Guiding Decisions on Authorization Policies: A Participatory Approach to Decision Support

Steffen Bartsch
TZI – Universität Bremen
P.O.B. 33 04 40
28334 Bremen, Germany
sbartsch@tzi.de

M. Angela Sasse
Department of Computer Science
University College London
London, WC1E 6BT, UK
a.sasse@cs.ucl.ac.uk

ABSTRACT

Most organizations have access control policies, and many have to change them frequently to get work done. Currently, the way such changes are made often has a significant impact on the organization's security, productivity, and employee satisfaction. Those who have to make the decisions are put on the spot, and depending on their perspective and circumstances, the decision is biased towards business or security interests. A decision support system for access control policies could mitigate these problems, but to be effective, such a system needs a significant amount of information about specific security and business risks and benefits, and collecting this information requires significant investment. In this paper, we present a participatory approach to collecting this information, which not only reduces cost, but increases effectiveness because it ensures that specific local knowledge and downstream risks are represented and visible to decision-makers. We evaluated our systematically developed decision-support prototype in formative evaluations with employees and decision-makers from a variety of backgrounds. We found that, among others, decision support is highly dependent on the organizational context and that the collected factors need to be contextualized for the contributing individuals.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

Keywords

Access control, Security usability, Decision support

1. INTRODUCTION

Effective access control requires that any changes to authorization policy[1] are made efficiently and maintain protection as required. When decisions on policy changes lack transparency or understanding of the resulting risks and benefits, this can impact an organization's productivity (an overly restrictive policy may stop employees from tackling tasks), security (if policies result in over-entitlements), and employee satisfaction (because they feel hampered in their tasks or unfairly barred from access to resources) [18, 23].

Theories on organizational decision-making describe those decisions as "organized anarchies" through a "garbage can" model [9]: In dynamic environment, streams of choices, problems, and solutions can take on the state of garbage that needs to be processed to take decisions. This can lead to actions being taken without considering the implications of policy changes. Employees in front-line business processes, who are affected by access restrictions, often have no insight into why a policy has been set that way.

To address the question of how to design adequate measures for specific access control contexts, and arrive at satisfactory approaches for functional and administrative staff, we need to understand and support the decision-making around policies. In this paper, we address whether and how we can guide the decision-making, and what information needs to be collected to offer effective support. Particularly, we examine how decision guidance can be efficiently implemented as part of policy-change procedures, and describe how a decision-support tool can be developed to fit a specific organizational context. We evaluated our decision-support prototype in formative evaluations with policy makers (making the decision on policy changes) and functional staff, and found that decision support is highly context-dependent: The formality of organization, the difficulty of decisions, and the mental framing of the involved individuals determine whether and how participatory decision-support is feasible and beneficial.

2. THE PROBLEMS WITH DECISIONS

Decision-making has been extensively researched in cognitive psychology, showing several cognitive effects that lead to decisions that differ from those expected from a careful weighing of arguments [10]. In information security, these effects have been, for example, shown for privacy decisions [1, 2]. The reason for this behavior is the "bounded rationality" of humans when taking decisions: They apply heuristics that depend on the framing of risk factors, whether the factors can be easily remembered, and other biases [7]. For authorization decisions, "satisficing" [14] is particularly relevant; decision-makers choose the first option that seems ade-

[1] "Policy" refers in this paper to the technical specification of allowed activities of principals. For more general rules of conduct w.r.t. security, we use the term "security policy."

SAC'12 March 25-29, 2012, Riva del Garda, Italy.

quate, instead of examining all available options. According to West [22], security decisions are difficult because the risks are often abstract, compared to benefits from taking risks.

Another theory that has been applied to organizational decision-making about information security is the principal–agent theory, which states that decisions are impacted by externalities and information asymmetry [16]. Externalities are positive or negative effects of the decision on entities not involved in the decision; for example, an individual may choose an insecure path that is convenient for them, but puts the organization at risk. Information asymmetry describes the different levels of information for staff and managers: Managers may choose some authorization policies because they do not know how this will impact employees' work.

3. IMPROVING DECISIONS

Participation and security awareness.

Participatory processes can motivate staff, particularly in small groups with high identification [20]. Participation can potentially increase the acceptance of policy decisions, and lead to higher satisfaction with, and effectiveness of, authorization. To make good decisions, the individuals involved need to be aware of the associated risks. Siponen [19] argues that all staff who interacts with information systems should be security-aware. A typical approach to awareness-building is reinforcement (supporting appropriate, and punishing inappropriate behavior), and social learning (learning from close contact, imitation, and the understanding of concepts) [3]. We argue that both can be fostered through appropriate decision-guidance.

Comprehensible decision factors.

The understanding of security is affected by the way humans conceive abstract security measures. Humans build mental models [12] of how security measures work. Generally, it is sufficient for them to have a simplified task-action mental model of how a mechanism works – the same way many people can drive a car, even if they do not understand in detail how it works. Camp [7] and Wash [21] have identified mental model humans have of security.

Abstract decision-factors are difficult to comprehend; mental-models theory suggests that understanding can be improved by presenting a specific example in a context that staff understand. For medical risk communications, Rothman and Kiviniemi [17] found that contextualizing risks can increase awareness and influence behavior – people need to be able to "simulate" or imagine the consequences of risks [13]. In sociology, Cannell and Otway [8] argue that "any risk communication must take into account the knowledge and experience of the audience it addresses."

For authorization policy decisions, we thus need to develop adequate and consistent mental models in the communication of decision factors and increase the concreteness of the factors by contextualizing them for the individual.

Guiding decisions.

Ahern et al. [2] argue that for privacy decisions in social networks, decision guidance could help to prevent atypical settings that may not reflect the individuals' intention. The decision-support approach by Beresnevichiene et al. [5] for security-investment is based on factors such as trustworthiness of users. However, they do not address the problem of eliciting the necessary information for the risk calculations.

4. DECISION-SUPPORT STUDY

To explore how selected approaches to decision support help to improve policy decision-making, and what problems occur in practice, we built a decision-support prototype based on the risk factors identified by employees of a large enterprise, and evaluated its practical viability.

4.1 Eliciting decision factors

In the first part of the study, we elicited and structured the factors which need to be considered in policy decisions. One researcher (not affiliated with the organization) coded transcripts of interviews on security compliance in a large, multinational organization. Semi-structured interviews (lasting about 45 minutes each) were conducted with 118 participants in two countries (78 face-to-face, 40 by telephone). Grounded Theory open coding [6, 11], identified 172 quotes and 62 raw codes on risk and benefit factors, which participants considered relevant in a variety of contexts, including in security-critical and privacy-relevant areas. Axial coding of these produced five high-level decision factors for risk: "benefit", "high-level policy", "data sensitivity", "impact", and "threat". For example, the quote:

> *"... but it could do damage to the company, the company share price and so forth"*

was coded as "Impact: Organizational: Share value". We then built the decision-support prototype by creating six spreadsheets as decision artifacts, assigning factor group and formulating questions for each factor.

4.2 Evaluation of a decision-support tool

In the second part of the study, we conducted a formative evaluation of the decision-support prototype with three staff and three policy makers from a variety of practical backgrounds. The evaluation questions were:

- In what context this type of decision-support tool effective?
- What decision factors can be collected how and from whom (comprehensibility, precision of data, willingness to give)?

Participants were selected to represent several types of organization (size, Mintzberg's Structural Configuration [15]) and position, as shown in Table 1. Using participants from a different context than the interviews in Study 1 allows us to assess the general applicability of the prototype. Whilst the evaluation sessions did not present representative and comprehensive coverage of decision-support problems, they provided us with rich subjective data to inform further research.

The evaluations lasted about one hour each and were semi-structured: They first covered preliminary questions on the participant's background and relation to authorization in practice. Then, the interviewer went with the participant through a participant-specific scenario, asking the participant to complete the questionnaires. While making the evaluations difficult to compare, the individual scenarios allowed us to reduce the effect of participants having to understand the possibly remote scenario [21]. The participants

	Role	Position	Organization
M1	Manager	Program manager of dev. team of 26	Software industry, multinational, 1000 emp., Divisionalized simple structure
M2	Manager	Project leader of 6	Web agency, 15 emp., simple structure
M3	Manager	Unit manager of 25	Dev. company of large bank, 300 emp., professional bureaucracy
S1	Staff	Food quality assurance	Food industry, multinational, 2500 emp., divisionalized professional bureaucracy
S2	Staff	Customer relations	Regional utilities company, 2500 emp., divisionalized machine bureaucracy
S3	Staff	Technical quality assurance	Security-sensitive electronics, 1500 emp., professional bureaucracy

Table 1: Study participant sampling

were asked to think out aloud while completing the forms and the walk-through were enriched with in-situ prompts. Following the walk-through, additional posterior questions were asked on the perception of the adequacy and usefulness for the participant's organizational context.

The evaluations were audio-recorded and transcribed. The transcripts were coded for the comments on and problems with the decision factors, and statements on the usefulness of decision support. The open coding resulted in 114 raw codes that were further consolidated as shown in the findings below.

5. DECISION-SUPPORT PROTOTYPE

The aim of the decision-support prototype is to separate different categories of risk factors, so that each group can be elicited individually when appropriate as part of the change procedure. The prototype consists of interrelated spreadsheets (artifacts) to collect the risk and benefit factors, and present aggregations of the factors to guide decisions.

5.1 Prototype design

The artifacts encompass questions to elicit the decision factors and aggregations of the factors. The questions aim for qualitative input, requiring either ratings (1–5 for a given scale, e.g. expected benefit), binary yes/no answers (e.g. having a specific awareness), or textual inputs (type of activity, informal benefit). Each question and output is accompanied by contextualizing clues, such as examples from the factor-elicitation study. The six artifacts of the tool are listed in Table 2.

While the decision-support tool does not prescribe a specific policy-change process, we assume an example procedure for didactic reasons: (1) A "requester" completes a request form for a concrete activity in a system on a specific set of data and chooses an adequate usage profile for the request; (2) the manager of the requester signs off the request, verifying the necessity of the request; (3) the "owner" of the resource decides on whether to enact the requested changes and how.

5.1.1 Change request

The change-request artifact is primarily thought to be completed by staff who require extended permissions, or on behalf of them. The artifact poses questions on 1) the general task, 2) the specific activity and data, 3) the benefit of providing the permission, and 4) a self-assessment of security awareness. While the participants were generally comfortable answering the questions, we still noted interesting difficulties: For example, there were contradicting statements how concrete the questions on the benefit need to be posed. A rather abstract question ("How high would you rate the benefit for the organization granting this permission?") can be difficult because it did not guide the individual on what to enter:

> *S1: "This is difficult to say [as one factor] since [activity] only makes out a small part of my work, but I need that transaction a lot if I do [activity]"*

Conversely, a more concrete form demonstrated the problem of specific benefits not fitting the given schema of frequency and time savings:

> *S3: "Productivity improvement would be from 0 to 100, because else I could not do it... there are also cases... [in which] having access improves the quality of work"*

Another benefit factor that the prototype asked for were indirect risks, i.e. risks that result from *not* granting the permission and staff needing to take more dangerous approaches to addressing the business needs (e.g. sharing passwords). This factor was problematic for the participants who were unfamiliar with this notion (S2: "We don't share passwords among each other").

5.1.2 Usage environment

The artifact on the usage environment should elicit risk factors that concern the context in which the permission – if granted – would be used, such as the physical security of the environment, the satisfaction of staff, and stress in the specific environment. Participants agreed that a distinction between the contexts is useful as it is common practice to take it into account for decisions, for example, distinguishing between desktop and laptop computers (e.g. S3 and M3).

Problems were seen in the added value of specific factors. For example, multiple participant raised doubts on whether the satisfaction has a significant impact on the threat of malicious activity (without referencing the participant):

> *"Well, the overall satisfaction in the company is not really high, but as I hear it people are all very loyal and rather shocked if someone takes information to another company"*

A more practical problem with the collection of the data was that staff stated that they would not answer honestly, fearing that the data could be misused:

> *"I could answer the employee satisfaction... but I would not answer questions on satisfaction, unless it is anonymous"*

Instead, it was suggested to reuse available data, for example, from employee surveys.

It was also interesting to observe how the physical-security factor was misunderstood or unclear depending on the framing of the participant. In case of organizations with a high emphasis on physical safety (e.g. utilities in case of S2), physical security is understood as the safety of the workplace (S2: "Is this about tripping hazards?").

Artifact	Example role	Activity	Information	Source
Change request	Requester	Permission request	Benefit from change, regulatory/qualification aspects, personal awareness of risks	Manual input
Usage environment	Requester	Permission request	Risks from the environment in which the requester uses the permission (e.g. “office”, “on the road”)	Manual input, reusable
Change approval	Requester manager	Approve request	Summary of the benefits and risks of the request	Aggregation of request and usage environment
Permission profile	Resource owner	Verify request	Risks associated with granting the permission to enact a specific activity in a system on a set of data	Manual input, reusable
Role profile	Resource owner	Verify request	Aggregate of the information on role members and risks from permissions assigned to the role	Aggregation of existing data from previous requests
Change decision	Resource owner	Verify request	Summary of the benefits and risks from permission–role and user–role assignments	Aggregation of data from prior artifacts

Table 2: Artifacts produced and used in the decision-support tool as part of the change procedure

5.1.3 Permission profile

The permission profile defines the risks associated with misusing a specific permission, such as “read source code from project X”. The factors of this artifact cover the general sensitivity of the data (e.g. personal data, commercial sensitivity), impact of misuse (e.g. from commercial or legal consequences), and the threat (the probability e.g. of a misuse or of accidental incidents). For higher precision of the risk estimation, we would need to elicit the impact and threat values for individual scenarios, and aggregate the risk scores. However, to reduce the burden of completing the form, we decided to approximate the overall risk from separate elicitations.

Whether staff participants were able to complete the form depended on the individual context. For instance, for the legal impact:

> *S3: “The data are also sometimes part of the contract. . . [the technical project manager] knows better about that than me”*

In other cases, the variation of the impact is high:

> *S1: “It depends the kind of information. . . it might be already rounded. . . or aggregated. . . in other cases you don’t want to hand out [at all]”*

Generally, there were doubts about the scalability of this kind of data collection:

> *M1: “What would be in the case that you had 20 different projects. . . Then, one would want to have a hierarchy, an ‘override’ for specific projects.”*

5.1.4 Role profile

The role profile is generated from aggregations of data on assigned permissions and contexts of assigned users. First, this artifact can inform decisions on whether it is appropriate to assign a role to a user, that is, whether the risks from the role are adequate for the benefit and the context of the request. Second, the artifact can support the decision of whether the users already assigned to a role make it adequate to assign an additional permission to the role. M1 remarked potential problems of scalability from the broad spread of roles.

5.1.5 Change approval and decision

Aggregating risks and benefits can support both approval (by the line manager of requester), and a policy-makers final decision. For approval by a manager of the requester, the approval artifact aggregates information on the benefits and context risks. For the actual decision, the policy-maker may derive insights on the adequacy of different change options from the risks and benefits. The decision artifact, in addition to the approval data, aggregates the information on the risks from the requested permission, from the users assigned to a role, and from permissions assigned to a role (see role profile). Problems stated by participants with respect to the aggregations of values primarily related to the transparency of the source of the aggregations (M2: “I don’t understand where those numbers come from.”).

5.2 Change procedures with decision support

Different organizations have different procedures for making policy changes, ranging from informal direct communication to highly regulated form-based procedures [4]. The decision-support prototype does not prescribe a specific process model. Of the studied authorization contexts, five had an informal and one had a formal procedure.

Although the forms of the decision-support prototype introduce extra effort to informal procedures, the participants did not categorically reject employing such a system and see advantages even for small organizations:

> *M2: “The current size of our company would not justify this tool, but in larger companies where you cannot have the overview over all areas and the applications. . . In our case, it would be nice to structure the decisions”*

S3, for example, further remarked with respect to the change-request artifact:

> *“Actually, I already provide this kind of information – only, I. . . formulate it as an email”*

In addition to the actual procedure, participants also reported that discussions take place around the requests to assign a permissions, and the tool needs to support these:

> *S1: “We discuss with [other department] how I can access that transaction. . . then my manager requests the permission from IT”*

5.3 Security awareness

We asked our participants about risks they are aware of, in connection with granting permissions. The participants primarily identified unintentional risks, such as “stolen laptop” (M1), or intentional risks, such as “data manipulation” (M2, S2, S3), but never gave a comprehensive range of threats.

The awareness of risks depended on the framing from the work practice, e.g. for the indirect risks in the change-request artifact, or the physical security for the usage-environment artifact.

> *M1: "On our level, we only look at the benefit and ignore the risk... that's why this could be helpful"*

6. DECISION-SUPPORT PROBLEMS

During the evaluation of the decision-support prototype, participants had problems in connection with the collection of information (all apart from transparency), and with the interpretation of aggregated data (only comprehensibility and transparency):

Availability of precise knowledge.

Depending on the perspective of the individual completing the form, some information may be difficult to elicit. One reason was that the data was not available to the specific role (see permission profile). In other cases, the participants did not have a comparison (e.g. for satisfaction in the usage-environment artifact). Finally, the accuracy of the data collection is also affected from the status-quo bias [10]: Individuals rely overly on the current situation for their estimation of risks (S1: "So many have the permission, I don't see it as critical").

Acceptability of information request.

Problems also occurred when the request for the data is seen as sensitive. Apart from the usage-environment factor of satisfaction (see artifact), this could be observed for the stress level in the team due to a general mistrust of how stress levels would be interpreted by superiors.

Adequate degree of abstraction.

Despite the goal of the prototype to achieve a high level of concreteness, we observed both problems due to abstract and concrete factors. Too abstract factors primarily affected overly broad questions (e.g. the benefit rating for the change request). Conversely, the questions could also be too concrete when they excluded a specific kind of input that does not fit the given questions (see request artifact).

Comprehensibility of the question and the factor.

Participants found questions difficult to understand if they were not familiar with the context – e.g. physical security. One reason can be that the factor is not applicable to the specific environment, as seen for the indirect risks when password sharing did not occur. Moreover, the factor behind the question can be conceptually difficult: For instance, participants had problems to distinguish impact and threat for the permission profile – two concepts that are difficult to separate for non-security experts.

Transparency of aggregations.

For aggregations of factors, participants had problems with the transparency of the information presented. For example, for the change-approval artifact, M2 was missing the indication of where the data came from (see artifact). M1 similarly requested for the role profile to receive richer information on its members (see artifact).

7. DISCUSSION

With respect to the applicability of decision support, our participants questioned whether a risk- and benefit-based decision is generally realistic:

> *M3: "If someone should develop... and needs a permission for that, we cannot say 'not possible'"*

Further, participants argued that a certain level of trust is necessary in a work relationship.

Regarding the usefulness decision support, participants stated a number of positive effects from such a system: First, it *improves the awareness:* Participants found the prototype to increase their security awareness (cf. Section 5.3). Second, it *improves request communication:*

> *S2: "It would reduce misunderstandings if I could formulate through such a form what permissions I require and for what reason"*

Third, it *improves decision transparency:*

> *M1: "What would be important, is a certain transparency in the decision... currently it's rather just 'no'... if some details were known, it would be more understandable"*

Validity of the results.

The study elicited subjective data from participants coming from different contexts. Consequently, we cannot expect to achieve a precise and comprehensive picture of the individual contexts. Because of the broad range of contexts that exist in practice, a formative evaluation with a limited number of participants cannot determine whether it will work for all circumstances. But the feedback obtained indicates that it has the potential to work for a range of organizational contexts.

Recommendations for decision-factor collection.

- *Adequately embed collection in procedures:* Despite the problems found in the study, the results indicate that participation through distributed data-collection is possible. However, considering the required formality and centralization, a decision-support system must be adequately integrated for the specific environment (cf. Section 5.2).

- *Contextualize factors:* Several of the problems were due to the difficulty in understanding the factors. Often a re-framing of the question in a more familiar way helped. Questionnaires for collecting information thus need to be domain-specific and tailorable to provide appropriate clues to those completing the form.

- *Respect the sensitivity of factors:* We need to respect that certain factors, such as employee satisfaction, are sensitive and employees may be reluctant to answer the respective questions honestly. The sensitivity of factors needs to be elicited, and indirect sources and the necessity need to be considered.

- *Offer flexibility in data collection:* For efficiency, the forms must be flexible to cater varying security needs, for example, requiring a baseline evaluation of risks in uncritical cases, but more details for critical ones (cf. Section 5.1.3).

- *Reuse existing data:* Every question in a form will require cognitive effort. As shown earlier, we can reuse data between requests to reduce the number of questions. In addition, we could leverage information already available elsewhere (e.g. employee surveys) to support and validate user input.

- *Support discussions:* Decisions often involve negotiations between stakeholders (cf. Section 5.2), who discuss the needs, risks, and technical alternatives as part of the process. Decision guidance should support this.

8. CONCLUSION

This paper presents a step towards providing decision support for authorization: We built a prototype decision-support tool and conducted a formative evaluation to assess the viability and usefulness of this type of tool. Our evaluation sessions explored how well the benefit and risk factors can be collected in a participatory form for efficiency. The responses we got show that effective decision-support is highly context-dependent: For instance, whether decision support is needed depends on how difficult the decisions on granting permissions are, and how distant policy makers are from the staff requesting permission changes. To be efficient, the decision-support system needs to be embedded in the organization-specific procedures, and support negotiations between stakeholders if necessary. Moreover, the study showed that the factors need to be understandable – and that means e.g. contextualized. The forms need to be adapted to the security needs of the organization and individual requests, and reuse existing data – from earlier requests and from external sources.

To develop the tool further, we will need to conduct detailed case studies, adapting the tool over time in a range of organizational contexts. Continuing the work on security awareness in this paper, we may further examine the connection between participation in decisions and gains in security awareness. This particularly involves whether completing forms with decision factors results in a better understanding of the consequences of circumventing security measures, e.g. sharing passwords.

9. REFERENCES

[1] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *Security Privacy, IEEE*, 3(1):26–33, jan. 2005.

[2] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '07, pages 357–366, New York, NY, USA, 2007. ACM.

[3] A. Bandura. *Social Learning Theory.* Prentice Hall, Englewood Cliffs, NJ, 1977.

[4] S. Bartsch. Exploring twisted paths: Analyzing authorization processes in organizations. In *Proceedings of the 5th International Conference on Network and System Security (NSS 2011).* IEEE Computer Society, 2011.

[5] Y. Beresnevichiene, D. Pym, and S. Shiu. Decision support for systems security investment. In *Network Operations and Management Symposium Workshops (NOMS Wksps)*, pages 118–125, 2010.

[6] P. Cairns and A. L. Cox. *Research methods for human-computer interaction.* Cambridge Univ. Press, Cambridge, 2008.

[7] L. J. Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3), Fall 2009.

[8] W. Cannell and H. Otway. Audience perspectives in the communication of technological risks. *Futures*, Oct 1988.

[9] M. D. Cohen, J. G. March, and J. P. Olsen. A garbage can model of organizational choice. *Administrative Science Quarterly*, 17(1):pp. 1–25, 1972.

[10] T. Gilovich, D. W. Griffin, and D. Kahneman, editors. *Heuristics and biases: the psychology of intuitive judgement.* Cambridge University Press, 2002.

[11] B. G. Glaser and A. L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine Transaction, 1967.

[12] P. Johnson-Laird. Mental models in cognitive science. *Cognitive Science*, 4(1):71–115, Jan 1980.

[13] D. Kahneman and A. Tversky. The simulation heuristic. Cambridge University Press, Cambridge, MA, USA, 1982.

[14] J. G. March, H. A. Simon, and H. S. Guetzkow. *Organizations.* Wiley, New York, 1958.

[15] H. Mintzberg. Structure in 5's: A synthesis of the research on organization design. *Management Science*, 26(3), March 1980.

[16] F. Pallas. *Information Security Inside Organizations – A Positive Model and Some Normative Arguments Based on New Institutional Economics.* PhD thesis, TU Berlin, 2009.

[17] A. J. Rothman and M. T. Kiviniemi. Treating people with information: an analysis and review of approaches to communicating health risk information. *J Natl Cancer Inst Monogr*, (25), 1999.

[18] S. Sinclair, S. W. Smith, S. Trudeau, M. E. Johnson, and A. Portera. Information risk in financial institutions: Field study and research roadmap. In *Proceedings for the 3rd International Workshop on Enterprise Applications and Services in the Finance Industry*, pages 165–180, 2008.

[19] M. T. Siponen. Five dimensions of information security awareness. *SIGCAS Comput. Soc.*, 31:24–29, June 2001.

[20] J. A. Wagner III and R. Z. Gooding. Shared influence and organizational behavior: A meta-analysis of situational variables expected to moderate participation-outcome relationships. *The Academy of Management Journal*, 30(3), Sep 1987.

[21] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, New York, NY, USA, 2010. ACM.

[22] R. West. The psychology of security. *Commun. ACM*, 51:34–40, April 2008.

[23] T. Whalen, D. K. Smetters, and E. F. Churchill. User experiences with sharing and access control. In *CHI '06: CHI '06 extended abstracts on Human factors in computing systems*, pages 1517–1522, New York, NY, USA, 2006. ACM.