The Practice Turn in IT security – An Interdisciplinary Approach

Laura Kocksch[1] Andreas Poller[2]

Abstract: IT security has traditionally been approached as an isolated technological phenomenon or as a matter of user incompetency. In our work, we suggest to apply a practice turn to the study of IT security to unfold the nexus of practices that is involved in engaging with IT security work. In doing so, IT security becomes an organizational, social and political phenomena that demands interdisciplinary attention from computer science and social science alike.

Keywords: IT security; social science; practice; organization

IT security has traditionally been perceived as a matter of technological precision and function. Recent events have demonstrated the effects of insecure IT systems for organizations, businesses and society as a whole. Hacks are socially and politically motivated and solely technological explanations do not suffice.

Because of its vital role, IT security is studied in computer science and engineering but also in interdisciplinary collaborations. For instance computer scientists and psychologists test technological security measures for their compliance with users' needs and competencies. While the usability of security measures has been in the focus of attention, recently, scholars have argued developers of software products need to be educated and need to comply too. By the same token, IT security is scripted into legal frameworks, standards are being set up and education resources have developed. We build on this impulse to unpack IT security as more than a technological failure or a question of users and software developers' in-/competency, and argue that we need to gain a broader understanding of what assembles IT security in social practice. To this end, we strive to account for the complex webs of practices that technologies are involved in and that insecurities can have potential effects on.

When turning our attention to the daily practices involved in engaging in security work, we shed light on its ambivalence and messiness. By taking the practice turn, we shift perspectives away from individual actors or social groups to situated actions and the heterogeneous stakeholders involved. We emphasize on the tense negotiation, collaboration and cooperation involved in situated security work, and ask how IT security is constantly enacted, maintained, contested and cared for in dispersed practices.

[1] Ruhr University Bochum, Faculty of Social Science, Universitätsstrasse 150, 44801 Bochum, Germany laura.kocksch@rub.de

[2] Fraunhofer Institute for Secure Information Technology, Rheinstrasse 75, 64285 Darmstadt, Germany, andreas.poller@sit.fraunhofer.de

doi:10.18420/inf2019_12

Practice-theoretical approaches in social science shift the attention to the assemblages of heterogeneous actors that contributed to a given situation. Turning to practice emphasizes on the organizational, social and material constraints of daily life. This turn has not yet been applied to the study of IT security. In doing so, we suggest to describe IT security as distributed across heterogeneous actors; not just individual developers or users.

We exemplify the practice turn in IT security in two empirical cases that we draw from a one-year-study at a large German software vendor in 2016. The first case stresses the *material practice of IT security in organizations* [Po17]. We investigated events in the aftermath of a software penetration test whose results the software developers translated into single defect reports managed by means of an issue tracking system. We realized that the issues themselves had agency. The issues demanded a specific way of taking care of security that complied with the company's business strategy. Had security taken on a different material than issues it could have been introduced more fundamentally in the software product. But as an *issue* it was merely one task to check of a list.

The second case emphasizes the *morality and politics of IT security* [Ko18]. We observed a security training using team-ethnographic methods with a particular focus on the interaction between a security consultant and a team of developers. We soon realized that the team comprised highly trained and expert developers. However, during the training, *bad* programming skills were blamed for the findings of the penetration test. The training session was conceptualized as a one time event that should scare and blame developers, while letting unnoticed the myriad of material, management and collaborative practices that contribute to a software product. IT security was defined as a shortcoming in developers' actions; clearing all other actors in the company of responsibility. The training located security at developer's hand framing political responsibility as an individual software development problem.

By applying the practice lens to the study of IT security in our two examples, we demonstrate that IT security demands *careful* intervention that is sensitive to the situated practices of developers. IT security is an issue for society, business and politics alike, and because of its significance, we suggest that it should not be reduced to isolated actors but acknowledged as a dispersed phenomena, entangled with heterogeneous practices. Further interdisciplinary research between computer scientists and social scientists is needed in this area.

Literaturverzeichnis

[Ko18] Kocksch, Laura; Korn, Matthias; Poller, Andreas; Wagenknecht, Susann: Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. Proc. ACM Hum.-Comput. Interact., 2(CSCW):92:1–92:20, November 2018.

[Po17] Poller, Andreas; Kocksch, Laura; Türpe, Sven; Epp, Felix Anand; Kinder-Kurlanda, Katharina: Can Security Become a Routine?: A Study of Organizational Change in an Agile Software Development Group. In: Proc. CSCW '17. ACM, New York, NY, USA, S. 2489–2503, 2017.