Security Managers Are Not The Enemy Either

Lena Reinfelder
Friedrich-Alexander-Universität Erlangen-Nürnberg
Erlangen, Germany
lena.reinfelder@fau.de

Robert Landwirth
TU Darmstadt/Fraunhofer SIT
Darmstadt, Germany
robert.landwirth@sit.fraunhofer.de

Zinaida Benenson
Friedrich-Alexander-Universität Erlangen-Nürnberg
Erlangen, Germany
zinaida.benenson@fau.de

ABSTRACT

Security managers are leading employees whose decisions shape security measures and thus influence the everyday work of all users in their organizations. To understand how security managers handle user requirements and behavior, we conducted semi-structured interviews with seven security managers from large-scale German companies. Our results indicate that due to the absence of organizational structures that include users into security development processes, security managers unintentionally obtain a negative view on users. Their distrust towards users leads to the creation of technical security measures that cannot be influenced by users in any way. However, as previous research has repeatedly shown, rigid security measures lead to frustration and discouragement of users, and also to creative (but usually insecure) methods of security circumvention. We conclude that in order to break through this vicious cycle, security managers need organizational structures, methods and tools that facilitate systematic feedback from users.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Organizational security; security managers

ACM Reference Format:
Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security Managers Are Not The Enemy Either. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland Uk*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3290605.3300663

CHI 2019, May 4–9, 2019, Glasgow, Scotland Uk

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300663

1 INTRODUCTION

Starting with the seminal work by Adams and Sasse "Users Are Not The Enemy" in 1999 [1], research in human-centered security has often portrayed a tension between leading employees who are responsible for security in organizations (we call them "security managers") and employees whose primary tasks do not involve security (we call them "users"). Since then, a multitude of studies showed that users act insecurely due to the lack of user-centered security rather than out of carelessness or ill will [2, 10, 12, 18, 20, 25, 34]. Accordingly, the negative perception of security by users (the users' side of the above-mentioned "tension") arises from conflicts between the requirements of their primary tasks and unusable security measures. In this work, we are asking the question: *How does this tension arise on the side of security managers, and what are its consequences?*

The main recommendation of the user-centric security research is that users and their working requirements should be considered when developing security measures. But how do security managers think of securing an organization while at the same time considering user needs? How can security managers fulfill their task while being limited in their freedom of action by the organizational and personal context? Security managers' decisions influence all employees in an organization and therefore, understanding how these decisions are shaped is important.

There is little research on security managers' attitudes towards users, how these attitudes arise, and how they influence decisions in security development processes. To investigate the above issues, we conducted semi-structured interviews with seven security managers in large-scale German companies. These companies belong to different industry sectors and cumulatively employ about 680,000 employees for whose security our respondents are responsible.

Our analysis shows that, paraphrasing the title "Users Are Not The Enemy" [1], security managers are not the enemy either. They think and act within their scope that is mainly shaped by the organizational structures in place. As these structures do not include users into the security development process and promote a negative view on users, the resulting security measures, although created with good intentions, become unusable.

2 BACKGROUND

Prior research on user-centered security in organizations has mostly focused on how users perceive and interact with security measures [1, 12, 25, 27–29], how they can be motivated to comply [24, 35–37], on factors influencing compliance [14, 28], as well as advice for security managers on how to implement security in organizations [9, 19, 31, 33]. However, there exists much less research regarding security managers' approaches to developing and implementing security in organizations.

The existing research can be roughly classified into learning about security managers and helping them. In this section we focus on what we know about security managers' attitudes to the users and to the usability and effectiveness of security, as this is the topic of our study. In the "Implications" section we connect our findings to the literature that discusses how to help security managers in developing user-friendly security.

In the past decade, several works compared security professionals' attitudes to security with those of employees' whose primary tasks lie outside of the security domain [3, 23, 32]. Uniformly, the main finding is that values and security attitudes differ sharply between the two groups. Moreover, both groups seem to know very little about each others' values, views and everyday work realities, a situation that Albrechtsen and Hovden call the "digital divide" [3]. They found that whereas security managers consider users as a security threat and want to control user behavior, the users report that they are willing to protect their organizations, but do not know how, or are hindered by poor usability of security measures and policies.

Posey et al. [32] report very similar results from interviews based on the Protection Motivation Theory. The employees most often mention hackers as a threat, whereas security professionals are most concerned about unintentional employee mistakes. Moreover, an overwhelming majority of the interviewed employees found that the main obstacles to compliance are restrictiveness and difficulty of security measures, but the security professionals greatly underestimated these sources of non-compliance. The security professionals also expressed a desire to control user behavior: "The professionals more than the [users] appear to believe in the effectiveness of authority and enforcement." [32, p. 561].

Hedström et al. [23] also note that information security management is mostly based on a control-based compliance model, meaning that user behavior has to be regulated. Based on the assumption that users and security managers in organizations have different and sometimes conflicting values, the authors propose a value-based compliance model. There, users are part of the security development process and non-compliant behavior is seen as a cause for changing and improving security management.

Although the above research describes the wish of the security professionals to control the users, this issue is not discussed in depth. Our study contributes to this research stream by analyzing how the attitude of control arises.

Another issue uniformly documented in the above research is the predominance of the one-way communication with users, such that they receive security tools, guidelines and policies from security practitioners, but do not have possibilities to give feedback on security measures. Studies that explicitly focus on security professionals document this phenomenon as well.

For example, Botta et al. [13] and Werlinger et al. [38] examine security professionals' tools, activities and interactions. In a case study on how security policies are created, they document that users are not involved in the creation of the policies, but just receive the resulting guidelines and are supposed to comply, although they can also ask for a revision of policies [38]. Thus, the communication with end users is mostly one-way, such that security professionals do not get feedback during the policy development phase.

Ashenden and Sasse [8] conducted five in-depth interviews with Chief Information Security Officers (CISOs) in order to gain insights into the role of CISOs in establishing organizational information security culture. They emphasize that CISOs are unable to effectively communicate with the employees and feel remote from them. Meanwhile, Haney and Lutters [21] assert that communication skills and service orientation are very important for security professionals' successful engagement with users.

We further investigate the engagement of security managers with users. In the following, we show how security managers think about including users into the security development processes, and what are the current impediments to user-centric security development.

3 METHOD

Our empirical analysis is based on interviews with seven IT security managers. Our respondents are leading employees of five large-scale German companies that in total employ about 680,000 employees.[1] As recruiting high-level managers for a study is challenging due to their high workload and poor reachability for outsiders, we used snowball sampling. Three former colleagues put us in touch with security managers of their organizations, who in turn recommended further colleagues from their or other organizations. Table 1 presents details regarding the respondents' industry sector and job

[1]The number of employees is reported cumulatively for the anonymity reasons.

title. All respondents hold a leading position within the IT department of their company.

We conducted exploratory semi-structured interviews using the following open questions:

- How are security goals developed in your company?
- How are security measures developed?
- What is the role of the users in the security development process?

We sent these questions to our participants in advance so that they could familiarize themselves with the topic.

All interviews were conducted by phone, except for one which was conducted personally. Data material included 371 minutes of raw audio data. Audio recordings were transcribed and approved by the respondents. All data were stored and processed in accordance to the German data protection laws. The participants provided an informed consent to the data processing.

Data analysis employed techniques elaborated on by Corbin and Strauss [17]. The interview material was first coded by two researchers independently, creating codes and memos. After a general picture of the data material was established, the findings were discussed, designing a final coding scheme. This coding scheme featured three major categories, which now represent major points of our argument: attitudes, practices and context. The category "attitudes" entailed codes that marked interviewees' attitudes towards various phenomena, such as security, threats, or usability. The category "practices" included codes for descriptions of the way security measures are designed and how the users are implicated in these processes. The codes in the category "context" referred to interviewees' context for action in organizations, i.e., explicit or implicit rules on how things can or have to be done in a specific organization.

After the material was coded, we condensed this material to case descriptions. One case represents one interview. Through joint analysis and discussion, we decided what is most relevant to a case, considering factors such as: the length and degree of detail an interviewee dedicated to a topic, the importance an interviewee assigns to that topic, what we understand from the interview text to be the typical context of actions for this security practitioner. Thus, a case description is a condensed form of the interview, achieved through abstraction. These case descriptions lent the basis to compare the material and led us to our results.

4 FINDINGS

We describe the process of security development in organizations with close attention to the role of users in this process, including the views of the security managers regarding usability, and their understanding of user behavior.

The role of users and usability in the development and evaluation of security measures

None of the companies reportedly include considerations of users' goals and daily workload at the point of conceptual design of security measures, although the importance of usability for security is salient to our participants: *"I've come to believe that a high level of security can only be achieved through a combination of measures which do not restrict usability. And therefore are not perceived as disturbing." (P6)*

While the importance of usability is stressed in the majority of interviews, participants also stated that organizational structures to support the consideration of usability are missing: *"There are no special surveys, which are conducted in advance to assess whether features are suitable for most of the users. The [security] team is making the decisions and is responsible for it." (P4)*

Organizational structures refer to relatively stable rules which would enable security managers to design security in a user-friendly way. The existence of such structures would imply that there are certain methods, for example for requirements engineering, or for getting systematic feedback from the users. These methods might be supported by tools (e.g., an online platform for getting feedback).

Only the company of P5 tried to include users into the development process of security measures as beta testers: *"We have tried [the security solution] in a pilot study to see how [the users] work with it and how satisfied they are." (P5)* User feedback was very negative, such that this security solution was rejected, and the company started looking for a replacement.

In the other cases, however, security measures are tested through regular use: *"There is no official evaluation. But we see it indirectly by receiving all these requests, this means that we see relatively quickly how many users are satisfied or dissatisfied with the security measure." (P1)* We note that P1 implicitly assumes that if the users do not complain, then they are satisfied.

Feedback concerning existing measures is received sporadically and through indirect channels, such as word of mouth, company owned social media or a helpdesk. This feedback is usually negative, e.g., a use case does not work anymore due to new security measures, or an operation takes more time and effort because of new security settings.

Managers feel frustrated and powerless, because they don't know how to account for usability in a systematic way, and there is no organizational support: *"What is now hanging on the walls are posters with "design thinking" [...]. That's why we have this great "security made easy" blah. This is of course always a nice management promise, but how to implement it?" (P6)*

Industry	Job Title	Participant number
Technology Group	Security Manager	P1
Healthcare	Security Manager	P2, P3
Telecommunication	Project Security Manager	P4, P6
Consulting	Senior IT Consultant	P5
Semiconductors	Managing Director	P7

Table 1: Industry sector, position in the IT department of their organization and participant number.

Perception of users by security managers

Knowledge about users is built through observation and is generally based on participants' own interpretation (or the shared understanding between colleagues) of how users act and what users need: *"When I meet my colleagues, I watch how they are using [a system]. How do they act? Then I get a feeling if they ever intend to update their device. Or do I have to educate them?" (P4)*

The perception of users is based on a feeling of distrust, which is rooted in three main ideas:

(1) Corporate security plays a minor role for users: *"The user says: information security again, this is just hindering me." (P2)*
(2) Users act out of self-interest, and the fulfillment of security tasks does not provide any use for them: *"Each individual, whether he admits or not [...], is always going to act in the direction: What's in it for me?" (P6)*
(3) Users act insecurely and are therefore the primary attack vector: *"Out of hundred people there are guaranteed two clicking [on a phishing link]. If I wanted to attack a company, I would take on the user." (P7)*

To summarize, users are broadly viewed as volatile elements, hard to control but in need of control (and education). They are assumed to have objectives different from the organizational goal to secure its information. This difference in goals is a constant, no matter whether the user is described as someone egoistically following their own interest, plain naive or just preoccupied with the successful completion of their daily workload. Users are viewed as fundamentally disinterested in, lacking understanding of or even showing disregard towards organization's security.

Since feedback to security measures received by the managers is indirect, impersonal and negative, the view that the user is someone who makes the creation of security difficult and has no concern for the security objectives of the organization is reinforced.

Coping with user behavior

The feeling of distrust results in the opinion that users have to be monitored and controlled in order to achieve compliant behavior. This goal is reached by implementing technical security measures that allow the security managers to monitor and to actively influence user actions. For example, MDM solutions[2] provide the possibility to check whether employees have changed settings, such as activating debug interfaces: *"Depending on the settings which were changed, [we are able to] wipe all company data from the device, which would be the worst case, or just disable email." (P1)*

Organizational measures (such as guidelines) are perceived as less effective, as compliance with them cannot be enforced. Although not complying with organizational measures can be penalized, this possibility might induce users to conceal their behavior: *"And if the only benefit [from complying with security policies] is to not get a written warning, then they will conceal [their non-compliant behavior]." (P6)*

In summary, users are considered to be fundamentally uncontrollable and might, despite all security measures, still fall into traps set by the attackers. While users show little interest in security measures, those security measures still need to be legitimized. If a security measure is not up to their taste, they will *"man the palisades"* (P6). Thus, users are (not very cooperative) partners in establishing (never fully secure) security measures.

5 IMPLICATIONS

We present a security development cycle that reflects our findings, discuss our results in the light of related work and outline future research directions. Finally, we discuss limitations of our study.

Missing structures lead to negative perception

The interviews indicate that security managers consider users when designing and implementing security measures in an incomplete and indirect way. Users are not included in a structured, organized process, as there are no such structures in place. While security managers recognize the need to provide usable security, they do not know how to do this.

Understanding what exactly makes a security measure usable in the context of an employee's workload is a complex endeavor that requires adequate skills, organizational structures, methods and tools. The organizational production of security we found in our interviews leaves security

[2]MDM means Mobile Device Management, which is a security solution for corporate smartphone usage.

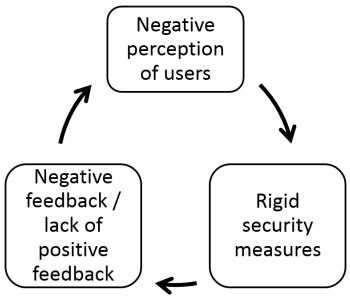

Figure 1: Security development cycle as emerged from the interview analysis

managers to their own devices and necessarily reliant on incomplete information.

We visualize the process of security development as described by the interviewees in Figure 1. When security measures are put in place, managers receive user feedback. As the users are not actively and systematically asked for feedback, this feedback is most likely unstructured and negative, reporting problems and expressing dissatisfaction. When confronted with the negative feedback, security managers perceive users as uninterested in security, and lacking understanding and motivation to behave securely. This negative view on the users results in the wish to control the users as much as possible by means of rigid technical security measures. Those security measures, in consequence, have a negative impact on the effectiveness and efficiency of users' tasks and therefore result in negative feedback.

By unpacking security development process in this way, we highlight how the lack of user feedback is connected to the wish of security professionals to rigidly control user behavior. Although both phenomena, the absence of two-way communication between users and security professionals, and the controlling attitude, are extensively documented in related work [3, 8, 23, 32, 38] (see also the "Background" section), previous work does not make their relation explicit.

Coles-Kemp et al. [16] point out that trust and collaboration are essential for effective security. Thus, the controlling attitude of security professionals, as well as the absence of a dialogue with the users are definitely counter-productive. In the following, we investigate how to break through the vicious cycle described above.

Security as an Organizational Learning Process

We connect our findings to the organizational learning theory by Argyris [4, 5]. According to our analysis, security managers and their organizations seem to be in a single-loop learning situation with regard to security. This situation is characterized by a unilateral definition of security goals through managers. The managers also develop means to achieve the intended goals. If the goals are not achieved, the organization in general and the security managers specifically change their methods in a way that should (hopefully) result in the initial intended goals. Thus, the organizations learn from unintended results (that can comprise security incidents or negative employee feedback) and try to improve their actions, but do not challenge their security objectives.

Development of security measures should become more efficient if the organizations move to double-loop learning which is characterized by going further than just adapting the means and methods. Instead, the organization and the security managers should evaluate whether their security goals are appropriate for achieving the intended consequences. If not, the initial goals have to be changed. Such changes, although they may include major changes in organizational security, are the only possibility to develop effective security.

However, double-loop learning has a non-trivial cost in time, resources and expertise, according to Argyris' account of his lifelong experience with action research on organizational change [6]. At the roots of the double-loop learning model are "valid information, informed choice, and vigilant monitoring of the implementation of the choice in order to detect and correct error" [6, p. 22]. Especially collection of valid information about organizational security and the subsequent monitoring of the implementations can be very resource-consuming. Current research in effective organizational security presented in the next section seems to corroborate this assumption.

Ways of Creating Effective Security

Hedström et al. [23] directly ground their value-based compliance model in the organizational learning theory. They assert that values of security managers, when imposed on employees by means of security policies and measures, constitute for them the "espoused theories", i.e., ideal theories of action that are not followed. The employees, on the other hand, act according to their "theories-in-action" that embed their professional and personal values. For example, in a hospital, the value of providing efficient patient care compels nurses and doctors to write some passwords on the wall, or share accounts with each other. The authors discover value conflicts in the hospital environment through an interview study, several observational studies and three expert panels.

Considering research on developing tools for security managers, Parkin et al. [30] developed and tested mockup prototypes with focus on the management of password composition policies to help security managers to integrate security, usability and an economic perspective on information security policy management. Unfortunately, we are not aware of a real-world tool with similar capabilities. This may be due to the difficulty of populating such tools with realistic and useful data for decision making.

Beautement et al. [9] developed a methodology that helps organizations to assess their security culture including prevailing security attitudes and behavior using interviews and a scenario-based survey. Identifying different user groups can be used to inform targeted interventions, plan further training and thus increase the organizational security level. This approach fits well into the requirement of the double-loop learning for gathering valid information.

Another promising approach for gathering data about ineffective security mechanism is the "shadow security" method by Kirlappos et al. [26]. Through analysis of interviews with around 100 employees in a multinational organization, researchers gather information about workarounds that the employees use when they want to work securely, but the security measures offered by the organization turn out to be unworkable in a particular situation. This method can lead an organization to reconsidering its security processes and co-design them with user participation.

Considering participatory security design, a question arises how to choose employees for the engagement in security feedback and design. One possibility is, according to Becker et al. [11], to find "security champions" in an organization. Using a scenario-based questionnaire developed by Beautement et al. [9], the researchers identify various types of employees who have the potential to be valuable allies in creation of effective security. Those are not only users that blindly follow the security policies, but also those who criticize or circumvent them.

Heath et al. [22] describe a participatory security design process where a system and its security were physically modeled using LEGO. Coles-Kemp [15] describes further techniques for creative security, called "collaborative collage" and "storytelling". All these techniques require a skilled facilitator. They can be used to emgage various stakeholders with different security perspectives and with each others' goals and values.

Ashenden and Lawrence [7] report on the iterative development of a "security dialogues" workshop for security professionals. A workshop comprises three days of intensive training. This endeavor is directed at mitigating the core problem in today security development: it teaches security professionals skills needed to engage with the users.

Research Directions

Current research in effective organizational security provides some excellent examples on how to organize double-loop learning in security. However, the application of these approaches by security managers seems to be beyond their skills and possibilities. Previous research [3, 7, 8] as well as our study show that security practitioners feel rather helpless when they are asked to engage with the users. This is not surprising as, according to the current research presented above, this engagement requires extensive "people skills" [21] as well as non-trivial expertise in usable security, such as interview and survey conduction and analysis, ethnographic observations or participatory design techniques.

This situation is similar to the situation of the users 20 years ago [1]: they were required to possess security skills that were beyond their human capacities, skills and work realities. The field of usable security moved forward since then, such that security professionals now take the responsibility for producing effective security. However, they cannot proceed without appropriate help. They need organizational structures, methods and tools that facilitate systematic engagement with the users. One of the most important research directions for future work is to conceptualize and develop these structures, methods and tools. An accompanying research question is: what skills should be realistically required from security managers to use these methods and tools?

Finally, returning to the double-loop learning, Argyris [5] states that the organizational change must start on the top managerial level, as otherwise the changes will not be stable. Thus, future research should investigate what level of commitment is required from the top management in order to implement effective organizational security.

Limitations

Our data analysis is based on interviews with seven IT security managers from large-scale German organizations. This limited amount of interviews makes the study explorative in nature. That said, we think that our results can show the breadth of factors in play (without making claims about their quantitative representativeness). While it is not certain if theoretical saturation was reached, we found little variety in our sample concerning major themes. We also think that it is likely that our results apply outside of Germany, as most considered companies operate internationally.

6 CONCLUSION

We showed how missing organizational structures for including users in the security development process lead to a negative perception of the users by security managers, and thus to a control-oriented approach rather than to a user-oriented approach. Implementing organizational structures for developing user-centric corporate security and providing security managers with appropriate methods and tools is an important research direction that needs future development.

Acknowledgments. We thank the four anonymous reviewers for carefully and critically reading the manuscript and suggesting substantial improvements. The authors were supported by the Bavarian State Ministry of Education, Science and Arts as part of the FORSEC research association.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.

[2] Eirik Albrechtsen. 2007. A qualitative study of users' view on information security. *Computers & security* 26, 4 (2007), 276–289.

[3] Eirik Albrechtsen and Jan Hovden. 2009. The information security digital divide between information security managers and users. *Computers & Security* 28, 6 (2009), 476–490.

[4] Chris Argyris. 1976. Single-loop and double-loop models in research on decision making. *Administrative science quarterly* (1976), 363–375.

[5] Chris Argyris. 1977. Double loop learning in organizations. *Harvard business review* 55, 5 (1977), 115–125.

[6] Chris Argyris. 1995. Action science and organizational learning. *Journal of managerial psychology* 10, 6 (1995), 20–26.

[7] Debi Ashenden and Darren Lawrence. 2016. Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy* 3 (2016), 82–87.

[8] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.

[9] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and M Angela Sasse. 2016. Productive security: A scalable methodology for analysing employee security behaviours. In *12th Symposium on Usable Privacy and Security (SOUPS)*. 253–270.

[10] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2009. The compliance budget: managing security behaviour in organisations. In *New Security Paradigms Workshop*. ACM.

[11] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2017. Finding security champions in blends of organisational culture. In *Workshop on Usable Security (USEC)*.

[12] John M. Blythe, Lynne M. Coventry, and Linda Little. 2015. Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors.. In *11th Symposium on Usable Privacy and Security (SOUPS)*. 103–122.

[13] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards understanding IT security professionals and their tools. In *3rd Symposium on Usable Privacy and Security (SOUPS)*. ACM, 100–111.

[14] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.

[15] Lizzie Coles-Kemp. 2018. Practising Creative Securities. https://bookleteer.com/collection.html?id=28

[16] Lizzie Coles-Kemp, Debi Ashenden, Kieron O'Hara, et al. 2018. Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance* 6, 2 (2018), 41–48.

[17] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research*. Sage.

[18] John D'Arcy, Tejaswini Herath, and Mindy K Shoss. 2014. Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems* 31, 2 (2014), 285–318.

[19] Gurpreet Dhillon and Gholamreza Torkzadeh. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal* 16, 3 (2006), 293–314.

[20] Paul Dourish, E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[21] Julie M. Haney and Wayne G. Lutters. 2017. Skills and Characteristics of Successful Cybersecurity Advocates. In *Workshop on Security Information Workers*. USENIX Association.

[22] Claude PR Heath, Peter A. Hall, and Lizzie Coles-Kemp. 2018. Holding on to dissensus: Participatory interactions in security design. *Strategic Design Research Journal* 11, 2 (2018), 65–78.

[23] Karin Hedström, Ella Kolkowska, Fredrik Karlsson, and Jonathan P Allen. 2011. Value conflicts for information security management. *The Journal of Strategic Information Systems* 20, 4 (2011), 373–384.

[24] Tejaswini Herath and H Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (2009), 106–125.

[25] Philip G. Inglesant and M. Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 383–392.

[26] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. 2015. Shadow security as a tool for the learning organization. *ACM SIGCAS Computers and Society* 45, 1 (2015), 29–37.

[27] Iacovos Kirlappos and M. Angela Sasse. 2014. What usable security really means: Trusting and engaging users. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 69–78.

[28] Michaela Luecke and Judith Simon. 2014. A Self-Regulatory Approach to Behavioral Compliance with IS Security Policies – "Come on, Baby, do the Locomotion". In *20th Americas Conference on Information Systems*.

[29] Seppo Pahnila, Mikko Siponen, and Adam Mahmood. 2007. Employees' behavior towards IS security policy compliance. In *40th Hawaii International Conference on System Sciences*. IEEE.

[30] Simon Parkin, Aad Van Moorsel, Philip Inglesant, and M. Angela Sasse. 2010. A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *New Security Paradigms Workshop*. ACM, 33–50.

[31] Shari Lawrence Pfleeger, M Angela Sasse, and Adrian Furnham. 2014. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management* 11, 4 (2014), 489–510.

[32] Clay Posey, Tom L Roberts, Paul Benjamin Lowry, and Ross T Hightower. 2014. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management* 51, 5 (2014), 551–567.

[33] Petri Puhakainen and Mikko Siponen. 2010. Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly* (2010), 757–778.

[34] Karen Renaud. 2012. Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy* 10, 3 (2012), 57–63.

[35] Mikko Siponen and Juhani Iivari. 2006. Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems* 7, 1 (2006).

[36] Mikko Siponen, Seppo Pahnila, and Adam Mahmood. 2006. Factors influencing protection motivation and IS security policy compliance. In *Innovations in Information Technology*. IEEE.

[37] Anthony Vance, Mikko Siponen, and Seppo Pahnila. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management* 49, 3-4 (2012), 190–198.

[38] Rodrigo Werlinger, Kirstie Hawkey, David Botta, and Konstantin Beznosov. 2009. Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies* 67, 7 (2009), 584–606.