Workarounds as Means to Identify Insider Threats to Information Systems Security

Pierre-Emmanuel Arduin, Dragos Vieru

Workarounds as Means to Identify Insider Threats to Information Systems Security

Emergent Research Forum (ERF) Paper

Pierre-Emmanuel Arduin
Université Paris-Dauphine
pierre-emmanuel.arduin@dauphine.fr

Dragos Vieru
TELUQ University
dragos.vieru@teluq.ca

Abstract

Workarounds represent deliberate actions of employees in contrast with the prescribed practices and organizations generally perceive them as unwanted processes. Workarounds may lead to information systems (IS) security policy violations, notably when prescribed practices lead employees to face obstacles in accomplishing their daily tasks. Such behavior generates new insider threats to IS security. In this article, we adopt the view that workarounds may enable the identification of new security threats. We propose a conceptual model that illustrates how workarounds generating non-malicious security violations might constitute sources of knowledge about new security threats.

Keywords: Workarounds, Insider threat, Security policy, Non-malicious security violation

Introduction

Information systems (IS) security is an important and complex organizational issue, and the implementation of the technical component is only part of an effective information security strategy. An efficient technological infrastructure provides a technical environment within which security is achievable; however, when an IS goes into production, its appropriation by users introduces possible changes, some favorable and some harmful to the system, that cannot be entirely taken into consideration during the design of the system. In this context, IS literature suggests that while during the last decade organizational employees have become more technology savvy, risk of attacks, especially those emerging from the inside, continued to grow (Röder et al., 2014; Silic and Back, 2014). According to Cybersecurity Ventures, a cyber economy research firm, global annual cybercrime costs will raise from $3 trillion in 2015 to $6 trillion in 2021 (Morgan, 2016). In general, literature on IS security takes into consideration both internal and external sources as threats to information security. However, more recently, Willison and Warkentin (2013) emphasize intentional insider threats as the main source of information access security breaches. Organizational security policies often are elaborated without sufficiently taking in to account their impact on employees' ways of performing their daily task. Security systems contain not only technical components, they also need to enable and encourage user cooperation that plays a critical role in providing efficient organizational security. Security systems design needs to consider the relationships between people, processes, and technology (Silic and Back, 2014). Where conflict exists between security systems and productive tasks, user resistance emerges (Pfleeger and Pfleeger, 2002). In this type of situations, users will most likely engage in security workarounds development by taking advantage of IS flexibility to bypass system's functionalities (Pavlou and El Sawy, 2010). According to Alter (2014), workarounds are situations in which actors will either enable or intentionally perform actions going against one or more routines, norms or expectations in order to overcome a technical or an organizational constraint. For some authors, the workarounds are inevitable within organizations (Suchman, 2007; György et al., 2012).

In the workplace, workarounds are studied as favorable or unfavorable phenomena. On one hand, the unfavorable camp perceives workarounds as violating and resisting the intentions, expectations and business process activities (Röder et al., 2014). On the other hand, the favorable camp suggests the

workarounds as essential sources to analyze and learn policies, procedures and issues (Alter, 2014). We consider that some workarounds will generate new insider threats to information systems security. Such threats may be regarded as unfavorable phenomena, as they violate the information systems security policy in place. Nevertheless, we argue that, as workarounds are inevitable, organizations may use them to identify these new threats to IS security.

To our best knowledge, research on workarounds, seen as sources of new knowledge on IS security, is rather scarce and has focused primarily on identifying factors that may lead to the enactment of a workaround or that might predict the intention to enact a workaround (Chua et al., 2014; Johnson, 2013). Therefore, this work-in-progress study suggests that specific workarounds and related resulting potential new insider threats may be regarded as favorable phenomena. We adopt the view that workarounds in the workplace contain useful, yet unknown knowledge that can assist organizations in their analyses, learning and improvements of work routines and policies (Alter, 2014). Representing a theory-building effort, we concentrate less on a complete review of the extant literature and put more emphasis on theoretical development (Rivard, 2014). To do so, we engage in theory development and propose a conceptual model to answer the following question: *How can knowledge generated by employees' workarounds may help identify insider threats to IS security?*

Next section presents the study's theoretical foundations. Then, we introduce and describe the conceptual model. At the end we provide conclusions and future directions for this research-in-progress study.

Theoretical Foundations: From Workarounds to Insider Threats

A workaround represents a goal-driven change to an existing work system in order to overcome a technical or an organizational constraint (Röder et al., 2014). The persistence of workarounds in a work environment is explained by the need for balance between bottom-up constraints (operationalization of the daily tasks) and top-down pressures (regulatory entities, physical constraints) (Azad and King, 2012). Workarounds often introduce security vulnerabilities as a side effect (e.g., using the same password to access both professional and private accounts). Sometimes, managers may tacitly approve workarounds if secondary tasks (such as security) stand in the way of business continuity (Röder et al., 2014). Balancing the demands of productive tasks and security tasks leads to cost-benefit dilemmas in which employees are forced to choose between security and productivity. Thus, organizational challenges and dilemmas are due to a combination of different perspectives on workarounds. These perspectives are comprised of the ability to operate despite the obstacles, adopt an interpretative flexibility, balance between personal, group, organizational and authorized interests and learning emerging changes. Workarounds in the workplace are considered as favorable or unfavorable phenomena. On one hand, the favorable camp suggests the workarounds represent a problem-solving strategy inspired by external sources (e.g., social networking, website) or discoveries (e.g., index, trial-and-error) (Alter, 2014). In this perspective, workarounds are presented as creative acts and sources of future improvements. For example, workarounds can be essential sources to analyze and learn policies and procedures, or enable positive resistance by ensuring the continuity of a work task (Campbell, 2012).

On the other hand, the unfavorable camp perceives workarounds as violating and resisting the business process norms (Boudreau and Robey, 2005) and security policies constraints (Pfleeger and Pfleeger, 2002). Thus, the main assumption of this perspective is that employees tend to resist top-down pressure due to conflicting goals. Moreover, even if some workarounds may be effective for certain tasks or quality of work the negative outlook seeks the adverse effects of these same workarounds, such as the costs in terms of time, loss of opportunity, and operations (e.g., maintaining ghost systems, non-reliable sources of information). Thus, the outcomes of workarounds may either offer value to the organization or may lead to a risk. Beneficial workarounds involve possible innovation, such as identifying the strengths and weaknesses of a security system which would reflect on the effectiveness of the related implemented security policies.

Defining an IS security policy is a crucial task that requires to be aware of users' behavior within organizations (Silic and Back, 2014). According Willison and Warkentin (2013) employees' violations of IS security policy can be categorized in: 1. non-intentional: mistakes committed by careless or inexperienced employees, e.g. input errors, accidental deletions of sensitive data; 2. intentional but not malicious: deliberate actions realized by employees obtaining a personal benefit with no intention to

harm, e.g. postponing backups, non-robust password choices, leaving doors open before a sensitive discussion; and 3. intentional and malicious: deliberate actions realized by employees with the intention to harm, e.g. sharing sensitive data, introducing malwares. While existing IS security studies have addressed how non-intentional or intentional and malicious violations of IS security policy occur, we argue that workarounds may generate intentional and non-malicious IS security policy violations. This study proposes to study such violations.

Non-malicious insider threats may be regarded as violations of IS security policies with benevolent intentions, notably when they are overcoming a technical or an organizational constraint through workarounds. In addition, security that overburdens employees and is not aligned with their practices can become less effective (Johnson, 2013). While security is presented to employees as being for their own good, it can introduce externalities, burdening the individual with indirect costs (e.g., having to use multiple authentication methods – password and biometric – in a successive manner) (Willison and Warkentin, 2013). Employees may rationally, perceive the personal cost of compliance as being greater than the gained security benefits. In this situation, IS users might engage in workarounds. The problem here is that almost no organization evaluates whether these IS security policies are fit-for-purpose in the real working environment, i.e. do not lead employees to engage in workarounds (Beautement et al., 2016). The increasing complexity of security threats makes it difficult to anticipate, define and communicate all desired policy-compliant behaviors for all potential exceptions and circumstances, even if concepts such as information security awareness aim at changing individuals work habits towards engaging in secure information practices (Tsohou et al., 2015). Thus, the traditional, centralized "command and control" approach to security becomes problematic (Willison and Warkentin, 2013), and IS managers need to rethink how information security is designed, implemented and managed (Silic and Back, 2014).

Conceptual Model: Workarounds as source of knowledge on how to improve security policies

Our three theoretical building blocks are Alter's (2014) theory of workarounds, Guo et al.'s (2011) taxonomy of non-malicious security violations, and McElroy's (2000) knowledge lifecycle model. Workarounds are developed by employees who do not willfully disregard security, but by necessity, in order to effectively perform their daily tasks. Drawing on McElroy's (2000) model based on the interplay between the individual and the organizational knowledge, we conjecture that a workaround solution on the part of an employee becomes an input for an organization knowledge base. Thus, workarounds produced by the user can yield a result that is associated with a new experience. The result and the experience of the employee will eventually become a part of the process of production of knowledge to create new or improve existing IS security policies. Rather than remaining passive, employees who have their own understanding of security, develop workarounds as novel solutions for a more adequate security system. Non-malicious security violations are defined as "the behaviors engaged in by end users who knowingly violate organizational IS security policies without malicious intents to cause damage" (Guo et al., 2011, p. 205). In a workaround context, security violations are not only non-malicious, but also intentional.

Figure 1 presents our conceptual model where workarounds are regarded through the four characteristics of non-malicious security violations according to Guo et al. (2011): (1) intentional behaviors; (2) self-benefiting without malicious intent; (3) voluntary rule-breaking; and (4) possibly causing damage or security risk. These workarounds characteristics highlight how they may impact (possible threats) IS security (arrow A in Figure 1). In a recurrent manner, we suggest that security rules may create the premises of workarounds (arrow B in Figure 1). Indeed, business processes provide work norms to employees within organizations. Norms-based security policies will lead to constraints in users' access to an IS. In this context, workarounds will arise and generate potential new security threats. We analyze workarounds through the lens of the four characteristics of non-malicious security violations introduced by Guo et al. (2011). The first two characteristics (intentionality and self-benefit without malicious intent) refine the ways workarounds might be regarded within organizations: as being based on intentional, non-malicious and ethical behaviors. The last two characteristics (voluntary rule-breaking and possibly causing damage or security risk) highlight how workarounds might generate knowledge on new threats to IS security: business process norms are violated and the perceived security risk is low. Such new

generated knowledge - on how employees were capable to work around the company's security policy -, will be valuable in refining the implemented IS security policies.

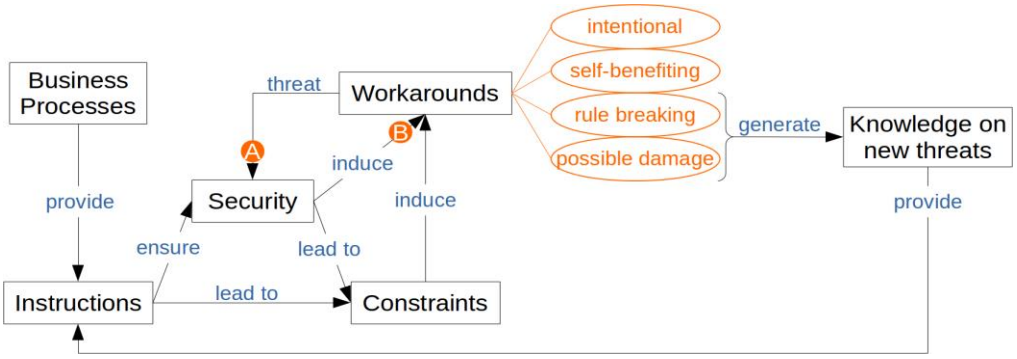

Figure 1. Workarounds, new knowledge, insider threats and security policy

Intentionality. Workarounds are intentional and employees make conscious decisions that lead them to *intentionally* engage in workarounds. This characteristic avoids considering non-intentional security violations such as input errors, but covers malicious security violations, such as sensitive data sharing, as well as non-malicious security violations that occur via workarounds, such as postponing backups. Thus, in terms of new potential security threats created and identifiable through workarounds, the "intentional" characteristic does not clearly differentiate malicious and non-malicious behaviors.

Self-benefit without malicious intent. Workarounds arise in order to overcome a technical or an organizational constraint. For example, employees are seeking self-benefit in their everyday working activities. According to Guo et al. (2011), employees engaging in non-malicious security violations not only, (1) do not have malicious intent to harm the security or business operations, but they also, (2) do not realize unethical self-benefiting actions at the enterprise's expense, such as stealing and selling company information for personal profit. Therefore, in terms of new potential security threats created and identifiable through workarounds, the "self-benefit without malicious intent" characteristic highlights threats that are not subject to legal prosecution.

Voluntary rule breaking. By creating and using workarounds employees violate business processes norms. Even if such norms are mandatory, as discussed in the two firsts characteristics, employees may intentionally violate them for their own benefit but without malicious intent. Thus, in terms of new potential security threats created and identifiable through workarounds, we argue that "voluntary rule breaking" characteristic will eventually generate knowledge on new potential security threats that will occur due to workarounds. This knowledge will help IS security professionals to design more efficient security policies.

Possibly causing damage or security risk. Workarounds, as violations of business processes norms, may engender damages or security risks. When employees perceive low security risks, they will be more likely engage in workarounds that are difficult to deter (D'Arcy et al., 2012). Thus, in terms of new potential security threats created and identifiable through workarounds, the "possibly causing damage or security risk" characteristic emphasizes that new threats will be intentional and non-malicious. This aspect must be taken into consideration when designing IS security policies.

Conclusions and Future Empirical Research Directions

This study contributes to the literatures on IS security and on knowledge management in that it begins to provide a theoretical structuring of how workarounds can be seen as sources of valuable knowledge on security threats. While Alter's theory of workarounds is extremely useful in structuring workarounds, this ERF paper proposes a dynamic explanation of the link between workarounds generated knowledge and IS security policies as a first step for addressing an important yet understudied topic in the literature (Spierings et al., 2016). In order to empirically validate our model, the next step will be to test our model in two different organizations. We adopt an explanatory theory-building-from-cases approach (Eisenhardt, 1989). Thus, we anchor our problem definition and preliminary construct specification in

extant literature and we craft our data collection instruments and protocols, following a deductive pattern. This will be followed, after our entry in the field, by a "flexible and opportunistic" (Eisenhardt, 1989, p. 533) data collection approach, and a within-case and cross-case data analysis, which are inductive in nature. We expect that empirically testing this model will result in a clearer picture of the underlying dynamics of workarounds in the context of IS security policies, thus providing an initial basis to encourage further research on this topic.

REFERENCES

Alter, S. 2014. "Theory of workarounds," *Communications of the Association for Information Systems,* (34), pp. 1041-1066.

Azad, B., and King, N. 2012. "Institutionalized computer workaround practices in a Mediterranean country: An examination of two organizations," *European Journal of Information Systems*, 21(4), pp. 358-372.

Beautement, A., Becker, I., Parkin, S., Krol, K, and Sasse, S. 2016. "Productive Security: A scalable methodology for analyzing employee security behaviors," *SOUPS*, Denver, CO.

Boudreau, M.-C., and Robey, D., 2005. "Enacting integrated information technology: A Human Agency Perspective", *Organization Science*, (16:1), pp. 3-18.

Campbell, D. 2012. "Public managers in integrated services collaboratives: What works is workarounds," *Public Administration Review*, (72:5), pp. 721-730.

Chua, C., Storey, V., and Chen, L. 2014. "Central IT or shadow IT? Factors shaping users' decision to go rogue with IT," *ICIS*, Auckland, New Zealand.

D'Arcy, J., Herath, T., and Shoss, M. 2014. "Understanding employee responses to stressful information security requirements: a coping perspective," *Journal of Management Information Systems*, (31:2), pp. 285–318.

Eisenhardt, K. M. 1989. "Building Theories from Case Study Research," *Academy of Management Review*, (14:4), pp. 532-550.

Gregor, S. 2006. "The nature of theory in information systems," *MIS Quarterly* (30:3), pp. 611-642.

György, A., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the shadows: IT governance approaches to user-driven innovation," *ECIS*, Barcelona, Spain.

Guo, K. H., Yuan, Y., Archer, N.P., and Connelly, C.E. 2011. "Understanding non-malicious security violations in the workplace: a composite behavior model," *Journal of Management Information Systems*, (28:2), pp. 203–236.

Johnson, S. 2013. "Bringing IT out of the shadows," *Network Security* (12), pp. 5-6.

McElroy, M. W. 2000. "Integrating complexity theory, knowledge management and organizational learning," *Journal of Knowledge Management*, (4:3), pp. 195-203.

Morgan, S. 2016. "2016 Cybercrime report," (online) http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, page retrieved on April 20, 2017.

Pavlou, P.A., and El Sawy, O.A. 2010. "The "Third hand": IT-enabled competitive advantage in turbulence through improvisational capabilities," *Information Systems Research* (21:3), pp. 443-471.

Pfleeger, C. P., and Pfleeger, S. L. 2002. *Security in computing*. Prentice Hall Professional Technical Reference.

Rivard, S. 2014. "Editor's comments: the ions of theory construction," *MIS Quarterly* (38:2), pp. iii-xiv.

Röder, N., Wiesche, M., and Schermann, M. 2014. "A situational perspective on workarounds in IT-enabled business processes: A multiple case study," *ECIS*, Tel Aviv, Israel.

Silic, M, and Back, A. 2014. "Shadow IT – A view from behind the curtain," *Computers and Security*, (45), pp. 274-283.

Spierings, A., Kerr, D., and Houghton, L. 2016. "Issues that support the creation of ICT workarounds: towards a theoretical understanding of feral information systems," *Information Systems Journal*.

Suchman, L. 2007. *Human-Machine Reconfigurations: Plans and Situated Actions*, Cambridge University Press.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2015. "Managing the introduction of information security awareness programs in organizations," *European Journal of Information Systems*, (24:1), pp. 38-58.

Willison R. and Warkentin M. 2013. "Beyond deterrence: An expanded view of employee computer abuse," *MIS Quarterly*, (37:1), pp. 1-20.