5-5-2022

A Preliminary Look at Information Security through a Social Practice Theory Lens

Alaa Nehme
Mississippi State University, a.nehme@msstate.edu

Merrill Warkentin
Mississippi State University, m.warkentin@msstate.edu

A Preliminary Look at Information Security through a Social Practice Theory Lens

Alaa Nehme
Mississippi State University
a.nehme@msstate.edu

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

ABSTRACT

The literature has mainly focused on examining information security behavior at the individual level. However, information security practice incorporates structural elements and as such may be explored as a social practice. In a preliminary step, we briefly review theories of social practice and explore information security as a social practice. We derive three propositions related to (1) the three elements of materials, competences, and meanings, (2) the relation of information security with other practices, and (3) the necessity of retaining practice "hosts." We briefly discuss the potential implications of this work.

Keywords

Information security, social practice, insider threat, security behavior.

INTRODUCTION

Cyber threats have proven to constitute a serious challenge to societies, organizations, and individuals. While technical security solutions have been developed to counter these threats in different domain applications, they have been limited in their capacity to stay ahead of cybercriminals who prey upon individuals' maladaptive security behaviors and actions. End-users remain the weakest link in the information security chain, and human actions introduce significant vulnerabilities to the workplace.

The human factor in cybersecurity has drawn IS researchers' attention in recent years (e.g., Nehme and George, 2020; Warkentin, Walden, Johnston, & Straub, 2016; Warkentin and Willison, 2009). Extant studies have examined the factors that affect individuals' (mal)adaptive security behaviors in individual and organization contexts by using different behavioral theories (e.g., Nehme and George 2018). Example theories include but are not limited to Protection Motivation Theory (PMT; Rogers 1975), Deterrence Theory (DT; Gibbs 1975), and Neutralization Theory (NT; Sykes and Matza 1957). The application of these theories in the information security context has indeed enhanced our understanding as to what motivates home and organizational users to take security precautions and comply with information security policies, respectively. Nonetheless, our understanding remains limited to the individual level as these theories (and the information security empirical studies that employ them) take 'individuals' (i.e., the user) as the unit of analysis, whereas cybersecurity incorporates social structural elements. Social interactions, whether explicit or implicit, embody security dimensions that transcend individual phenomena and encompass data sharing (Menard et al. 2014), online process sharing (Trinkle et al. 2014), and financial exchanges (Lee et al. 2004).

Consider Distributed Denial of Service (DDoS) cyberattacks that exploit IoT (connected) consumer devices and employ them in botnets to carry out malicious activities (e.g., disrupt Internet platforms and websites, disseminate malware, etc.). For such attacks to take place, they require a set of different security vulnerabilities to exist across space and time. These vulnerabilities may include user behavioral deficiencies (e.g., when users do not take the necessary security precautions to protect their devices from being hacked), technical and design vulnerabilities, and control vulnerabilities (e.g., the lack of regulatory policies). Here, the interrelatedness of these different structural elements allows the cyberattack to take place. This warrants examining information security at a *social level*, and not only at the individual-level. To that end, we turn to social practice theories, which unlike the theories used in the extant information security literature (i.e., PMT, DT, NT, etc.) take social structure into account and take entities as the unit of analysis, as opposed to individuals.

The present paper is an emergent research work (or a work in process). We first provide a brief overview of social practice theories. Then, we analyze information security as a social practice and derive several propositions. We conclude with a brief discussion of this work's potential implications and contributions.

THEORIES OF SOCIAL PRACTICE

Social practice theories have been examined across different disciplines and streams of research, such as energy consumption, transport, and linguistics. Most relevant to this paper is the use of these theories in Information Systems (for a comprehensive review, see Jones and Karsten, 2008). Traditionally, theories of social practice in IS have mainly concentered around the 'socio-material' role of the technology in organizations (e.g., Kellogg, Orlikowski, and Yates, 2006; Orlikowski, 2000; Orlikowski and Scott, 2008; Suchman, Blomberg, Orr, and Trigg, 1999). Recently, however, IS research has examined non-organizational IT practices and information public goods, such as open source development, from a social practice theoretical lens (e.g., von Krogh, Haefliger, Spaeth, and Wallin, 2012). Also, very recent research in the information security context has begun to consider social practice theory (e.g., Andersson, Hedstrom, and Karlsson, forthcoming). Along the same course, this paper considers the outcome of information security, which like open source software is essentially a public/social good, as a process that reflects social practice.

Theories of social practice manifest an effort toward resolving the structure-agency dualism in social systems, and as such promote social order and change (Bourdieu 1990; Giddens 1984). One such theory, the theory of structuration, describes social systems as systems exhibiting structural properties, as opposed to having embedded structures (Giddens 1984). Structuration considers structure and agency to be "co-constitutive" (Brock, Carrigan, and Scambler, 2016), to consist of a set of social practices executed by "knowledgeable human agents," and as such to establish the "structural properties" of societies (Giddens 1984, 1991). Central to structuration is the instantiation of practice by actions (i.e., "doing" or "performance"). Bourdieu's thesis of practice also accentuates actions (Schatzki 1997). The framework considers social practice as a function of habitus (i.e., a system of permanent dispositions, schemata, perceptions, conceptions, and actions) and field (i.e., a structure or hierarchy of social positions), wherein both are inter-related. This inter-relation is generated and governed by the following process: (1) conditions in the field generate dispositions, (2) dispositions produce activities and (3) "interwoven activities" form practices executed in the field. Both theories (i.e., Giddens' and Bourdieu's) consider that practices are perpetual (i.e., have "space-time extension") and that a structure is the "medium and result" of practices (Schatzki 1997). Despite the theories' dominance in social practice research, they have been criticized for their limitations.

The limitations of the theory of structuration include: (1) its lack of temporality, which arguably renders it unsuccessful in explaining or inducing social change (Archer 1996, 1982), (2) its limited scope of empirical application (Archer 1982; Schatzki 1997), and (3) its sensitivity to the assumption that human agents have the required knowledge and power to carry out social practice (Adams 2006). Similarly, the theoretical account of field and habitus is limited in that it overemphasizes individuals' attributes (i.e., habitus). Additionally, both theories are criticized for ignoring the role of non-human agents (i.e., materials), such as technologies (Reckwitz 2002a). Given these limitations, extensions of Giddens' and Bourdieu's theoretical accounts have emerged with a unique focus on analyzing practice as an entity, as opposed to an individual's outcome of knowledge and habitus.

Contemporary theories of social practice address those limitations through describing practice as an entity of interrelated elements (Reckwitz 2002b; Shove et al. 2012). These elements include the following: (1) materials, (2) meanings, and (3) competences (Shove et al. 2012). Materials refer to the objects, tools, goods, and infrastructure involved in a practice. Meanings refer to shared social understandings of a practice, its societal significance, and its outcome experiences. Competences refer to skills, practical know-how, and understandings of performance (i.e., performing the practice). Fundamental to this view of social practice is the distinction between performance and entity. Performance represents momentary observable behavior, whereas the three entity elements underpin the performance. Through identifying those underpinnings, recent theories have facilitated the empirical study and prediction of practice and social change (Shove et al. 2012; Warde 2005).

In addition to identifying the three elements of social practice, contemporary theories highlight the interdependency characteristics of practices, through which they interact (Schatzki 2002). Interdependent practices form "bundles" (i.e., complex systems) that underlie the spatiotemporal aspect of social change. On that basis, relations within bundles harmonize or conflict, and as such bundles co-evolve (Schatzki 2002). Thereby, "trajectories" of practices affect each other and impact people's everyday life. In turn, people also affect these trajectories. In that sense, practices' survival depends on the recruitment and retention of human actors, who in turn reshape them (Shove et al. 2012). This implies that a practice may only survive by its "carriers," or "hosts," also referred to as "practitioners" (Reckwitz 2002b).

INFORMATION SECURITY AS A SOCIAL PRACTICE

Information security has drawn the attention of researchers, industry players, and government agencies, each of whom have influenced society in one form or another. Recently however, information security has increasingly been recognized as an integral part of society. It is important to note that information security is not only an end in itself, but rather it is practiced for attaining safer computing. Thereby, the practice of information security lies within a broader social practice, which is social

computing. In that sense, information security practice is not a cause or effect of social systems but a prominent component of social computing.

As previously discussed, social practices do not only involve human agents but also incorporate what is termed the "missing masses" of artifacts, devices, and infrastructures (Latour 1992; also referred to as "material arrangements," Schatzki 2010). Information security practice comprises the following materials among others: secure infrastructures, secure devices, and secure software/applications. The set of materials involved differ with each of the different structural components mentioned in the introduction (i.e., behavioral (user), technical (design), and control). Competences in the practice of information security involve the skills and knowledge of securing information artifacts at the control, design, and use levels. For instance, users' competences include (but are not limited to) knowing how to update their mobile applications and changing default device credentials. Meanings complement competences by integrating the 'know-why' rather than the 'know-how.' They include understanding why information security is essential in terms of protection against cybercrime and insider threats.

From a social practice theory perspective, information security is an entity of the three interrelated elements of materials, competences and meanings. Thus, as a practice, it is only fulfilled if all elements are present. For instance, taking the necessary behavioral measures to secure an information artifact (i.e., competence) would be insufficient in the absence of security patches or a secure design that may conform to security standards (i.e., materials).

Proposition 1: The absence of any of the three elements (i.e., materials, competences, and meanings) disrupts information security as a social practice.

From a social practice theory lens, a practice entity does not persist in separation of other practices. As a social practice, information security is interconnected with other practices, such as adopting the technology at the use phase, innovating (convenient) IT artifacts in the design phase, and releasing trade policies in the control phase. As such, information security depends on other related social practices. These dependencies form a bundle that evolves and impact social order across time and space. For instance, information security practice by home users would be negatively affected by a high level of sub-optimal application security development, or adequate compliance by employees would be inadequate with an insufficient push of software patches from the vendor, etc.

Proposition 2: As a social practice, information security belongs to a bundle of practices. The focus on its elements, comprising materials, meanings, and competences, independent of its relations with other bundles of entities (i.e., social practices) is insufficient.

The relationships within the bundle are generated and maintained by information security "practitioners" (i.e., people who perform security practice). The survival of information security practice depends on its carriers (i.e., practitioners). By substitution, its survival depends on its capacity for recruiting and retaining carriers. This capacity is a function of the preset conditions and available resources that practitioners act by and use respectively (Reckwitz 2002b). In the information security context, conditions may include policies, and resources may include users' access to security knowledge and information.

Proposition 3: The provision of the necessary requisites (i.e., conditions and resources) enhances the capacity of information security practice to recruit and retain practitioners (i.e., hosts, or carriers of the practice).

In sum, from a social practice theory lens, information security as a social practice engages social structure and agents. The elements of information security practice include secure artifacts, platforms, and infrastructure (i.e., materials), information security knowledge and skills (i.e., competences), and information security comprehension (i.e., meanings). The absence of any of three elements puts the practice at risk. The entity, comprised of the three elements, does not exist independently. Rather, it is a constituent of a larger network of social practices, such as policy development and technology design. The practice's survival depends on the retention of its practitioners. The process of retention is dependent on the provision of resources and conditions that facilitate 'hosting' the practice. Therefore, as proposed by the contemporary theories of social practice (Reckwitz 2002b; Shove et al. 2012), information security practice is a unit of analysis. Examining information security practice as a unit of analysis complements other inquiries that focus on individuals as the unit of analysis.

CONCLUSION

In this work, we have taken into account the social structure incorporated into information security. On that basis, we have deviated from looking at security at the individual (user) level with the individual as the unit of analysis. We have turned to social practice theory and have derived several propositions about information security as a social practice. As this work continues, it may have far-reaching research implications and contributions considering that it looks at a new dimension of information security, whereas the literature is largely restricted to the individual level by which the behavioral component of

information security is examined. A main potential implication we may reach is that users' information security behavior is not only an outcome of individual choice but also a function of social structure and change.

REFERENCES

1. Adams, M. 2006. "Hybridizing Habitus and Reflexivity: Towards an Understanding of Contemporary Identity?," *Sociology,* 40, 3, 511–528.
2. Archer, M. 1996. "Social Integration and System Integration: Developing the Distinction," *Sociology*, 30, 4, 679–699.
3. Archer, M. S. 1982. "Morphogenesis Versus Structuration: On Combining Structure and Action," *The British Journal of Sociology,* 33:4, 455–483.
4. Bourdieu, P. 1990. *The Logic of Practice*, Stanford University Press.
5. Brock, T., Carrigan, and Scambler, G. 2016. "Introduction," in *Structure, Culture and Agency: Selected Papers of Margaret Archer*, Routledge.
6. Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence.*, New York: Elsevier.
7. Giddens, A. 1984. "The Constitution of Society: Outline of the Structuration Theory," *Cambridge: Polity*.
8. Giddens, A. 1991. "Structuration Theory: Past, Present and Future," in *Giddens' Theory of Structuration. A Critical Appreciation.*, C. Bryant and D. Jary (eds.), London: Routledge.
9. Jones, M. R., and Karsten, H. 2008. "Giddens's Structuration Theory and Information Systems Research," *MIS Quarterly*, 32, 1, 127–157.
10. Kellogg, K. C., Orlikowski, W. J., and Yates, J. 2006. "Life in the Trading Zone: Structuring Coordination across Boundaries in Postbureaucratic Organizations," *Organization Science,* 17, 1, 22–44.
11. von Krogh, G., Haefliger, S., Spaeth, S., and Wallin, M. W. 2012. "Carrots and Rainbows: Motivation and Social Practice in Open Source Software Development," *MIS Quarterly,* 36, 2, 649–676.
12. Latour, B. 1992. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts," in *Shaping Technology/Building Society: Studies in Sociotechnical Change*, W. E. Bijker and J. Law (eds.), Cambridge, MA: MIT Press, 225–258.
13. Lee, C.-P., Warkentin, M., and Choi, H. 2004. "The Role of Technological and Social Factors on the Adoption of Mobile Payment Technologies," in *Proceedings of the Tenth Americas Conference on Information Systems*, New York, New York, August.
14. Menard, P., Gatlin, R., and Warkentin, M. 2014. "Threat Protection and Convenience: Antecedents of Cloud-Based Data Backup," *Journal of Computer Information Systems*, 55, 1, Taylor & Francis, 83–91.
15. Nehme, A., and George, J. 2020. "Taking It out on IT: A Mechanistic Model of Abusive Supervision and Computer Abuse," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*.
16. Nehme, A., and George, J. F. 2018. "Iterating the Cybernetic Loops in Anti-Phishing Behavior: A Theoretical Integration," in *Proceedings of the 24th Americas Conference on Information Systems (AMCIS)*, New Orleans, LA.
17. Orlikowski, W. J. 2000. "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations," *Organization Science,* 11, 4, 404–428.
18. Orlikowski, W. J., and Scott, S. V. 2008. "Sociomateriality: Challenging the Separation of Technology, Work and Organization," *The Academy of Management Annals*, 2, 433–474.
19. Reckwitz, A. 2002a. "The Status of the 'Material' in Theories of Culture: From 'Social Structure' to 'Artefacts,'" *Journal for the Theory of Social Behaviour,* 32, 2, 195–217.
20. Reckwitz, A. 2002b. "Toward a Theory of Social Practices: A Development in Culturalist Theorizing," *European Journal of Social Theory,* 5, 2, 243–263.
21. Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology,* 91, 1, 93–114.
22. Schatzki, T. R. 1997. "Practices and Actions a Wittgensteinian Critique of Bourdieu and Giddens," *Philosophy of the Social Sciences*, 27, 3, 283–308.
23. Schatzki, T. R. 2002. *The Site of the Social: A Philosophical Account of the Constitution of Social Life and Change*, Pensylvannia: Penn State Press.

24. Shove, E., Pantzar, M., and Watson, M. 2012. *The Dynamics of Social Practice: Everyday Life and How It Changes*, London: Sage.
25. Suchman, L., Blomberg, J., Orr, J. E., and Trigg, R. 1999. "Reconstructing Technologies as Social Practice," *American Behavioral Scientist,* 43, 3, 392–408.
26. Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review,* 22, 6, 664–670.
27. Trinkle, B. S., Crossler, R. E., and Warkentin, M. 2014. "I'm Game, Are You? Reducing Real-World Security Threats by Managing Employee Activity in Online Social Networks," *Journal of Information Systems,* 28, 2, American Accounting Assocation, 307–327.
28. Warde, A. 2005. "Consumption and Theories of Practice," *Journal of Consumer Culture,* 5, 2, 131–153.
29. Warkentin, M., Walden, E., Johnston, A., and Straub, D. 2016. "Neural Correlates of Protection Motivation for Secure IT Behaviors: An FMRI Examination," *Journal of the Association for Information Systems*, 17, 3, 194–215. (https://doi.org/10.17705/1jais.00424).
30. Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems,* 18, 2, Taylor & Francis, 101–105.