security* (2009:2), pp. 5–10. (https://doi.org/10.1016/S1361-3723(09)70019-3).

Galvez, S. M., Shackman, J. D., Guzman, I. R., and Ho, S. M. 2015. "Factors Affecting Individual Information Security Practices," *SIGMIS-CPR'15, June* (26:8), pp. 555–557. (https://doi.org/10.1145/2751957.2751966).

Greene, G., and D'Arcy, J. 2010. "Assessing the Impact of Security Culture and the Emplyee-Organization Relationship in IS Security Compliance," *5th Annual Symposium on Information Assurance (ASIA ' 10)*, pp. 42–49. (https://doi.org/10.1108/IMCS-08-2013-0057).

Hajdarevic, K., Allen, P., and Spremic, M. 2017. "Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments," *24th Telecommunications Forum, TELFOR 2016*. (https://doi.org/10.1109/TELFOR.2016.7818717).

Herath, T., and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), Elsevier B.V., pp. 154–165. (https://doi.org/10.1016/j.dss.2009.02.005).

Hina, S., and Dominic, P. D. D. 2018. "Information Security Policies ' Compliance : A Perspective for Higher Education Institutions," *Journal of Computer Information Systems* (00:00), Taylor & Francis, pp. 1–11. (https://doi.org/10.1080/08874417.2018.1432996).

Hovav, A., and Putri, F. F. 2016. "This Is My Device! Why Should I Follow Your Rules? Employees' Compliance with BYOD Security Policy," *Pervasive and Mobile Computing* (32), Elsevier B.V., pp. 35–49. (https://doi.org/10.1016/j.pmcj.2016.06.007).

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers and Security* (31:1), Elsevier Ltd, pp. 83–95. (https://doi.org/10.1016/j.cose.2011.10.007).

Kaspersky. 2018. "Kaspersky Lab Survey: One-in-Ten Employees Are Aware of Their Organization's IT Security Policies."

Kirsch, L. J. 2004. "Deploying Common Systems Globally: The Dynamics of Control," *Information Systems Research* (15:4), pp. 374–395. (https://doi.org/10.1287/isre.l040.0036).

Miller, K. W., Voas, J., and Hurlburt, G. F. 2012. "BYOD: Security and Privacy Considerations," *IT Professional* (14:5), pp. 53–55. (https://doi.org/10.1109/MITP.2012.93).

Mylonas, A., Kastania, A., and Gritzalis, D. 2013. "Delegate the Smartphone User? Security Awareness in Smartphone Platforms," *Computers and Security* (34), pp. 47–66. (https://doi.org/10.1016/j.cose.2012.11.004).

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 1–10. (https://doi.org/10.1109/HICSS.2007.206).

Putri, F., and Hovav, A. 2014. "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," *Ecis*, pp. 1–17. (https://doi.org/10.1109/ISCAIE.2014.7010235).

Staglianos, T., Dipoalo, A., and Coonelly, P. 2013. *Consumerization of IT The Consumerization of Information Technology Prepared By : Tom Stagliano Anthony DiPoalo*.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers and Security* (24:2), pp. 124–133. (https://doi.org/10.1016/j.cose.2004.07.001).

Thompson, N., McGill, T. J., and Wang, X. 2017. "'Security Begins at Home': Determinants of Home Computer and Mobile Device Security Behavior," *Computers and Security* (70), Elsevier Ltd, pp. 376–391. (https://doi.org/10.1016/j.cose.2017.07.003).

Thomson, G. 2012. "BYOD: Enabling the Chaos," *Network Security* (2012:2), Elsevier Ltd, pp. 5–8.

(https://doi.org/10.1016/S1353-4858(12)70013-2).

Timms, K. 2017. "BYOD Must Be Met with a Wider Appreciation of the Cyber-Security Threat," *Computer Fraud and Security* (2017:7), Elsevier Ltd, pp. 5–8. (https://doi.org/10.1016/S1361-3723(17)30058-1).

Tu, C. Z., Adkins, J., and Zhao, G. Y. 2019. "Complying with BYOD Security Policies : A Moderation Model Based on Protection Motivation Theory," *Journal of the Midwest Association for Information Systems* (2019:1), pp. 11–28. (https://doi.org/10.17705/3jmwa.000045).

Tu, C. Z., Adkins, J., Zhao, G. Y., Tu, C. Z., Adkins, J., and Zhao, G. Y. 2018. *Complying with BYOD Security Policies : A Moderation Model A Moderation Model*.

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* (24:6), pp. 2799–2816. (https://doi.org/10.1016/j.chb.2008.04.005).

Zahadat, N., Blessner, P., Blackburn, T., and Olson, B. A. 2015. "BYOD Security Engineering: A Framework and Its Analysis," *Computers and Security* (55), Elsevier Ltd, pp. 81–99. (https://doi.org/10.1016/j.cose.2015.06.011).