WISP 2018 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2018

Non-Malicious Information Exposure Through Personal Device Usage

Tyler M. Pieron
Nova Southeastern University, tp877@mynsu.nova.edu

James N. Smith
Augusta University, jasmith8@augusta.edu

Non-Malicious Information Exposure Through Personal Device Usage

Tyler M. Pieron
College of Engineering and Computing, Nova Southeastern University,
Fort Lauderdale, Florida, United States
tp877@mynsu.nova.edu

James N. Smith
School of Computer and Cyber Sciences, Augusta University,
Augusta, Georgia, United States
jasmith8@augusta.edu

ABSTRACT

Information technology security policies are designed explicitly to protect IT systems. However, overly restrictive information security policies may be inadvertently creating an unforeseen information risk by encouraging users to bypass protected systems in favor of personal devices, where the potential loss of organizational intellectual property is greater. Organizations that implement overly restrictive web filtering, website blocking, and other security measures to protect the integrity of their information systems are likely introducing a risk that sensitive or protected information will be processed on personal devices, outside of the organizational framework, as users identify the most efficient and effective way to accomplish work-related tasks unimpeded.

Current models regarding the acceptance and use of technology, primarily TAM3 and UTAUT2, address the use of technology in organizations and by consumers, but little research has been done to identify an appropriate model to begin to understand what factors would influence users that can choose between using their own personal device and using organizational IT assets, separate and distinct from "bring your own device" constructs. This research aims to bridge that divide by identifying the factors that influence users to select their own device to overcome organizational restrictions in order to accomplish their work.

Keywords: Insider threat, information security, compliance, information security policy, behavioral issues of information security, information security awareness, information security management, theory of planned behavior

INTRODUCTION

Insider threats have existed for millennia, acknowledged in the earliest known writings, including in the histories of Herodotus of Halicarnassus where he described Greek spies being spared by Xerxes (Herodotus and Grene 1987). Sun Tzu also recognized insider threats in his famous treatise *On the Art of War*, where he identified five classes of spies, including "having local spies means employing the services of the inhabitants of a district" and "having inward spies, making use of officials of the enemy" (Sawyer and Sawyer 1994). Insider threats are nothing new, but the vastness of information that can be compromised by one trusted insider has increased exponentially since the advent of the information age. Indeed, Bickers (2000), cited the potential loss of company information as a restraining factor for companies when first contemplating e-commerce in the late 1990s and 2000s.

Despite the multitude of historical examples, research into insider threats to information systems has long been neglected in favor of the perceived threats posed by external factors, such as viruses, worms, hackers, and others. This general trend continues, with recent research by Beckett (2015) indicating that while organizations have doubled their spending to protect themselves against the loss of information and systems, the vast majority of spending has been used to harden systems against external threats. One potential reason for this divide is the lack of reliable data concerning insider threats, as organizations aim to minimize the damage caused by malicious insiders in order to limit their exposure to the secondary and tertiary effects of losses (Bulgurcu et al. 2010; Pfleeger and Stolfo 2009).

Despite the focus on systems and processes for identifying threats to information systems against external threats, and the recognition of the threats posed by malicious insiders, there has been little study or effort to identify ways in which critical information can be exposed by non-malicious insiders who use personal devices to conduct work related tasks outside of the organizational information systems infrastructure.

Management and organizational restrictions regarding Internet usage within large organizations are common. Within agencies of the U.S. government (Department of Defense 2012), these restrictions impede the ability of intelligence analysts to conduct Internet based research, known as “open source” research (Glassman and Kang 2012). These restrictions include prohibitions on “viewing, storage, copying or transmission of materials related to…illegal weapons, terrorist activities or any other illegal activities or activities otherwise prohibited” (Frederick 2014). Offensive, prohibited and resource intensive websites, such as video and audio streaming services, are frequently blocked by web filtering tools. These restrictions are specifically applicable to the unofficial use of IT systems, allowing for access to these materials and subjects for official purposes, but through practice and design, there are limited methods to differentiate between official and unofficial use except in ex post facto reviews (Frederick 2014).

Consequently, intelligence analysts that wish to avoid lengthy review processes in which they have to justify accessing prohibited content, or burdensome processes required for requesting permission in advance, may choose to forego accessing potentially problematic materials while using government systems, opting instead to use personal devices and networks to access information.

PROBLEM STATEMENT

Organizations that impose significant restrictions on Internet use increase the likelihood that employees will use personal devices to conduct work related tasks, escalating information security risks (Gundu and Flowerday 2012; Hovav and Putri 2016). The use of web filters and other information technology approaches to limit the accessibility of potentially inflammatory, objectionable, or ostensibly non work-related websites are largely effective in reducing employee misuse of information technology resources (Glassman et al. 2015); however, when access to Internet resources that are necessary to accomplishing work related tasks are restricted, these constraints may encourage employees to bypass organizational constraints by using their own devices and networks to access Internet based information. The use of personal devices and Internet resources to conduct work related activities increase the risk of information compromise (Garba, Armarego, Murray, et al. 2015; Hovav and Putri 2016). Previous studies examining how and when people use technology have largely approached the issue in a bifurcated manner, examining the use of technology in organizations and by consumers as discrete and separate (Venkatesh et al. 2012; Venkatesh and Bala 2008). This study aims to bridge the gap between these two approaches by examining the factors that influence the behavioral intention and use behavior of technology when employees can bypass organizational restrictions by using personal devices to accomplish work related tasks, potentially exposing sensitive information.

Research Goal and Significance

The purpose of this research is to investigate whether internet usage restrictions influence intelligence analysts to conduct open source research on personal devices, which can lead to organizational harm including potentially exposing confidential information to adversaries (Fleischer et al. 2018; Fredericks 2018; Timberg 2018).

Recent discoveries of advanced intelligence collection systems near U.S. intelligence and defense facilities, known colloquially as “IMSI catchers” and “Stingrays”, which act as a man in the middle attack on cellular telephones and devices, allowing for the interception and collection of both voice and data, lend credence to the concept that unwitting use of personal devices may expose information (Fleischer et al. 2018; Fredericks 2018; Timberg 2018). As a result, employees who fully comply with applicable restrictions while operating enterprise IT systems may unknowingly expose critical information by conducting research using personal equipment such as at home or using mobile devices.

The use of personal devices, including such generally benign devices like fitness trackers, have been used to reveal confidential and sensitive information (Ching and Singh 2016; Lidynia et al. 2017). In 2018, a security flaw in a mobile fitness application revealed “6,400 users believed to be exercising at sensitive locations, including the NSA, the White House, MI6 in London, and the Guantanamo Bay detention center in Cuba, as well as personnel working on foreign military bases” (Whittaker 2018). In another example, the location of U.S. military personnel engaged in combat operations in Syria and Afghanistan were revealed through another fitness tracking device (Sly 2018). While these incidents did not violate organizational policies (Sisk 2018), nor did they involve organizational information systems, they nevertheless, and apparently entirely inadvertently, exposed highly sensitive information to potential adversaries.

There have been extensive studies evaluating how, when, and why users accept and use technology. The two primary competing models reflect the differences between the organizational use of technology and how consumers use technology. The primary model used to understand how technology is used within organizations is known as the Technology Acceptance Model 3 (TAM3) (Venkatesh and Bala 2008), which includes antecedents such as voluntariness as well as perceptions of external control. Recognizing that models developed to understand how users accept technology they are required to use for employment is fundamentally different from technology users choose for themselves, a separate model known as UTAUT2 was developed (Venkatesh et al. 2012). UTAUT2 is similar in many ways to TAM3 but reflects the unique influences that individual choice has on using technology, such as incorporating age, gender, and experience as moderating factors. While TAM3 is well suited to evaluating technology acceptance in organizations, UTAUT2 is better suited and designed to accomplish the same for individual consumers. The TAM3 and UTAUT2 models represent the current state of acceptance theory in information systems.

Addressing both technical violations that are inadvertent, as well as those committed maliciously or with reckless disregard for the potential consequences has long been a challenge when developing appropriate definitions for insider threats (Loch et al. 1992). Brackney and Anderson (2004) proposed one of the foundational definitions of what constitutes an insider threat in the context of information assurance concerns: "malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems" (p. 9). Significant research has been conducted regarding the implementation and effectiveness of internet use policies, web filtering tools, formal and informal control mechanisms and sanctions, and behavioral and motivational pressures, all which have undoubtably decreased misuse of information technology systems. However, there is limited research as to what effect these policies have on users avoiding using provided information systems, instead choosing to more efficiently access information on personal devices, representing a potential insider threat in regards to the loss of information.

Integral to the choice of users selecting personal devices instead of organizational IT resources, is the concept of privacy. Sometimes also referred to as trust, privacy has been approached in a number of ways within the literature, including as a contextual relationship within the existing UTAUT2 and TAM3 models, specifically as part of adoption beliefs such as effort expectancy and facilitating conditions (Venkatesh et al. 2011), but generally not as an independent moderating factor. Other works, such as Dinev, McConnell and Smith's (2015) expanded Antecedents–Privacy Concerns–Outcomes (APCO) approach recognizes the impact privacy plays in individuals' choices, which is not reflected in current technology acceptance models. The confluence of privacy, user acceptance of technology, as well as security is partially addressed in the various evolutions of technology acceptance models. However, there is little understanding or study of what influences users to choose between organizational resources, such as those modeled and described in TAM3, and the use of personal devices, which UTAUT2 models for consumers.

Conceptually, this paper will attempt to bridge the gap between TAM3 and UTAUT2 by examining what factors influence users to select personal devices over organizational systems to accomplish work related tasks. Additionally, this research will incorporate the impact that the perception of privacy has on the behavioral intention and use behavior of employees to avoid use restrictions and other barriers to free access of the Internet. This proposed research model incorporates selected constructs as antecedents to behavioral intention and use behavior inspired by the TAM3 and UTAUT2 models to investigate what effect organizational policies as well as the impact the perception of privacy has on users selecting between organizational resources and personal devices to conduct work related activities.

The use of personal devices and systems to accomplish work related information gathering tasks likely does not pose a direct threat to information systems of an organization, however, the use of extra-organizational resources, such as personally owned smart phones or home computers, may introduce unintended risks to sensitive information (Garba, Armarego, and Murray 2015). Intelligence analysts provide a unique social milieu in which to examine the factors influencing personal device usage, as they are prohibited by law and policy from possessing or using personal devices within their work spaces (National Counterintelligence and Security Center 2017). This allows for a clear demarcation between organizational IT devices and other situations wherein personal devices are not provided by the organization but authorized for use, such as is the case with BYOD (Hovav and Putri 2016).

By gaining a fuller understanding of the prevalence of personal device usage, as well as the impact organizational policies has on personal device use behavior, organizations can make informed decisions as to what Internet use policies are appropriate and develop remediation strategies to mitigate risks.

Approach

In order to develop empirical support within a framework inspired by UTAUT2/TAM3, this study will employ an exploratory quantitative research design conducted in three phases. During the first phase, the survey instrument will be developed following a review of literature and validated against a panel of experts using the Delphi method. The Delphi method is generally considered a quick, inexpensive, and relatively efficient method to ensure consensus regarding a topic or process that require individual judgements (Powell 2003). The survey instrument will be developed based on validated scales from previous studies, which according to Hair (2010), is consistent with established best practices. A pre-test will be used to increase confidence and fit (Oksenberg and Kalton 1991) and will be examined to minimize issues related to instrument validity, including content and construct validity as well as reliability as identified by Straub (1989).

In the final phase, following the development of the survey instrument and validation, an online survey will be provided to members of the United States Intelligence Community through a variety of platforms, with the goal of receiving ~500 valid responses. This survey will be submitted for approval for distribution through the Office of the Director of National Intelligence for posting on US government systems to increase the quality and quantity of responses.

REFERENCES

Beckett, P. 2015. “An Intelligent Approach to Security,” *Network Security* (2015:2), pp. 18–20. (https://doi.org/10.1016/S1353-4858(15)30009-X).

Bickers, C. 2000. “Playing It Safe.,” *Far Eastern Economic Review* (163:23), p. 56.

Brackney, R. C., and Anderson, R. H. 2004. “Understanding the Insider Threat. Proceedings of a March 2004 Workshop,” DTIC Document.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly* (34:3), pp. 523-A7.

Ching, K. W., and Singh, M. M. 2016. “Wearable Technology Devices Security and Privacy Vulnerability Analysis,” *International Journal of Network Security & Its Applications* (8:3), pp. 19–30.

Department of Defense. 2012. “Joint Ethics Regulations (DOD 5500.7-R),” Washington, D.C: Government Printing Office, September 11. (http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/550007r.pdf).

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. “Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the ‘APCO’ Box,” *Information Systems Research* (26:4), pp. 639–655. (https://doi.org/10.1287/isre.2015.0600).

Fleischer, J., Yarborough, R., and Piper, J. 2018. “Potential Spy Devices Which Track Phones Found All Over DMV,” *NBC4 Washington*, , May 17. (http://www.nbcwashington.com/investigations/Potential-Spy-Devices-Which-Track-Cellphones-Intercept-Calls-Found-All-Over-DC-Md-Va-482970231.html, accessed May 19, 2018).

Frederick, H. 2014. *Authorized Unofficial Use of Government-Provided Information Technology (DISA Instruction 630-225-15)*, Defense Information Systems Agency.

Fredericks, B. 2018. “Feds Reportedly Find Surveillance Tech near White House,” *New York Post*, , June 1. (https://nypost.com/2018/06/01/feds-reportedly-find-surveillance-tech-around-white-house/, accessed June 4, 2018).

Garba, A. B., Armarego, J., and Murray, D. 2015. “A Policy-Based Framework for Managing Information Security and Privacy Risks in BYOD Environments,” *International Journal of Emerging Trends & Technology in Computer Science* (4:2), pp. 189–98.

Garba, A. B., Armarego, J., Murray, D., and Kenworthy, W. 2015. “Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments,” *Journal of Information Privacy & Security* (11:1), pp. 38–54.

Glassman, J., Prosch, M., and Shao, B. B. M. 2015. "To Monitor or Not to Monitor: Effectiveness of a Cyberloafing Countermeasure," *Information & Management* (52:2), pp. 170–182. (https://doi.org/10.1016/j.im.2014.08.001).

Glassman, M., and Kang, M. J. 2012. "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," *Computers in Human Behavior* (28:2), pp. 673–682.

Gundu, T., and Flowerday, S. V. 2012. "The Enemy within: A Behavioural Intention Model and an Information Security Awareness Process," in *2012 Information Security for South Africa*, IEEE, August, pp. 1–8. (https://doi.org/10.1109/ISSA.2012.6320437).

Hair, J. F. (ed.). 2010. *Multivariate Data Analysis*, (7th ed.), Upper Saddle River, NJ: Prentice Hall.

Herodotus, and Grene, D. 1987. *The History*, Chicago: University of Chicago Press.

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), pp. 35–49.

Lidynia, C., Brauner, P., and Ziefle, M. 2017. "A Step in the Right Direction – Understanding Privacy Concerns and Perceived Sensitivity of Fitness Trackers," in *Advances in Human Factors in Wearable Technologies and Game Design*, Advances in Intelligent Systems and Computing, Springer, Cham, July 17, pp. 42–53. (https://doi.org/10.1007/978-3-319-60639-2_5).

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *Mis Quarterly*, pp. 173–186.

National Counterintelligence and Security Center. 2017. *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, Office of the Director of National Security. (https://www.dni.gov/files/NCSC/documents/Regulations/Technical-Specifications-SCIF-Construction.pdf).

Oksenberg, L., and Kalton, G. 1991. "New Strategies for Pretesting Survey Questions," *Journal of Official Statistics* (7:3), p. 349.

Pfleeger, S. L., and Stolfo, S. J. 2009. "Addressing the Insider Threat," *IEEE Security & Privacy Magazine* (7:6), pp. 10–13. (https://doi.org/10.1109/MSP.2009.146).

Powell, C. 2003. "The Delphi Technique: Myths and Realities," *Journal of Advanced Nursing* (41:4), pp. 376–382. (https://doi.org/10.1046/j.1365-2648.2003.02537.x).

Sawyer, R. D., and Sawyer, M. 1994. *The Art of War*, Westview Press.

Sisk, R. 2018. "Pentagon Reviewing Fitness Trackers That Could Expose Troop Locations," *Military.Com*, , January 29. (https://www.military.com/daily-news/2018/01/29/pentagon-reviewing-fitness-trackers-could-expose-troop-locations.html, accessed July 17, 2018).

Sly, L. 2018. "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *Washington Post*, Washington, D.C. (https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html).

Straub, D. W. 1989. "Validating Instruments in MIS Research," *MIS Quarterly*, pp. 147–169.

Timberg, C. 2018. "Signs of Sophisticated Cellphone Spying Found near White House, U.S. Officials Say," *Washington Post*. (https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/signs-of-sophisticated-cell-phone-spying-found-near-white-house-say-u-s-officials/).

Venkatesh, V., and Bala, H. 2008. "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences* (39:2), pp. 273–315.

Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., Hu, P. J.-H., and Brown, S. A. 2011. "Extending the Two-Stage Information Systems Continuance Model: Incorporating UTAUT Predictors and the Role of Context," *Information Systems Journal* (21:6), pp. 527–555. (https://doi.org/10.1111/j.1365-2575.2011.00373.x).

Venkatesh, V., Thong, J. Y., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157–178.

Whittaker, Z. 2018. "Fitness App Polar Exposed Locations of Spies and Military Personnel," *ZDNet*, , July 8. (https://www.zdnet.com/article/fitness-app-polar-exposed-locations-of-spies-and-military-personnel/, accessed July 17, 2018).