On the possible impact of security technology design on policy adherent user behavior: Results from a controlled empirical experiment

Sebastian Kurowski[1], Nicolas Fähnrich[2], Heiko Roßnagel[3]

Abstract: This contribution provides results from a controlled experiment on policy compliance in work environments with restrictive security technologies. The experimental setting involved subjects forming groups and required them to solve complex and creative tasks for virtual customers under increasing time pressure, while frustration and work impediment of the used security technology were measured. All subjects were briefed regarding existing security policies in the experiment setting, and the consequences of violating these policies, as well as the consequences for late delivery or failure to meet the quality criteria of the virtual customer. Policy breaches were observed late in the experiment, when time pressure was peaking. Subjects not only indicated maximum frustration, but also a strong and significant correlation (.765, p<.01) with work impediment caused by the security technology. This could indicate that user-centred design does not only contribute to the acceptance of a security technology, but may also be able to positively influence practical information security as a whole.

Keywords: Policy Compliance; Technology Acceptance; Task Technology Fit; Information Security; Due Care

1 Introduction

Understanding human adherence or deviance to information security policies is a key element for future security architectures. Human behaviour is an important antecedent for attacks on organizational and private information systems [Jo16], with 34.8% of german corporations reporting social engineering as a main cause of industry espionage [Co14], and human error being one of three root causes for data breaches [Po16]. Therefore users in information security are often treated as a potential vulnerability [AH09]. Existing literature indicates that users are either naïve poorly educated, or risk takers in their security behaviour [Ke17] and should be faced with due process (e.g. sanctions) [DHG08] in the case of non-compliance. Other research indicates that users are an important security asset and

[1] Fraunhofer-Institute for Industrial Engineering IAO, Competence Team Identity Management, Nobelstr. 12, 70569 Stuttgart, sebastian.kurowski@iao.fraunhofer.de

[2] University of Stuttgart, Institute for Labour Science and Technology Management IAT, Competence Team Identity Management, Nobelstr. 12, 70569 Stuttgart, nicolas.faehnrich@iat.uni-stuttgart.de

[3] Fraunhofer-Institute for Industrial Engineering IAO, Competence Team Identity Management, Nobelstr. 12, 70569 Stuttgart, heiko.rossnagel@iao.fraunhofer.de

doi:10.18420/sicherheit2018_11

should be considered more thoroughly [AS99, ZR12] in the design process of security architectures. This existing contradiction has led to an ongoing discussion in the topic of security technology design as to which extent a technology should meet user requirements [Fr07, ZR12, HRZ10], and to which extent a technology should enforce security aspects in order to provide a contribution to an effective security architecture. Finally, there are existing contributions that emphasize the impact of an individuals' environment, e.g. the actions of the individuals' peers [AH09] with regard to information security, or the impediment on the individuals work [KB13]. All these contribution have one thing in common: they mostly use static, momentary data capture methods such as self-reporting questionnaires, or focus on changes e.g. in password use, rather than observing human behaviour. This contribution aims at providing the question how human behaviour changes prior and after a policy violation. We aim to observe changes in social interactions, frustration, and use of security technologies in the context of a policy violation. In the following, we provide insights from a 2-day controlled experiment that was conducted in order to gain an understanding on the impact of the individuals' environment with regard to task load, social cues, and work impediment on the individuals' policy compliance. A security technology that provide strict policy enforcement capabilities was applied as a technical control in the setup. Since perfect policy enforcement is unrealistic in most real-world cases, the technical control was weakened with a backdoor. Use of this backdoor was clearly prohibited by an information security policy (administrative control) that was read to, handed out and signed by all participants. By observing the factors that occur during, prior and after a violation of the security policy by participants, we hope to get a more unified insight into what observable circumstances contribute to the security policy violation. The contribution is structured as follows: The following Section 2 provides an overview on currently used empirical research methodologies in security policy compliance research, and outlines why we have chosen a controlled experiment for our purposes. The experiment setup, sampling of participants, participant monitoring and measurement instruments are being introduced in Section 3. Observations regarding the policy compliance of the individuals, and a discussion of the observed factors that impact security policy compliance are laid out in Section 4, followed by conclusions in Section 5.

2 Methodology of Security Policy Compliance Research

Most of security policy compliance research uses self-reporting questionnaires, mostly implemented as web-surveys. For instance the contributions [ADO16, AMA15, AM14, BB13, BK07, BCB10, HB15, If16, KB13, Li14, PKS13, PH14, RFE16, Sa15, SKH15, WP13, WJS11, YBD16, YK13] use questionnaire item sets for measuring the intention to comply or the actual compliance. In this case individuals are asked, e.g. if they intend to comply with information security policies. Another possibility of measuring policy compliance or policy deviance is by using scenarios and asking the individual whether it would behave similarly as the individual described in the scenario. Such a factorial survey approach [RA82] is often used in research on policy deviant behaviour such as

[BS16, Ch13, DHS14, DHG08, Jo16] The advantages of both methods is obviously easier acquisition and maintenance of data, since the questionnaire must only be administered to the individuals, recollected and analysed. However, one must keep in mind that such surveys are often only able to provide a snapshot of policy compliance in time. Also in order for complex processes such as social interactions to be captured by these instruments, the researcher must anticipate these processes. In order to add context to the observation, and e.g. be able to find indications of not anticipated processes, one may refer to qualitative semi-structured interviews. Semi-structured interviews have e.g. been applied by [Ng09] in order to gain insights on the rather complex topic of security culture. Semi-structured interviews use pre-formulated questions, but do not require strict adherence to them [My09]. This adds the advantage that an interviewer is able to focus at the interview subjects' world, allowing improvisation and adaption of the interview process, while providing consistency between interviews. However, interviewers are not invisible to the interview subject, which may alter the situation and the outcome of the interview [FF05]. The contributions [SM16], [Je14], and [Va14] each use a controlled experiment. A controlled experiment allows for the observation of a group under treatment. The advantage of such a controlled experiment is that the condition of subjects can be observed in a controlled environment prior and after a treatment. This way changes in the conditions of the subjects cannot only be observed but also be accounted for. e.g. [Va14] used such a setup for observing the security behaviour of individuals. The research subject were observed in their behaviour on security warning disregard, while EEG data was being monitored. A security incident was applied as a treatment during the experiment and the experimenters could observe the changes in security perception. Obviously, there are methods available that involve easier maintenance and acquisition of data, such as self-reporting questionnaires, factorial survey methods, or qualitative semi-structured interviews. However, policy compliance may be subject to social cues, and environmental cues. Therefore, a controlled experiment, that allows the experimenters to measure and observe changes in social cues and subject behaviour, while controlling for changes in the subjects environment is applied for the research purposes of this contribution.

3 Methodology

3.1 Experiment Setup

The experiment setup aimed at providing a realistic engineering scenario, in which participants were equipped with an access control mechanism for use, while solving complex tasks for virtual customers. In their research on policy compliance in different professions, [Ra13] observe that innovative professions such as engineering or information systems showed the lowest indications for compliance with their organizations information security policy. Therefore, the experiment setup aimed at emulating engineering use cases. This was achieved by providing tasks that required the participants to innovate, be creative and improvise, all under increasing time pressure. Participants were required to use an

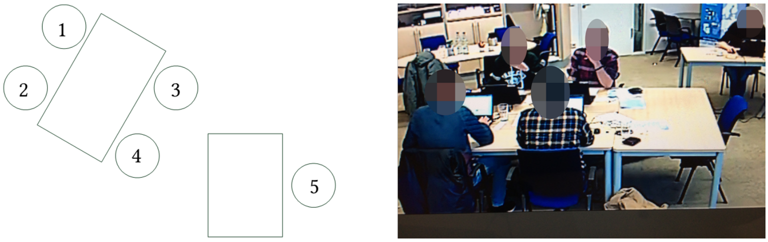

Fig. 1: Experiment setup. Participants were seated with respect to their role (left), whereas project leads (1-3) and the worker (4) were seated together, while the administrator (5) was seated apart. The right picture shows a screenshot from the observation stand of the setup.

access control mechanism. This mechanism was able to enforce access by encryption and signature of files. The mechanism was embedded into the computers operating system and could therefore be applied without any additional effort by the participants. The operating system used virtualization to provide Windows, Word and an E-Mail Client to the participants. Familiarity with Microsoft Windows and Word was a prerequisite during participant acquisition. Ten participants were randomly sampled into 2 groups from a sample of engineering, marketing and computer science students that had previously applied for participation in the experiment. The resulting groups however consisted of four students with a computer science background and one student with a marketing background in the first group, and 4 students with a computer science background and one student with an engineering background in the second group. Each group was participating for two days, whereas one day was set to 3 hours of experimentation, and the other day was set to 4 hours. Unfortunately, since the security mechanism was only available for a limited amount of time, scheduling of the experiment required one group to participate for 3 hours on the first and 4 hours on the second day, while the second group participated for 4 hours on the first, and 3 hours on the second day. This was solved by introducing a break each for the first and second group. This enabled both groups to stay aligned. The scenario, that participants were introduced into, looked as follows: The participants were told that they act as a virtual supplier in the automotive industry. They have three customers and the common duty to ensure due care, timely delivery and satisfaction of their customers quality expectations. This way, participants were able to receive a reward for their work between 80€ and 100€. However, if their group failed to deliver a task in due time, or to meet their customers quality expectations they would receive sanctions in terms of minus points. Each collected minus point collected by the group would then decrease the reward for each participant in the group. Additionally, participants were schooled that they were required to keep the data of their customers separate, as the customers themselves were competitors. This aligns well with the circumstances implied by engineering environments, such as in the automotive industry [WRZ12]. Participants were trained on how they could ensure this by using the access control mechanism provided to them. Participants were also told that failure to separate their customers data, may result in a security incident. Such an incident would also result in the group collecting a minus point. However, unlike in the case of late delivery, or not satisfying their customers quality criteria, participants were also told that a security incident may only facilitate with a chance of approximately 2.8% (This is the probability of six eyes on two dices). Since individual misbehaviour does not with certainty but only by chance lead to a security incident, this further ensured realism of the scenario. The setup design used a backdoor: An e-mail client was provided to the participants for communication of the customers with the participants, and in order to inform the participants when measurements take place. Participants could also use this e-mail client for data exchange with each other. However, encryption of the exchanged data would not be provided via e-mail. Participants were thus told, that any exchange of customer data between each other would be an unsecure data exchange and could thus lead to a security incident with a chance of approximately 2.8%, and thus to a minus point for the whole group. Instead, participants should exchange data via secured USB sticks which, while requiring more effort, enabled them to apply the access control mechanism on the data stored on the USB stick. Participants were not only schooled regarding the adequate security behaviour, but were also provided with this information in a written policy. While all participants shared the common duty for due care, timely delivery and satisfaction of the customers quality criteria, some participants had additional roles. Three participants were assigned as project leads, one project lead for each customer. The special responsibility of the project leads was to communicate with the customer, which included receiving the work specification from and providing the work result to the customer. They also had the responsibility to ensure secure, timely and adequate project execution. The other special role that was assigned was the administrator. The access control mechanism that was applied by all participants separated data between the projects for the different virtual customers. This was done by providing a group-like concept for the virtual customers. The administrators role was to ensure assignment and revocation of participants to the different groups. Its special duty was to ensure that no access rights creep was taking place so that the need-to-know was ensured at each participant. The administrator could do this by communicating with a virtual IT, demanding the assignment or revocation of participants to groups. Apart from these special roles, all participants also had the duty to work on the projects (worker role). Figure 1 provides an overview on the setup. Participants were told about the different special roles, and all participants were told to assign themselves to a special role if desired. Participants were seated, with regard to their role. This ensured that the participant observation could be more easily attributed to the participant role. All participants were briefed prior to the experiment regarding the increase in stress over time, but not regarding the hypotheses and objectives of the experiment. Particpants were also trained and reminded that they are able to cancel the experiment at any time. However, participants were told, why the stress was increased by the different suppliers after the experiment. This debriefing also included a detailed explanation of the experiment setup, the hypotheses and the overall objective of the experiment. All participants were observed during the experiment, in order to be able to cancel the experiment if any harm or danger is imminent for the individuals.

3.2 Treatments

Over the time of the experiment, the work load of the participants was gradually increased. The goal was to see, what amount of stress level will be measurable when the participants break the policy. Increase of stress was achieved by the projects that the participants were required to solve. These treatments were gradually, increased by decreasing (a) available time resources by decreasing the project deadlines, and (b) available work force by parallel customer requests. An example for such a treatment is provided in the Annex. The treatments over time are shown in Figure 2. The experiment started with only customer 1 asking for delivery, allowing participants to work collaboratively. However, until hour 3:00 into the experiment, the workforce is first decreased from 1:15 to 2:00, and then the workforce is decreased along with the available time resources by requiring the participants to provide results to all three customers in less time than in the previous projects. The treatment then drastically decreases the available time resources by requiring delivery for a project between 3:15 and 3:45. And then goes on into further decreasing the workload. The overall goal of this schedule is to continuously increase the amount of workload that the participants receive, by decreasing available time and workforce. Additionally, treatments were provided through customer interactions. If participants have already become familiar with the work, these interactions were designed to increase uncertainty and thus the participants stress. Such customer interactions could be complaints about the quality and threats of minus points by the customers, demanding additional work for projects shortly before the deadline, requiring an earlier delivery of the project results, demanding a draft of the work results or even a final draft with 90% completion status, or asking the project lead who currently works on the project. For instance, one customer might ask after 50% of the projects' time has passed, who is working on the project at the supplier. After the suppliers response, the customer would then ask for an earlier delivery. This combination of treatments by time reduction and work force reduction through the project situation, and increasing uncertainty at the participants by customer interaction, both aimed at gradually increasing the workload of the participants.

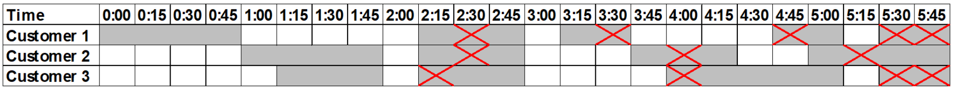

Fig. 2: Gantt chart of the treatments relative to the experiment time. Project-based treatments are shown in gray, whereas the right end of each gray area indicates the project deadline. Red crosses indicate treatments through customer interaction..

3.3 Data Acquisition

The experiment subjects were treated in an isolated room, in which they could act and organize autonomously. The room was monitored via three cameras that recorded and allowed the experiment team to observe the participants behaviour. The experiment team was situated in a separate room in order to minimize interference of the team with the subjects. In fact, after the participants were introduced, their consensus gathered, and led into the experiment room, the door was closed, and no interference from outside the experiment room was permitted. The experiment team consisted of two researchers, who created a protocol of the participants actions and group behaviour. By monitoring the mail server that was setup for the experiment, the experiment team also observed if any policy violations took place. During the experiment participants would fill out seven surveys at predefined times into the experiment. These surveys consisted of an item set for measuring work impediment by the security technology, taken from [KB13], along with a paper version the NASA Task Load Index (TLX) measurement instrument [Ha06]. The latter provides participants with the possibility to indicate their perceived mental, physical, and temporal demand by the task, their performance, effort and frustration. Since NASA TLX is a subjective measure of workload, results may vary drastically between participants. Therefore weighting of the participants indications is required. In order to provide this weighting, participants were required to answer a survey, which weighted the seven different categories of workload to each other. This resulted in an individual weighting of the different categories for each participant. The combination of experimenter protocols, the Work Impediment Item set, and NASA TLX allows both for capturing the participants work load and stress, the perceived work impediment by the security technology and the participants' and participant group behaviour. We assume that measurements of the workload that is created by working on an objective is virtually indistinguishable from the workload that is created by working on an objective with a certain security mechanism. Therefore, work impediment introduces a scale that focuses only on the impediment created by a security mechanism when working on an objective.

4 Analysis and Discussion

4.1 Observation of the groups

In the beginning (t+0:00) of the first day, both groups started off with the lowest amount of pressure, at least according to the treatments (see Section 3.2). It was observed, that the subjects of the first group had trouble understanding the provided access control system. Especially, the concept of groups seemed confusing in the beginning. This caused the subjects to work around the technology and to work without computers by dictating to the project lead, what he or she should write into the result report for the customer. After the break of the first group, the observed frustration seemed to increase, while three parallel projects were requested by the customers. Now the subjects seemed to arrange into smaller groups, and information exchanges via USB stick and in line with the communicated policy took place. During the experiment it became apparent, that the first group, even though they showed technical expertise, had a hard time to understand the security mechanism and how to adjust the group memberships. Still, even when, later in the experiment day, the USB sticks malfunctioned, the subjects remained to work in line with the policy. The second group showed more technical interest and competence than the first group. Already in the first project, this group build a hierarchy, whereas the administrator seemed to assign work and check-off decisions made by the group. This resulted in work being shared already in the first project. During the second project however, the group already started discussing whether they should violate the policy, since it would be quicker and deemed to be unlikely that something happens. However, the administrator as the informal leader of the group vetoed this option, which led to the other participants immediately disregarding the policy violation. Data exchange happened via USB stick, in compliance with the security policy. After the end of the first day both groups said they felt that the security mechanism restricted their work. The mechanism automatically encrypted every file. This effect was not visible for the participants, when working in one group. However, when transferring data from one group to another, e.g. via clipboard, participants only received encrypted data. While this strict enforcement of data separation between the groups was meant to be, it became evident that when participants were accidentally researching, e.g. with a web browser, for one customer but in the group of another customer, this feature would start to become annoying and obstructive for them. On the second day, the second group showed that they took the separation of customer data very seriously. Even though the time pressure was increased and the available work force was decreased due to parallel running projects, policy violations at first did not take place. However, 1:39 hours into the second day (at t+3:59), the USB sticks started to malfunction for the second group, and they started to violate the security policy after it became apparent to the group that they could not bypass this issue by e.g. dictating contents to the project lead who compiled the project report. Frustration and resignation of the participants become visible after this point, and more and more policy violations took place with the justification that nothing had yet happened (2:20 hours into the day at t+4:35 and 2:39 hours into the day at t+4:54). The first group made more use of the possibility to assign and revoke users to customer groups on the second day. This resulted in more cooperation between the participants. Information was being exchanged with USB sticks. However, it seemed to confuse participants sometimes that content that was not assigned to the group of their customer was encrypted. Finally, with increasing stress and being shortly before the deadline of a project, one of the project leads started to show a maximum amount of stress, yelling to another cooperating participant to “send the [. . .] thing per e-mail!”. This policy violation took place 1:47 hours into the second experiment day at t+5:02. This means, that while the policy violation in the second group took place at a later point in the experiment itself, it took place at a similar point in time of the experiment day for both groups (1:39 and 1:47 hours after start of the project), and at the moment of maximum visible frustration and highest time pressure. The experiment ended after t+06:00 hours, which means that the policy violation for the second group took place nearly at the end of the whole experiment. Both groups seemed to be very exhausted at the end of the experiment.

4.2 Task Load Index and Work Impediment

Overall, seven measurements of task load and work impediment were obtained per participant. The NASA TLX values were then weighted for each participant, by using the weights obtained from the survey at the end of the experiment (see Section 3.3). Since the experiment was spread over two days, participants had time to recreate between measurement three and four for group 1, and measurement two and three for group 2. Although, breaks were included in the experiment, to provide each group also with a moment to recreate, TLX values may be biased by this circumstance. Therefore the TLX values were further normalized with the minimum and maximum value for each participant on the respective experiment day. The resulting TLX values are provided in the annex.

The TLX values for both groups show, that the largest changes seem to be indicated with Frustration, Performance and Effort. Temporal Demands, while increasing, seem to only play a minor role. Cognitive demands remain relatively untouched by the treatments. Finally, physical demands as expected were all zero, since the factor was weighted to zero by all participants. Therefore physical demands are excluded from our analysis. In order to analyse the TLX values, we chose a correlation analysis. The results are indicated in Table 1[4] . It is clearly visible that the treatments resulted in an increase of the perceived performance (A self assessment of how successful the participant has been), , the participants effort (how hard was the work for the participant?), and the participants frustration. The indicated correlations are all highly significant ($p \leq .01$) and indicate high values. Temporal demands only weakly correlate with the participants frustration ($p \leq .05$). Also interesting is the relationship between work impediment, frustration, performance, and effort. The larger the demand that was introduced by the treatements showed to be, the larger the values for frustration, performance, effort and work impediment become. Illustrative for both experiment groups, showing this correlation are provided in the annex. The correlation between frustration and work impediment becomes evident in both, and is also indicated by the correlation analysis ($.765, p \leq .01$). Also the perceived work impediment by the security technology rises with the perceived performance ($.775, p \leq .01$), and the perceived effort ($.705, p \leq .01$).

4.3 Discussion of the findings

The participants, though affine to technology, were all neither security experts, nor familiar with security technologies. Yet, on the first day of the experiment one group decided to rather work with obstacles (e.g. by dictating contents to the project lead), than breaking the

[4] Due to length restrictions the annex to this contribution, that contains the data visualization and data tables along with the questionnaire, was not included in the printed version. It is however available online at: https://www.researchgate.net/profile/Sebastian_Kurowski/publication/323177670_Annex_-_On_the_possible_impact_of_security_technology_design_on_policy_adherent_user_behavior_Results_from_a_controlled_experiment/data/5a8479d4a6fdcc201b9ef0eb/sicherheit2018-annex.pdf

policy. The other group, although considering policy violations, kept to the security policy. Policy violations were, in both groups, only observed late into the experiment. The second group violated the policy twice between the fifth and sixth measurement, and again after the sixth measurement. The first group on the other hand took until shortly after the sixth measurement to violate the policy. This was surprising, since obviously all participants knew that there is only a minor chance that they got a disadvantage out of the action and it would have improved their work efficiency and reduced their level of task load. Participants argued after the end of the first day of the experiment that they wanted to keep the customer data secure, although they had no security expertise whatsoever. Another interesting observation is the correlation of work impediment. We would have expected, that work impediment remains steady, or at most weakly correlates with the amount of effort, performance and frustration. However, work impediment indicates one of the strongest correlations with these task load factors. Also in both groups, the policy violation could be observed at 1:39 / 1:47 and at a point when the frustration and work impediment each climaxed (between the fifth and the sixth measurement). This of course raises the suspicion, that the surge in frustration, work load and work impediment may be a cause for the policy violation. Participants all had one thing in common: they complained about the usability of the security technology. This is also shown by the work impediment. Furthermore, the bad user experience seemed to contribute to the frustration of the participants. The Theory of Planned Behaviour (TPB) [AH09], that plays a role in some contributions for information security policy compliance [SKH15, Hu12, If12, BCB10] may provide a possible explanation for this observation. TPB postulates that human behaviour is constituted out of the attitude of the individual towards the behaviour, the subjective norm of the behaviour, and the perceived behavioural control of the individual over the behaviour. The subjective norm hereby indicates the amount of pressure implied by the individuals peers. Since a violation of the security policy would have led to the chance of sanctions for the whole group, each participant may have perceived the subjective norm of not violating the security policy. The attitude of the individual may also have been positive towards keeping the customer data safe. This also aligns well with the observations from Section 4.1. However with increasing reduction of available time, work-force and the increase of uncertainty came an increase not only in performance and required effort, but also in the work impediment. This means, that the lack of usability was perceived worse, when under more stress by the individuals. This may have led to a change in attitude, from keeping the customer data secure towards not failing to meet the deadline and risking certain minus points. This is obviously a blatant contradiction to the naïve, unknowing or risk-affine user. None of our participants exhibited naivity or risk-affinity. All were unknowing. But neither violated the policy in the beginning. However, our results indicate that the work conditions, including the design of the security technology, may actually contribute to a security policy violation, not the disposition of the user.

5 Conclusion

To our knowledge this is the first time such a controlled experiment has been conducted in the field of security policy compliance research. The advantage of our approach over classic survey-based approaches that are widely used in policy compliance research lie in the opportunity to observe changes to behaviour prior and after the policy violation and to observe the actions that led to the policy violation. Our measurements indicated, that the work impediment of the security technology is perceived differently under different workloads, and that a surge in work impediment, frustration, performance and effort of the tasks contribute to a policy violations. Our observations showed that the participants, albeit being unknowing of security, showed a large willingness to protect the customer data and even switched to more work-intensive workarounds even though they could have gained an obvious advantage from breaking the policy. An explanation for this observation however could be provided by a change of attitude in the light of TPB. If these observations are true, this means that the users role in policy compliance must be reconsidered. Policy violations may be subject to bad working conditions, and the security technology design. All these correlations show a high likeliness of not being random ($p \leq .01$) even though rather small sample sizes were used in the experiment. We therefore argue that the impact of the security technology, along with basic assumptions about the user in information security must be reconsidered in order to provide an effective and secure working environment.

References

[ADO16] Abed, J.a; Dhillon, G.a; Ozkan, S.b: Investigating continuous security compliance behavior: Insights from information systems continuance model. In: AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems. 2016.

[AH09] Albrechtsen, E.; Hovden, J.: The information security digital divide between information security managers and users. Computers & Security, 28(6):476–490, September 2009.

[AM14] Aurigemma, S.a; Mattson, T.b: Do it OR ELSE! exploring the effectiveness of deterrence on employee compliance with information security policies. In: 20th Americas Conference on Information Systems, AMCIS 2014. 2014.

[AMA15] Al-Mukahal, H.M.a; Alshare, K.b: An examination of factors that influence the number of information security policy violations in Qatari organizations. Information and Computer Security, 23(1):102–118, 2015.

[AS99] Adams, Anne; Sasse, Martina Angela: Users are not the enemy. Commun. ACM, 42(12):40–46, December 1999.

[BB13] Borena, B.a; Bélanger, F.b: Religiosity and information security policy compliance. In: 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. volume 4, pp. 2848–2855, 2013.

[BCB10] Bulgurcu, B.; Cavusoglu, H.; Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly: Management Information Systems, 34(SPEC. ISSUE 3):523–548, 2010.

[BK07] Boss, S.R.a; Kirsch, L.J.b: The last line of defense: Motivating employees to follow corporate security guidelines. In: ICIS 2007 Proceedings - Twenty Eighth International Conference on Information Systems. 2007.

[BS16] Bansal, G.; Shin, S.I.: Interaction effect of gender and neutralization techniques on information security policy compliance: An ethical perspective. In: AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems. 2016.

[Ch13] Cheng, L.a; Li, Y.a b; Li, W.a; Holm, E.c; Zhai, Q.c: Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers and Security, 39(PART B):447–459, 2013.

[Co14] Corporate Trust: Studie: Industriespionage 2014 - Cybergeddon der deutschen Wirtschaft durch NSA & Co.? Studie, Coprorate Trust Business Risk & Crisis Management GmbH, München, 2014.

[DHG08] D'Arcy, J.; Hovav, A.; Galleta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, pp. 1–20, 2008.

[DHS14] D'Arcy, J.a; Herath, T.b; Shoss, M.K.c: Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems, 31(2):285–318, 2014.

[FF05] Frey, James H; Fontana, A: The interview: From neutral stance to political involvement. The Sage handbook of qualitative research, pp. 695–726, 2005.

[Fr07] Fritsch, Lothar: Privacy-Respecting Location-Based Service Infrastructures: A Socio-Technical Approach to Requirements Engineering. Journal of Theoretical and Applied Electronic Commerce Research, 2(3), 2007.

[Ha06] Hart, Sandra G: NASA-task load index (NASA-TLX); 20 years later. In: Proceedings of the human factors and ergonomics society annual meeting. volume 50. Sage Publications Sage CA: Los Angeles, CA, pp. 904–908, 2006.

[HB15] Humaidi, N.a; Balakrishnan, V.b: The Moderating effect of working experience on health information system security policies compliance behaviour. Malaysian Journal of Computer Science, 28(2):70–92, 2015.

[HRZ10] Hühnlein, D.; Roßnagel, H.; Zibuschka, J.: Diffusion of Federated Identity Management. In (Freiling, F.C., ed.): Sicherheit 2010, pp. 25–36. Köllen Druck + Verlag GmbH, Bonn, 2010.

[Hu12] Hu, Q.a; Dinev, T.b; Hart, P.b; Cooke, D.c: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences, 43(4):615–660, 2012.

[If12] Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers and Security, 31(1):83–95, 2012.

[If16] Ifinedo, P.: Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? Information Systems Management, 33(1):30–41, 2016.

[Je14] Jenkins, J.L.a; Grimes, M.b; Proudfoot, J.G.b; Lowry, P.B.c: Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. Information Technology for Development, 20(2):196–213, 2014.

[Jo16] Johnston, A.C.a; Warkentin, M.b; McBride, M.c; Carter, L.d: Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems, 25(3):231–251, 2016.

[KB13] Kajtazi, M.a; Bulgurcu, B.b: Information security policy compliance: An empirical study on escalation of commitment. In: 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. volume 3, pp. 2011–2020, 2013.

[Ke17] Kelm, D.: Security-Fatigue I - Wenn Anwender es müde sind, sich um Sicherheit zu bemühen - und was man dagegen tun kann. <kes> Die Zeitschrift für Informations-Sicherheit, 33(4):54–57, August 2017.

[Li14] Li, H.a; Sarathy, R.b; Zhang, J.c; Luo, X.d: Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. Information Systems Journal, 24(6):479–502, 2014.

[My09] Myers, MD: Qualitative research in business and management. Sage Publications Ltd, London, 1 edition, 2009.

[Ng09] Ngo, Leanne; Zhou, Wanlei; Chonka, Ashley; Singh, Jaipal: Assessing the level of I.T. security culture improvement: Results from three Australian SMEs. IEEE, pp. 3189–3195, November 2009.

[PH14] Putri, F.; Hovav, A.: Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In: ECIS 2014 Proceedings - 22nd European Conference on Information Systems. 2014.

[PKS13] Pahnila, S.a; Karjalainen, M.a; Siponen, M.b: Information security behavior: Towards multistage models. In: Proceedings - Pacific Asia Conference on Information Systems, PACIS 2013. 2013.

[Po16] Ponemon Institute: 2016 Cost of Data Breach Study: Global Analysis. Benchmark research sponsored by IBM, Ponemon Institute, IBM, Traverse City, Michigan, USA, June 2016.

[RA82] Rossi, Peter H; Anderson, Andy B: The factorial survey approach: An introduction. Measuring social judgments: The factorial survey approach, pp. 15–67, 1982.

[Ra13] Ramachandran, Sriraman; Rao, V Srinivasan Chino; Goles, Timothy; Dhillon, Gurpreet: Variations in information security cultures across professions: a qualitative study. Communications of the Association for Information Systems, 33(11):163–204, 2013.

[RFE16] Rocha Flores, W.; Ekstedt, M.: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 59:26–44, 2016.

[Sa15] Safa, N.S.a; Sookhak, M.a; Von Solms, R.b; Furnell, S.c; Ghani, N.A.a; Herawan, T.a: Information security conscious care behaviour formation in organizations. Computers and Security, 53:65–78, 2015.

[SKH15] Sommestad, T.; Karlzén, H.; Hallberg, J.: The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security, 23(2):200–217, 2015.

[SM16] Shepherd, M.M.a; Mejias, R.J.b: Nontechnical Deterrence Effects of Mild and Severe Internet Use Policy Reminders in Reducing Employee Internet Abuse. International Journal of Human-Computer Interaction, 32(7):557–567, 2016.

[Va14] Vance, A.a; Eargle, D.b; Anderson, B.B.a; Brock Kirwan, C.a: Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). Journal of the Association of Information Systems, 15:679–722, 2014.

[WJS11] Warkentin, M.a; Johnston, A.C.b; Shropshire, J.c: The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems, 20(3):267–284, 2011.

[WP13] Wall, J.D.; Palvia, P.: Control-related motivations and information security policy compliance: The effect of reflective and reactive autonomy. In: 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. volume 2, pp. 894–902, 2013.

[WRZ12] Wehrenberg, Immo; Roßnagel, Heiko; Zibuschka, Jan: Secure Identities for Engineering Collaboration in the Automotive Industry. Bamberg, pp. 202–213, 2012.

[YBD16] Yaokumah, W.a; Brown, S.b; Dawson, A.A.c: Towards modelling the impact of security policy on compliance. Journal of Information Technology Research, 9(2):1–16, 2016.

[YK13] Yoon, C.; Kim, H.: Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology and People, 26(4):401–419, 2013.

[ZR12] Zibuschka, Jan; Roßnagel, Heiko: On Some Conjectures in IT Security: The Case for Viable Security Solutions. Presented at the SICHERHEIT 2012. 2012.