User's Information Security Awareness in BYOD Programs: A Theoretical Model

Bo Han
College of Business, Texas A&M University-Commerce
bo.han@tamuc.edu

Abstract

We propose a new theoretical model to investigate the user's information security awareness in bring-your-own-device (BYOD) programs. This model is built on the protection motivation theory and general deterrence theory. In addition, it has a discussion on the influence of a user's cyber security inertia, a personal security management procrastination tendency, on the user's security awareness of organization information resources. This model can provide a useful guideline for a BYOD security management.

Introduction

The "Bring-Your-Own-Device" (BYOD) program has become a very popular information system management practice in recent years (Business Wire, 2015; E&Y, 2013). It is reported that more than half of the companies in North America and Europe have already adopted or plan to develop BYOD programs (Forrester Research, 2016). Over 340 million smart devices worldwide are currently participating in BYOD programs (I-CIO, 2013). Over 65% of smartphone users in the U.S. use their smart devices as "mobile offices" for work (Han et al., 2014). An International Data Corporation's study predicts that the population of mobile technology supported workers may surpass 105 million in the U.S. by 2020 (Business Wire, 2015). The time users spend on smart devices for work increases significantly in BYOD. A study shows that users who are given BYOD access may check their smartphones for work emails 20 times a day on average (Telegraph, 2012). Some BYOD users spend up to 3 hours making work phone calls or sending work emails on their smart devices during the after-work hours (Telegraph, 2012). Even though BYOD programs are broadly and intensively used, a user's information security awareness in such programs has not been well studied. In this study, we propose a theoretical model to investigate the influential factors of a user's information security awareness when participating in a BYOD program.

Literature Review

A BYOD program is an information systems (IS) management practice, in which an organization authorizes its members to use personal devices to access, process, and store work related data (French et al., 2014). This new model introduces two new concepts, including the IS openness and the IS autonomy, to organizational IS management. The IS openness refers to the exposure of an organization's IS infrastructures to a user's personal devices. A typical example of the IS openness is that users can not only receive and send emails in a BYOD program, but will also be given the email system's configurations such as the server domain, server type, and port number, so that they can set up email apps on their own smart devices (Digital Guradian, 2016). The IS openness increases a user's mobility in information management, but it also creates vulnerabilities in the organization's information systems (ITLP, 2012). If a cyber-attack were initiated, hackers would not directly attack the organization's web servers, which are usually equipped with more comprehensive security countermeasures. Instead, they would choose a BYOD user's poorly protected smart devices as agents to bypass the web servers' defense, and carry out attacks inside of the organization's intranet (TrendMicro, 2012). Thus, the IS openness introduced by BYOD requires

users to take great responsibilities in helping IS managers to detect and prevent threats to the organization's information security (Crossler et al., 2014, Morrow, 2012).

The IS autonomy is another bold movement that BYOD initiated in modern IS management. The IS autonomy refers to the authority given to users, in order to enable them to use and manage information and systems in their preferred ways (Harris et al., 2012; Harris et al., 2014). Before the emergence of BYOD, the centralized IS governance model was prevalent among organizations (Herath and Rao, 2009, Johnston et al., 2015; Warkentin and Willison, 2009). This model requires users to comply with organizational policies, and use information systems as directed. Typical security management practices of a centralized IS governance model include: All users must install the same anti-virus software onto their office desktops as instructed by the IS department. All users must follow the same principles (e.g., using a mix of numbers, texts, and special symbols) to set up their passwords, etc. In a BYOD program, when an organization increases its IS openness, it basically gives users a large degree of control over how to protect organizational IS resources on their personal devices (Harris et al., 2012; Weeger et al., 2015). For instance, users are able to choose their preferred security apps to protect the information stored on their smartphones in a BYOD program. Users can also decide how to set up passwords to protect their devices, or even not to set up a password at all. The IS autonomy increases the user's flexibility in information management; however, users have long been identified as "the weakest link" in an organization's security chain (Bulgurcu et al., 2010, Warkentin and Willison, 2009; Workman et al., 2008). Only if users establish good information security awareness, and are willing to use the information and systems with cautions and protections, the IS autonomy in BYOD can reach its intended goals without compromising the organization's information security.

Theoretical Model

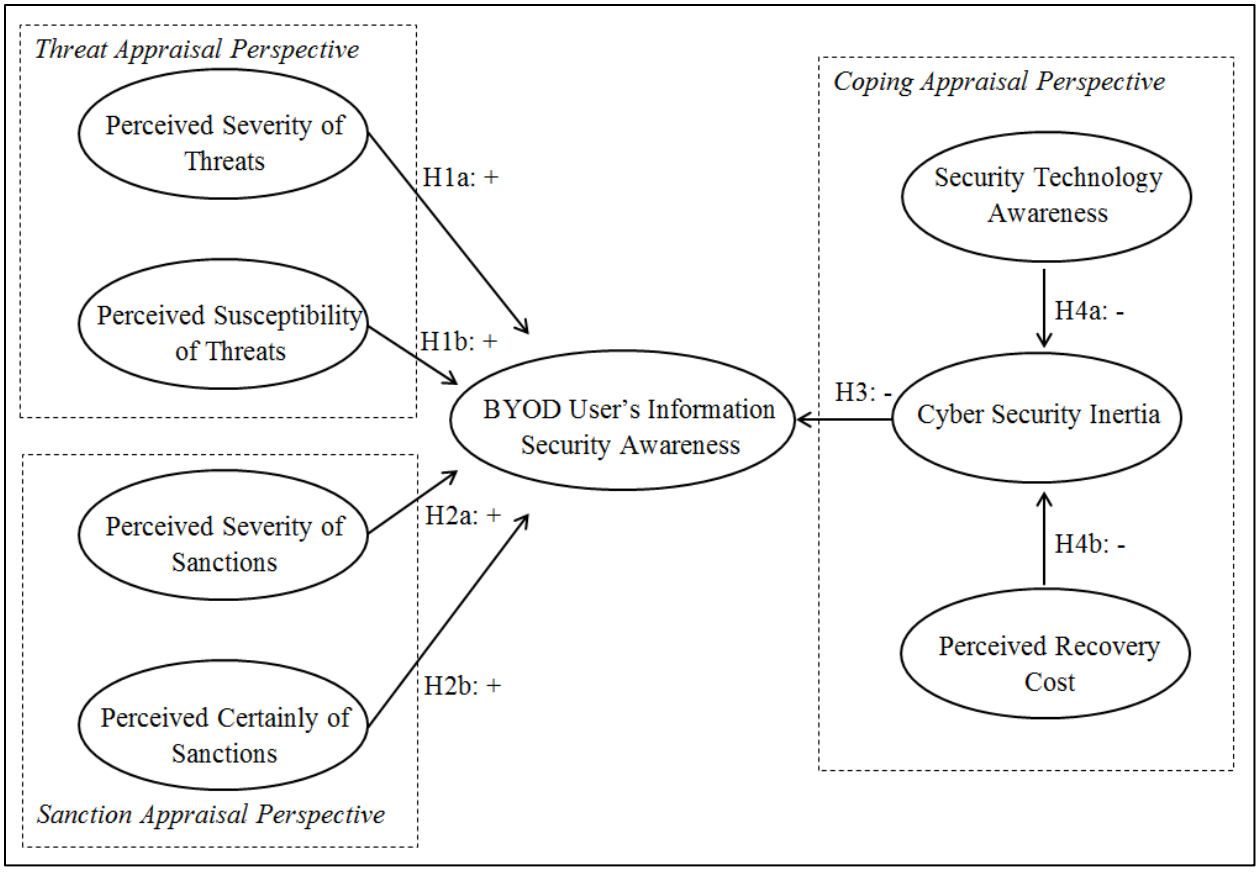

Figure 1. BYOD User's Information Security Awareness Model

Because of its importance, we place an emphasis on a BYOD user's information security awareness in this study. Extending prior studies (Siponen, 2000; Siponen, 2001), we define the awareness as the degree to which the user is aware of the security countermeasures she should adopt and implement, in order to protect the organization information security in a BYOD program. We study this constructs from two lenses of research, including the protection motivation theory and the general deterrence theory.

The protection motivation theory (PMT) was introduced by Rogers (1975) to study an individual's reactions and subsequent behaviors when facing potential threats to her health. This theory believes that an individual's motivation for searching for protections is aroused, if she believes that negative outcomes from threats are severe, and the consequences are likely to occur (Rogers, 1983). Subsequently, the motivation can increase the individual's intention to adopt protection countermeasures and her actual use of the countermeasures (Rogers, 1983). Extending this point of view, prior studies (Herath and Rao, 2009, Johnston and Warkentin, 2010, Liang and Xue, 2010, Siponen et al., 2014; Vance et al., 2012) argue that an information system user's threat appraisal factors such as her perceived severity and susceptibility of threats can strongly influence the user's information security postures and practices. According to the PMT, we introduce the following hypotheses:

H1a. A user's perceived severity of threats can have a significant positive effect on her information security awareness in a BYOD program.

H1b. A user's perceived susceptibility of threats can have a significant positive effect on her information security awareness in a BYOD program.

The general deterrence theory (GDT) was introduced to study the deterrence effects of an organization's sanction policies on a user's computer misuse intention and behaviors. We are interested in two influential factors in this study, including a user's perceived severity and perceived susceptibility of sanctions if she fails to protect the organizational information resources in a BYOD program. Extending prior studies (D'Arcy et al., 2009), we define a user's perceived severity of sanctions as the degree to which the user believes that sanctions from failing to protect the organization's information security can bring severe consequences to her. We define a user's perceived susceptibility sanctions as the degree to which the user believes that punishments are likely to fall on her, if she fails to protect the organization's information security. Even though prior studies (D'Arcy et al., 2009, Lowry et al., 2015; Siponen and Vance, 2010) have conflicting findings about the deterrence effects of a user's sanction appraisals on her computer misuse, we take a more conservative view, and assume that the two sanction appraisal factors (i.e., a user's perceived severity and perceived susceptibility of sanctions) can raise her information security awareness in a BYOD program. We introduce the following hypotheses:

H2a. A user's perceived severity of sanctions has a significant positive effect on her information security awareness in a BYOD program.

H2b. A user's perceived certainty of sanctions has a significant positive effect on her information security awareness in a BYOD program.

Because a successful security management greatly depends on the end user's security practices and behaviors, we also look at how a user's personal security habit, especially the one with negative tone, can influence her information security awareness in a BYOD program. We develop a new construct, cyber security inertia, to measure the impact of negative personal security habit on a user's information security awareness. We define cyber security inertia as the degree to which a user tends to postpone the adoption and implementation of security countermeasures on her personal devices used for BYOD. We have the following hypothesis:

H3. A user's cyber security inertia has a significant negative effect on her information security awareness in a BYOD program.

We explore the possibility of using a user's security technology awareness and perceived recovery cost as solutions to resolve the cyber security inertia issue in BYOD. A user's security technology awareness is defined as the degree to which the user is aware of the existence and functionalities of the latest protective technologies (Han et al., 2014). Because damages from a cyber threat are difficult to detect, most users do not have the knowledge about the threat, until they are presented with corresponding protective technologies (Dinev and Hu, 2007, Han et al., 2014; Kruger and Kearney, 2006). Thus, raising a user's security technology awareness can not only remind the user the importance of information security, but

can also update her with the new movement in cyber threats and how to handle those threats with available protective technologies. When the user recognizes the potential threats, and comprehends the benefits of using the new protective technologies, she is likely to adopt and implement the protections in a timely manner. We introduce the following hypothesis:

H4a. A user's security technology awareness can have a significant negative effect on her cyber security inertia in a BYOD program.

We define a user's perceived recovery cost as the degree to which the user believes that she has to consume valuable resources such as time, effort, and money, in order to restore the information lost in cyber threats. According to the rational choice theory (McCarthy, 2002; Paternoster and Pogarsky, 2009), increasing a user's perceived benefits and decreasing the user's perceived costs of using security countermeasures can build the user's positive security attitude and practices. However, a user's decision making regarding information security is peculiar. Benefits are usually negligible and unpredictable to the user, but costs such as the effort and money spent on using a security countermeasure can be enormous (Bordin et al., 2008; Gordon and Loeb, 2006). The biased estimation can lead to the user's resistance to security countermeasures and practices. To address this issue, prior studies (Bulgurcu et al., 2010; Herath and Rao, 2009) suggest using an opportunity cost approach such as raising the user's perceived cost of not complying with organizational policies, raising the perceived cost of not using protections to rectify the user's prejudices. When the user realizes that using information with cautions and protections now can help her avoid overwhelming recovery costs in the future, she is more likely to adopt and implement the protection countermeasures in a timely manner. We introduce the following hypothesis:

H4b. A user's perceived recovery cost can have a significant negative effect on her cyber security inertia in a BYOD program.

Future Research

We plan to use an online survey methodology to collect data. We suggest that findings from the current and future studies can make the following contributions: First, we can validate how factors of the PMT and GDT can influence a user's information security awareness in an open computing environment. The PMT and GDT have been broadly used to study a user's security awareness, security policy compliance, and computer misuse in a centralized information system, in which users are required to use the computer systems with the same settings and follow the uniform security policies. However, in a BYOD program, users usually do not have such requirements. Thus, it is necessary to validate the PMT's and GDT's roles in an open computing environment such as a BYOD program. Second, our study takes a user's cyber security inertia into account. This approach can better describe the actual environment of a BYOD program, in which the user's security practices established in her personal computing environment may have a strong effect on her security awareness of organizational information resources. To our best knowledge, there have not been many studies looking at this influence. Thus, findings from our studies can address this knowledge gap.

References

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, 51(4), 64-68.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Business Wire. (2015). IDC forecasts U.S. mobile worker population to surpass 105 million by 2020. Retrieved from http://www.businesswire.com/news/home/20150623005073/en#.VYmhfEZB58m

Crossler, R. E., Long, J. H., Loraas, T. M., & 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), 209-226.

Digital Guardian. (2016). BYOD security: Expert tips on policy, mitigating risks, & preventing a breach. Retrieved from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 386.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.

E&Y. (2013). Bring your own device: Security and risk considerations for your mobile device programs. Retrieved from http://www.ey.com/GL/en/Services/Advisory/Bring-your-own-device---mobile-security-and-risk

Forrester Research. (2016). Bring your own device (BYOD). Retrieved from https://www.forrester.com/Bring-Your-Own-Device-%28BYOD%29

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, 35(10), 191-197.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, 49(1), 121-125.

Han, B., Wu, Y., & Windsor, J. (2014). User's adoption of free third-party security apps. *Journal of Computer Information Systems*, 54(3), 77-86.

Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive*, 11(3), 99-112.

Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security*, 10(4), 186-202.

Herath, T., & Rao, R.H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-25.

I-CIO. (2013). Four top CIOs herald an era of "bring your own... everything". Retrieved from http://www.i-cio.com/strategy/workspace-it/item/four-top-cios-herald-an-era-of-bring-your-own-everything

ITLP. (2012). Bring your own device: Is it worth it? Retrieved from http://www.itlpblog.com/2012/04/30/bring-your-own-device-is-it-worth-it-2/

Johnston, A. C., & Warkentin, M. (2010), Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 540-566.

Johnston, A. C., & Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-34.

Kruger, H.A., & Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computer & Security*, 25(4), 289-96.

Liang, H., & 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.

Lowry, P.B., Posey, C., Bennett, R.J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal*, 25(3), 193-230.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, 28, 417-442.

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 12, 5-8.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology*, 25(2), 103-127.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-114.

Rogers, R. W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protected motivation. In: Cacioppo, J. T., & Petty, R.E., editors. *Social psychophysiology: A sourcebook*. The Guilford Press: 1983.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society*, 31(2), 24-29.

Siponen, M., Mahmood, M.A., & Pahnila S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.

Telegraph. (2012). Smartphones and tablets add two hours to the working day. Retrieved from http://www.telegraph.co.uk/technology/mobile-phones/9646349/Smartphones-and-tablets-add-two-hours-to-the-working-day.html

TrendMicro. (2012). Mobile threats in action. Retrieved from http://www.trendmicro.com/us/boxes/lightboxes/20120802163027.html

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3/4), 190-198.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18, 101-105.

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

Workman, M., Bommer, W.H., & Straub, D.W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.