Smartphones Usage at Workplace: Assessing Information Security Risks from Accessibility Perspective

Asif Shaikh[1]

[1] Florida State University, Tallahassee, Florida, 32301, USA
ashaikh@fsu.edu

Abstract. Innovations in technology have created opportunities for employees to be increasingly efficient, productive and always connected to both internal and external customers as they go about their everyday lives using consumer IT tools and resources. This leads to increasingly employee's use of such resources at hand while performing their routine activities at workplaces due to inherent features of connectivity that allow ease of access to information assets. Building on the significance of effort expectancy (ease of use) in earlier research on smartphone adoption at workplace, this study seeks to examine from the aspect of accessibility (ease of access) as a key feature of smart phone usage. It adapts key constructs of Routine Activity Theory (RAT) in the premises of information systems security, viewing the construct of accessibility (ease of copying/transfer data) as a risk associated with the smartphone usage at workplace. That is, focusing on the probability of convenience (opportunity) as a motivation to commit crime. Through analysis of extant literature and theoretical assertions, it presents a theoretical model that can help identify the relationship between smartphone usage and occurrence of insider fraud incidents in the presence of certain situational stimuli. This study assumes that there are possible implications at workplace in terms of ease of access which a smartphone device provides to an employee allowing them to copy/transfer sensitive information assets conveniently, the practice that may actually increase the occurrence of detrimental security behaviors in the absence of management controls.

Keywords: Smartphones Usage, Identity Fraud, Personal-IT, Routine Activity Theory.

Introduction

The practice of using a smartphone at workplace, whether at an individual employee or a group act, is conceptualized in Information System literature as Personal-IT or as an informal-IT usage.

Smartphones Usage Context

There are two contexts in which smartphones are being used in organizations currently:

Personal-IT. Some employers decided to adapt to this change by recognizing the benefits of personal devices on task and employee performance while understanding the limitations of their official IT, infrastructure set up, and policies so they permit users to deploy their personal devices for personal as well as for business purposes, both on site and remotely[1]. As a result, the concept of Bring-Your-Own-Device (BYOD) emerged [1].

Shadow-IT. Sometimes organizations, do not allow; approve of informal or personal IT use at work; or have not devised any (BYOD) policy guidelines as yet, or are unaware of how extensive usage of personal devices is in the organization and in what ways it has been accessing information assets, in that case, management has no control in maintaining or regulating its usage [2]. This practice of an informal IT use, characterizing a hidden; unauthorized; unsanctioned; or a non-transparent practice is conceptualized as Shadow-IT [3]. Rogue IT, Hidden-IT, and Grey-IT are similar terms that were used in the early stages of Shadow-IT research [4]. In such cases, there is more likelihood of a compliance issues, wasted time, inconsistent business logic, increased risks for data loss or leaks, wasted investment, and other potential damage [5].

Smartphones Usage Risks

Although smartphones for personal and/or official use at workplace bring positive outcomes, two entirely opposite in scope but interrelated phenomena have emerged in the context of its usage over time. First, internet enabled devices (smartphones) have made the processes easier than ever [6] and work performances better. Second, it has also led to unpredictable growth in digital crimes. Hence, the risk of information security cannot be ignored in certain situational contexts.

Risk of Insider (ID) Fraud. Insider-fraud is an access policy violation [7]. Since employee is a 'trusted agent', [8;9;10], who while interacting with the information assets of the organization, choses to abuse that trust. Identity (ID) fraud is one of the forms of insider fraud which has been a mounting concern for scholars and practitioners. Identity such as name, social security numbers, driver's license number, credit card numbers, mother's maiden name are considered as sensitive information and also known as Personally Identifiable Information (PII). According to the Identity Theft Resource Center, in the U.S. 9,395 such cases were documented from January 1, 2005 to September 30, 2018. The criminals use those identities to steal money, claim social security and unemployment benefits, and so on. While, the number of such data breaches in the organizations continue to rise making ID fraud the central crime of the information age [11], there is no research available that signifies the relationship between smartphone usage and employees' intention to commit (insider) fraud.

Assuming that smart phone technologies have introduced new organizational risks and have intensified the growth of data breaches incidents in the organizations by employees. This study specifically explores possible implications of smartphone usage by employees who work in an environment where the PII is handled or managed as a routine activity.

The premises that an insider engaged in an organizational misbehavior is more likely a motivated offender is based on a work drawing on social bond/control theory [12]; Rational choice theory (RCT) [13]; and theory of planned behavior (TPB) [14] studying dispositional factors in IS research. A malicious insider has the distinct advantage of understanding the corporation's information assets with legitimate and often privileged access to information [15]. Advancing the current research on personal-IT usage as an insider threat, my work further proposes that the smartphones usage of an employee increases the convenience of engaging in crime [16] in situations when accessibility to organizational information assets intersects with lack of management controls as envisaged in a Routine Activity Theory (RAT) [17].

Focusing on the convenience of crime as a motivation, I propose the following research question:

RQ: Does greater accessibility to an information asset of high value such as PII affect the behavioral intention and subsequently the likelihood to commit an insider fraud for an employee using smartphone at workplace?

A theoretical model that focuses on the "risk" side of the smartphone usage of an employee has been developed on the basis of smartphone features that provides ease or convenience to access, copy/transfer and then steal sensitive information. That is, the framework examines the accessibility phenomenon both as a privileged access of an employee and the accessibility features of a smartphone that increases the risk of insider fraud in the presence of favorable situational stimuli.

The remainder of this paper is organized as follows: First, I will review the extant literature and then will explain the theoretical constructs of Routine Activity Theory (RAT) [17] vis a vis the associated concept under study. Second, I will hypothesize how *greater access* to information assets of *high value* through model development and Last, I will briefly discuss how the model can be applied for valuable contributions in the field.

Smart Phones- A tool of Convenience- A Literature Review and a Theoretical Framework

Smartphone is a tool of convenience. A digital camera and other multimedia features of a smartphone are typically utilized by employees at workplace for various reasons. In prior studies [18], examination of people's intentions at the time of capture and subsequent patterns of use and found out that employees capture images for both affective and functional reasons [18]. The most common social reason for capturing an image was to enrich a mutual experience by sharing an image. The functional reasons might include performing a mutual task, a remote task [18]. Employees might also want to prove they have done a job by taking a picture [19], or to keep as a record for making

decisions in future. Another study [20] on information capture opportunities at workplace found out that taking picture is easier for them as for many other tools available to capture information several time-consuming steps are to be followed. In addition to in-built features of a smartphone that enable capturing information, the connect feature of a smartphone such as with its carrier network, a local Wi-Fi network, a Bluetooth network, and its mobile operating system, allows data to be further stored and transferred to other devices or medium with ease.

Earlier research [21] [22], used effort expectancy (EE) to assess the degree of ease that influence behavioral intention to use a technology that is significantly related to the adoption of smartphones at workplace. And performance expectancy (PE), a degree to which an individual believes that using the system will help employee to attain gains in job performance, as key constructs. Theses studies [21] [22] revealed that ease of use and performance improvement have significant positive relationship with the intention to adopt smartphone application at workplace.

Another study [23] indicated in their study that smart phone is emerging as a primary computing device is expected to replace or reduce the usage of other devices like personal computers. Some studies [19] indicated a surprising amount of use of a smartphone with a computer, but people also took pictures of their screen, made videos of programs running, and even browsed the web with the phone rather than the computer.

With the advancement of mobile phone technology, in built cameras have high precision and quality that even can produce a print that is similar to the quality obtained with a scanner. Copies and printers are not portable but Smart phones are portable and can even incorporate a feature of quick scan and share on different mediums with a simple touch command.

Studies [24] on the information security challenges of using personal devices at work are of view that once data is downloaded to a portable device, it is easier to make copies and transfer files to other mediums. The confidentiality of a sensitive data such as corporate data is vulnerable to many threats and attacks once it is on a portable (BYOD) device [24]. Further, when use of mobile devices are not in compliance with the organizations' security policies or management does not have a security policy (Shadow-IT use), there pois a potential opportunity for the fraudulent behavior from respective shadow users [25].

Theoretical Framework

The base of the overarching framework I plan to investigate is essentially an integration of theoretical constructs of a Routine Activity Theory (RAT) [17]. RAT informs of the likelihood of organizational misbehavior of an insider when an *accessibility* to an attractive target of significant value and *lack of a capable guardian* intersects in time and space. RAT provides a theoretical lens of crime event triangle depicted in the work of Cohen and Felson (1979) that has three necessary elements (suitable target, motivated offender and lack of capable guardianship) each coming together in time and space to produce a criminal event [17].

Suitable Target – Greater Access. The attractiveness of a target is better interpreted from the offender's point of view [26;27]. RAT posits that target-objects vary in attractiveness to offenders based on four characteristics: value, inertia, visibility, and access (VIVA) (Felson & Cohen, 1980). The effects of target suitability, and guardianship on victimization of six cyber-crimes [28] were analyzed in context of IS environment, showed that some RAT elements (visibility, accessibility and capable guardianship) are more applicable than others. Accessibility refers to the ability of an offender to get to the target and then get away from the scene of the crime. The greater the accessibility a target has, the more suitable it is for theft [24]. Common identity fraud is an access policy violation when the insider is entrusted with access to sensitive data assets but abuse that trust [7].

A Motivated Offender. A Motivated Offender is a person with criminal inclinations and the ability to put those impulses into practice [17; 29]. Cohen and Felson (1979) assume that all humans are criminally inclined, as almost everyone is capable of deviant conduct if an opportunity were to present itself. As predictor variables, within RAT, motivated offenders are assumed to exist—and their individual cognitions and motivations are considered tangential [30].

Absence of a Capable Guardian. According to RAT, a capable guardian is a person or object which deters a crime to occur. Guardian can be a supervisor, manager, coworker [27]. Also, security measures such as security cameras, lighting, and alarm systems can be guardians [31]. Whereas network administrators, security staff, and IT auditors serve as social guardians [32]. The most vital duties for guardians are availability and monitoring that means someone is watching the activities and could detect inappropriate behaviors that discourage the likely offender from committing a criminal act [30].

Accessibility-based Model Development

A suitable or an attractive target can be an object of sufficient value and accessibility [29] to the potential offender with certain desired characteristics that the offender might want or might make the criminal act easier to perform [17; 26;27]. Given these formulations about target suitability in RAT, my focus on two sub variables of the construct of suitable target are: ***high value*** of, and ***greater access*** to secure data assets, that makes it a significant target when sold on to others who are better placed to monetize the information [33].

High Value of a Personal Information (such as PII):

Sensitive information can be any data or piece of information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. Among the three main types of sensitive information: Personal information, business information, and classified information, "Personal information" also named as sensitive personally identifiable information (PII) is the most significant

data asset. PII is data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers (passport or Social Security numbers).

Personal data is a valuable resource that has developed into a uniquely coveted asset. This information is worth billions. When data breaches expose unique identifiers, potential offenders can use these either to impersonate individuals and apply for loans, housing, utilities, or government benefit, or this information may be sold on the black market to other hackers.

Greater Access

This theoretical construct has two dimensions: First ***Privileged access*** to the sensitive information and Second, ***Ease of access*** to copy/transfer sensitive information.
Privileged access refers to any access privilege to permission to access the target system enabling employee access unique personal identifiers of a client, customer or patient in any given organization. This includes password access, policy control, or, any other form of accessing the personal information for work purposes. Privileged or authorized access to the network with either an account on a server or physical access [34;35] which one can choose to abuse, or misuse may lead to unexpected security violation (e.g., acquire and disseminate sensitive information).

Accordingly, the following hypothesis is offered in the specific context of ID-fraud:

H1: Greater Access (GA) to the information assets of high value by an employees' using smartphone such is positively associated with the behavioral intention (BI) to commit insider fraud.

H2: Greater Access (GA) to the information assets of high value by an employees' using smartphone ones is positively associated with the likelihood to commit insider (LIF) fraud in the absence of a capable guardianship (CG).

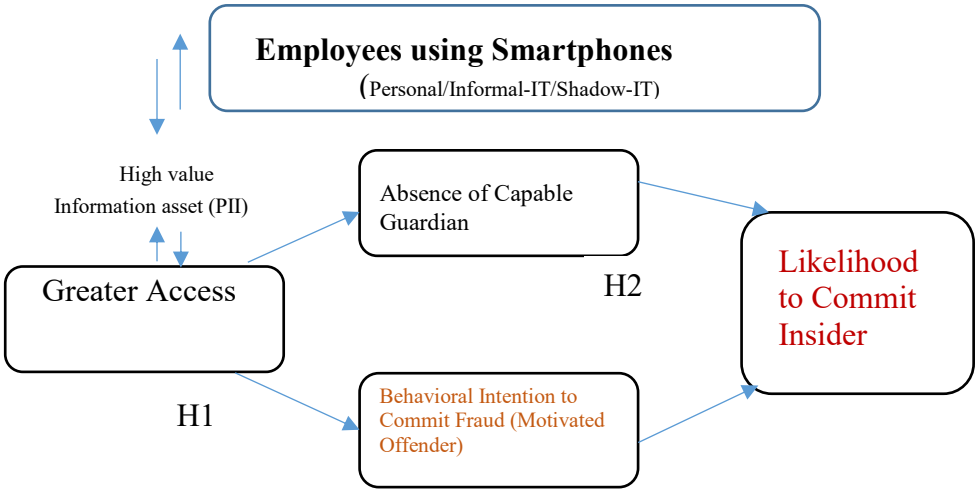

Fig. 1. A Proposed **Accessibility-based Theoretical Model** building relationship between Employees' Smartphone Usage and Insider Fraud

Next Step- Measuring and Analysis

Although smart mobile technology continues to be a vital resource, it also forms the source of a unique means for offenders by providing infinite opportunities to engage in crime.

To test this theoretical model, future studies may use a scenario-based web survey from a population sample of employees (public and corporate). By asking the respondents to read a scenario and imagine themselves in the context of the scenario's character, the researcher can establish a reliable and valid measure for behavioral intention as it relates to the various factors found in the scenario, even though the behavior may be socially undesirable [10]. A scenario-based survey approach has its ability to elicit forthright responses from study participants who were under the duress of potential retribution from the disclosure of truth (social desirability bias), as well as because of its ability to reveal the structure of individual decision-making [10]. A rich tradition of using scenario analysis established in the criminology field has been applied recently in IS research [36;37]. This method is found to yield valid and truthful data because the respondents are not asked to admit to personal intentions but instead to place themselves in the position of the scenario's characters, whereby they are more likely to self-report their likelihood to commit a crime [38] (Trevino & Victor, 1992).

The survey instrument can also be developed from existing scales borrowed and adapted from relevant literature [10;33]. I suggest using partial least squares (PLS) after developing specific measures to analyze the measurement model and test the research hypotheses. PLS, as a component-based structural equation modeling approach, places minimal restrictions on sample size [39].

The proposed theoretical model is expected to yield significant outcomes as it is essential for the securement of organizational information assets to understand where and how data can leave their systems [38]. In addition, this theoretical framework might furnish some insights to organizations that they will need a watchful eye to the use of smartphones in the sensitive environment. The survey, a quantitative data collection approach, brings breadth to a study by gathering data about different aspects of a phenomenon from many participants [22].

References

1. Köffer, S., Ortbach, K., Junglas, I., Niehaves, B., Harris, J.: Innovation through BYOD? Business & Information Systems Engineering 57(6), 363-375 (2015).
2. Raden, N.: Shadow IT. A lesson for BI. Information Management (2005).
3. Silic, M., Barlow, J. B., Back, A.: A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & management 54(8), 1023-1037 (2017).
4. György, A. A. B., Cleven, A., Uebernickel, F., Brenner, W.: Exploring the shadows: IT governance approaches to user-driven innovation. In: Proceedings of the European Conference on Information Systems, Barcelona, Spain (2012).
5. Silic, M., Back, A.: Shadow IT–A view from behind the curtain. Computers & Security 45, 274-283 (2014).
6. Balmer, J. M., Yen, D. A.: The Internet of total corporate communications, quaternary corporate communications and the corporate marketing Internet revolution. Journal of Marketing Management 33(1-2), 131-144 (2017).
7. Willison, R., Warkentin, M.: Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly 37(1), 1-20 (2013).
8. Im, G.P., Baskerville, R.L.: A longitudinal study of information system threat categories: the enduring problem of human error. The Data Base for Advances in Information Systems 36(4), 68-79 (2005).
9. Willison, R.: Understanding the perpetration of employee computer crime in the organizational context. Information and organization 16(4), 304-324 (2006).
10. Willison, R., Backhouse, J.: Opportunities for computer crime: Considering systems risk from a criminological perspective. European Journal of Information Systems 15(4), 403-414 (2006).
11. Zaeem, R. N., Manoharan, M., Yang, Y., Barber, K. S.: Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Computers & Security 65, 50-63 (2017).
12. Hirschi, T.: A control theory of delinquency. Criminology theory: Selected classic readings, 289-305 (1969).
13. Cornish, D. B., Clarke, R. V.: The reasoning criminal: Rational choice perspectives on offending. In: Cornish, D. B., Clarke, R. V. (eds.) Transaction Publishers (2014).
14. Ajzen, I.: From intentions to action: A theory of planned behavior. In: J. Kuhl., J. Beckmann (eds.) Action control: From cognition to behavior, pp. 11-39. Springer, New York, NY (1985).
15. Ho, S. M., Hollister, J.: Cyber insider threat in virtual organizations. Encyclopedia of Information Science and Technology. 3rd edn. IGI Global, USA (2015).
16. Padayachee, K.: A conceptual opportunity-based framework to mitigate the insider threat. In: Proceedings of the Information Security for South Africa, pp. 1–8. Johannesburg, South Africa (2013).
17. Cohen, L. E., Felson, M.: Social change and crime rate trends: A routine

activity approach. American Sociological Review 44(4), 588-608 (1979).
18. Kindberg, T., Spasojevic, M., Fleck, R., Sellen, A.: The ubiquitous camera: An in-depth study of camera phone use. IEEE Pervasive Computing, 4(2), 42–50 (2005).
19. Thakur, A., Gormish, M., Erol, B.: Mobile phones and information capture in the workplace. CHI Extended Abstracts on Human Factors in Computing Systems, 1513–1518 (2011).
20. Brown, B. A., Sellen, A. J., O'hara, K. P.: A diary study of information capture in working life. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 438–445 (2000).
21. Mohadis, H. M., Ali, N. M.: Smartphone application for physical activity
22. enhancement at workplace: Would office workers actually use it? In: Proceedings of 3rd International Conference on Information and Communication Technology for the Muslim World (ICT4M), pp. 144–149 (2018).
23. Venkatesh, V., Thong, J. Y., Xu, X.: Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly 36(1), 157–178 (2012).
24. Karlson, A. K., Meyers, B. R., Jacobs, A., Johns, P., Kane, S. K.: Working overtime: patterns of smartphone and PC usage in the day of an Information worker. In: Proceedings of the 7th International Conference on Pervasive Computing, pp. 398-405, Springer,Verlag, (2009).
25. Wang, Y., Wei, J., Vangury, K.: Bring your own device security issues and challenges. In: Proceedings of the IEEE 11th Consumer Communications and Networking Conference (CCNC), pp. 80–85 (2014).
26. Shaikh, A.: Shadow-IT system and insider threat: An assessment of an opportunity dimension for the Identity theft. In: Proceedings of International Conference on Human-Computer Interaction, pp. 314–317. Springer, USA (2018).
27. Felson, M.: Those who discourage crime. In: J.E. Eck and D. Weisburd (eds.) Crime and place 1995, vol. 4, pp. 53-66. Crime Prevention Studies. Monsey, Criminal Justice Press, NY (1995).
28. Felson, M.: Crime and Nature. Thousand Oaks, CA: Sage, pp. 80 (2006).
29. Leukfeldt, E. R., Yar, M.: Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior 37(3), 263-280 (2016).
30. Geer, D.: Six key areas of investment for the science of cyber security. The Futurist 49(1), 10–15 (2015).
31. Hollis-Peel, M. E., Reynald, D. M., Welsh, B. C.: Guardianship and crime: An international comparative study of guardianship in action. Crime, Law and Social Change 58(1), 1-14 (2012).
32. Tseloni, A., Wittebrood, K., Farrell, G., Pease, K.: Burglary victimization in England and Wales, the Unites States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories, British Journal of Criminology (44), 66-91 (2004).
33. Yar, M.: The novelty of cyber crime: An assessment in light of routine activity theory, European Society of Criminology (2), 407-427 (2005).
34. Williams, L.M., Levi, M., Burnap, P., Gundur, R.V.: Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. Deviant Behavior, 1-13 (2018).
35. Jouini, M., Rabai, L. B. A., Aissa, A. B.: Classification of security threats in information systems. Procedia Computer Science 32, 489-496 (2014).
36. Nostro, N., Ceccarelli, A., Bondavalli, A., Brancati, F.: A methodology and supporting techniques for the quantitative assessment of insider threats. In: Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing, pp. 3 (2013).
37. Siponen, A., Vance, A.: Guidelines for improving the contextual relevance of field surveys. The case of information security policy violations. European Journal of Information Systems 23, 289–305 (2014).

38. Silowash, G. J., Cappelli, D. M., Moore, A. P., Trzeciak, R. F., Shimeall, T., Flynn, L.: Common sense guide to mitigating insider threats. Software Engineering Institute, USA (2012).
39. Trevino, L., Victor, B.: Peer reporting of unethical behavior: A social context perspective. Academy of Management Journal 35, 38–64 (1992).
40. Chin, W. W.: How to write up and report PLS analyses. In Handbook of partial least squares, pp. 655-690. Springer, Berlin, Heidelberg (2010).