Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Analyze Before You Sensitize: Preparation of a Targeted ISA Training

Andreas E. Schütz, Kristin Weber and Tobias Fertig
Faculty of Computer Science and Business Information Systems
University of Applied Sciences Würzburg-Schweinfurt
Sanderheinrichsleitenweg 20, 97074 Würzburg, Germany
{andreas.schuetz, kristin.weber, tobias.fertig}@fhws.de

Abstract

This paper describes a procedure to enable the planning of targeted measures to increase the Information Security Awareness (ISA) of employees of an institution. The procedure is practically applied at a German university. With the help of a comprehensive analysis, which is based on findings of social psychology, necessary topics for ISA measures are identified. In addition, reasons are sought for why employees do not conduct information security. The procedure consists of a qualitative phase with interviews and a quantitative phase with a questionnaire. It turned out that the procedure provided many clues to the design of ISA measures. These include organizational and technical measures that can help employees to ensure information-safe behavior. In addition, it was found that there were deviations between the qualitative and quantitative phases and therefore, both phases are necessary. The paper critically discusses the procedure and also addresses the strengths and weaknesses of the analysis.

1. Introduction

In the digital age, the importance of information technology in companies and public institutions is increasing. In addition to facilitating work processes, digitization also creates challenges. Ensuring the security of information in particular is one of the biggest concerns in this context [1]. Protection is so important because information is now regarded as an enterprise asset and thus has a direct influence on business success [2]. The disclosure of sensitive information such as research results or personal data can lead to financial losses or negative effects of the image of an institution. The governments of states and countries have also recognized the high relevance of information security. For example, the government of the German federal state of Bavaria has enacted an e-government law obliging public institutions to draw up an information security concept and to create the technical and organizational prerequisites for its implementation.

When it comes to increasing information security, first and foremost technical measures are considered. Anti-virus software or firewalls are classic technical tools to protect information systems and an important part of a defense strategy. Current studies show, however, that attackers circumvent these technical defense mechanisms by directly manipulating the human factor in the system: The user who interacts with the computer [3, 4].

With attacks like phishing, malware, and social engineering these users are tricked to reveal their password or to transfer large amounts of money by using psychological tricks [5]. Organizational measures, such as the existence of guidelines, can create the necessary framework in companies and institutions to help to prevent such attacks. However, users must also be persuaded to comply with these regulations. The research area Information Security Awareness (ISA) deals with how people can be sensitized to behave in accordance with information security regulations. To raise ISA, measures are used which mainly aim at increasing the knowledge of the users [6]. However, this "One-Size-Fits-All" approach is not always effective. In order to change the interaction of people with computers in a targeted way, it is important to consider the influencing factors that lead to a certain behavior. For this purpose scientific findings of social psychology can be used [7]. In addition, it is also important to consider the individual situation in the company. For example, if employees know the rules for a secure password and still do not follow the rules, there is no point in teaching them the rules again. In this case, one need to look for other reasons for the prevailing behavior in order to persuade employees to conform. In order to implement such tailor-made training, a prior analysis of the current situation is essential. Good preparation increases the success of the measures and saves money, as unnecessary measures are avoided.

URI: https://hdl.handle.net/10125/64542
978-0-9981331-3-3

This paper presents the initial steps of an analysis in preparation for an tailor-made ISA training. The analysis was carried out at a German University of Applied Sciences. Due to the Bavarian E-Government Act, this university is obliged to develop an information security concept. The analysis was part of a project to implement the legal requirements. In the initial qualitative phase of the analysis, interviews were conducted with individual members of the organization. This served to generate insights into how users are confronted with information security in their daily work and what they think about it. In the following quantitative phase these impressions were taken up in the context of a questionnaire, which this time was addressed to all members of the organization and examined. The Integrated Behavior Model (IBM) from [8] is used as the basis for the procedure for the analysis and theory of human behavior. The use of IBM in the context of ISA was already motivated by [9]. This paper begins with basics of the research field, followed by an overview of related work. Afterwards we describe our research approach. We then present the results of the qualitative and quantitative analysis phases. These results and the strengths and weaknesses of the analysis are discussed afterwards. Finally, we give an outlook on future research.

2. Basics

The research area ISA targets the "human factor" and how IT users can be brought to an information security-compliant behavior. Users should be motivated to use their theoretical knowledge about information security in practice [10] and should be convinced of the importance of their actions. Three possible perspectives to ISA are described [11]:

1. Employees know, which threats exist and recognize them ("perception").
2. Employees further know, how to protect themselves against threats ("protection").
3. Employees know what a threat is, what they can do about it and that they behave accordingly ("behavior").

Only employees that behave compliantly, described in the third perspective, promise an actual increase in information security within an institution or company. ISA means that employees know how to behave in compliance with information security (e.g., choosing a secure password), what consequences they and the company may face in the event of non-compliant behavior (e.g., loss of image and financial loss due to loss of customer data) and that they actually apply this knowledge in critical situations. With the organization an additional aspect of security awareness is named by [12]. The organization ensures that employees in the company are able to behave in compliance with information security, i.e., no barriers exist, which are in conflict with compliant behavior. For example, a barrier is a password change link which is hidden in the depths of the company's intranet. At the same time, organizational measures, such as increasing usability of applications, can support information security.

The integrated behavioral model (IBM) [8] from health psychology helps to explain human behavior. The IBM was already interpreted in the context of ISA and used to explain the mental construct Security Awareness [9]. As shown in Figure 1 the ISA of a person is the sum of the four factors knowledge and skills ("I know how the behavior is performed"), habit ("I'm used to perform the behavior"), salience ("The performance of the behavior is in my mind"), and behavioral intent ("I want to perform the behavior"). Especially the factor behavioral intention is complex. It is formed by the mental constructs Attitude, the Perceived Norm and the Personal Agency of a person. These, in turn, are formed by emotions and beliefs. In order to achieve an information security-compliant behavior of a person for a certain behavior, the four indicated factors must be influenced. But even if the factors are perfectly pronounced, environmental constraints can still prevent the performance of the behavior. This clearly shows that the environment is also decisively involved in the behavioral formation of a human being. In addition, the influence of environmental factors can also affect the behavioral intention [8].

3. Related Work

In the past, the analysis of ISA has already been considered in various scientific papers. Kruger and Kearney [13] use the Knowledge-Attitude-Behavior (KAB) Model for their analysis. The KAB model assumes that the three factors knowledge, attitude, and behavior influence each other. The characteristics of these three dimensions were tested in six areas relevant to information security: adherence to guidelines, password security, diligence in handling e-mails and the Internet, diligence with mobile devices, reporting security incidents and the awareness that actions are followed by consequences. The individual topic areas were divided into several sub-areas. Both the dimensions and the subject areas were weighted differently by the researchers. By weighting the individual dimensions and areas, different companies

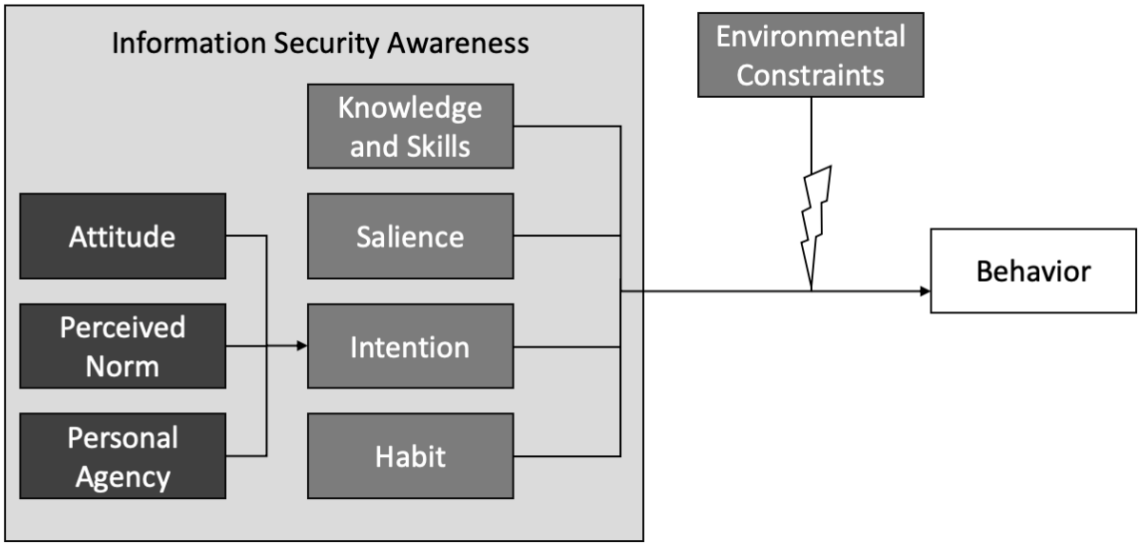

Figure 1. Factors of Behavior

can individually address the relevance of the dimensions and subject areas. The measurement itself takes place in the model using a questionnaire. Finally, the evaluation of the questionnaire provides both results of the respective dimension and subject areas as well as an aggregated overall result as a percentage. Khan et al. [14] proposes an approach for presenting the actual security awareness in companies. These are, for example, the number of helpdesk calls, the number of accesses to unauthorized pages or the evaluation of questionnaires that query knowledge on the subject of information security. Khan et al. [14] also recommend the use of questionnaires, but use the result as only one of several key figures. The remaining indicators are collected in real business operations and show how employees behave regardless of the level of knowledge.

4. Research Approach

This work distinguishes itself from the analysis methods presented in the section Related Work, which primarily aim to make ISA measurable. The aim of this paper is to determine the reasons for a specific behavior and to derive contents for targeted measures in a later ISA-training. It should also be examined whether different target groups have to be distinguished. In addition, first experiences with the procedure for analysis should be gained. It should be examined whether the results of the qualitative and quantitative part differ from each other and which advantages and disadvantages arise from the use of the method. For this, we chose the following research approach.

The current study is part of a project to introduce an information security management system (ISMS) at a German university. The general procedure of the project is based on the ISMS-Framework ISIS12 [15]. ISIS12 reduces the detailed and widespread standard IT-Grundschutz of the German Federal Office for Information Security (BSI) to measures that meet the requirements of small and medium-sized enterprises. It is also recommended for authorities. At the time of the survey, the university employed a total of 1079 staff. Employees at the university are a particularly important group in terms of information security awareness. They work with sensitive data, like personal data of students, and systems on a daily basis, making them a target for potential attackers as well as an important defense against various attacks.

The process performed for the analysis is based on the approach used by [8] to use the IBM in the field of health psychology. As seen in Figure 2 the scope was set initially by identifying the relevant topics that needed to be investigated. This was followed by a qualitative analysis which was carried out in the form of interviews. The interviews were subsequently analyzed and hypotheses were defined from the findings. These hypotheses were used in the quantitative analysis to develop questionnaires completed by the members of the university. The results of the questionnaires were also analyzed later to identify the content that needs to

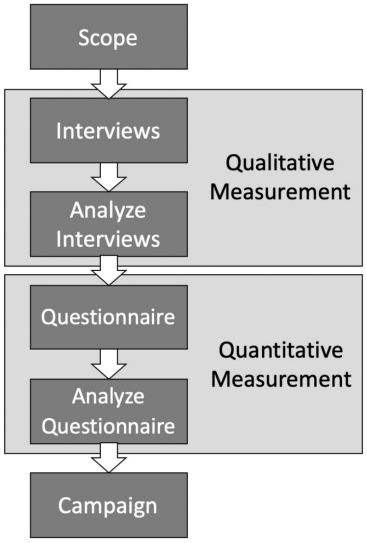

Figure 2. Process of Analysis

be addressed in a future campaign.

The investigation was carried out in the period May 2017 to March 2018. Since the later measures should aim all members of the university, it was necessary to include all subgroups of this broad target group in the analysis. The employees divide into the academic staff / lecturers, technical staff, administrative staff and others, which is mainly composed of external lecturers.

As a further preparatory action, the individual information security issues were identified, which should be considered in the analysis. For this purpose, in the first step, the 53 IT-Grundschutz measures listed in ISIS12 were selected in which a human factor is involved. These were discussed together with the responsible persons of the IT department of the university. Measures that were not relevant for the university were removed. The individual measures were arranged thematically and finally grouped into subject areas. In the following, these topics and the focused behaviors are enumerated.

- Passwords: Choosing a secure password for the university account. Periodical change of the password.
- Mobile devices: Use authentication methods for mobile devices used for business applications.
- Information exchange: No use of removable media (eg USB flash drives).
- E-mails: Detection of malicious e-mails. Use of certificates for secure communication.
- Workplace: Locking of the screen when leaving the workplace. Locking of work documents when leaving the workplace.

From these behaviors, the questions for the qualitative analysis were derived. Before the actual analysis, the procedure was coordinated with the staff council.

5. Qualitative Phase

The qualitative analysis was carried out in the form of interviews. In a first step, we determined departments and faculties of the university from as different areas of expertise as possible. The intention was to diversify the interview partners and provide insights into the various departments. Different representatives of the scientific, technical and administrative staff should be involved. In order to find interview partners, the superiors were sent an informative e-mail. The superiors in turn specifically asked their employees to participate in the interviews and passed on the names of the interested parties. In this way, 20 employees were persuaded to voluntarily participate in the qualitative analysis. The interviews were conducted between July 24, 2017 and November 14, 2017. The interviews were recorded with the prior consent of the participants in order to be able to evaluate them more easily later. The recordings were analyzed during the evaluation. In order to gain useful insights on the intention to behave and also to analyze the reasons for a certain behavior, we paid attention to questioning and collecting convictions and emotions about the respective behavior in the interviews.

In the area of “passwords”, it was found that the interviewed employees attach importance to choosing a secure password for the university account. When presenting different passwords, the participants were also able to identify those that correspond most closely to the current recommendations for passwords. The interviewees were more likely to have problems changing a password. The majority of the participants said they do not change their password. A few participants did not even change the initial password provided at the beginning of their career. The employees know that it is security relevant, but still do not do it. Two barriers were particularly noticeable here: Many employees find it difficult to remember new passwords. Almost all of them therefore wanted support, such as wishing to have a password manager. The second barrier is that many of the employees do not know how and where to change the password. Almost no one knew the university’s requirements for the design of secure passwords.

In the area of “mobile devices”, we learned that both private and business devices are used in the

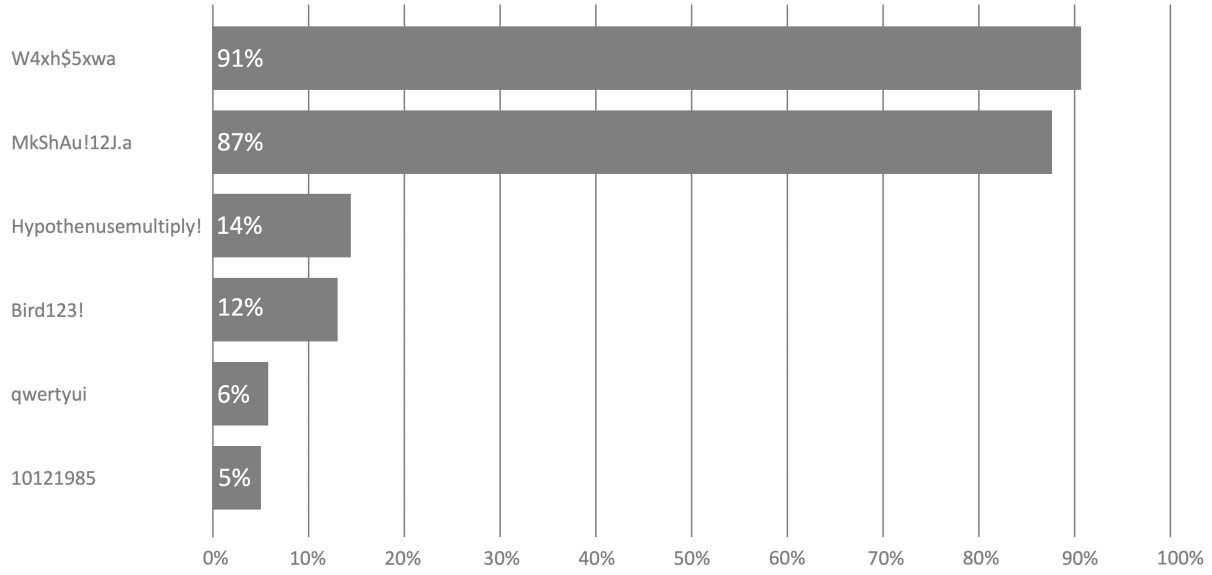

Figure 3. In my opinion, the following passwords are hard to break or to guess.

university environment. The most frequently used business application is the retrieval of business e-mails. The devices are secured with a PIN or fingerprint for most employees.

The participants indicated that they use external removable media, especially USB flash drives, at the workplace. The flash drives mostly are from students who want to transfer or print documents. Some were aware of the dangers this poses, but not all. On the contrary, lack of alternatives and convenience were identified as reasons for use.

In the case of malicious e-mails, most employees stated that they manually checked whether an e-mail was potentially dangerous (sender, file type, etc.). Potentially dangerous file formats in attachments, such as .exe, were identified by most employees. The rest rely on technical verification by an anti-virus software or the mail program. Few employees were aware of certificates for secure e-mail communications and only one respondent used a certificate.

Approximately half of respondents said they deliberately used the screen lock when leaving their workplace. The other half said that they either rarely or never do so. This second half saw no danger from their behavior. “There is no one else in my office” or “I have not stored any important data” are statements that were made in the process. Some of the employees leave their work documents on the desk (“Nobody comes in here anyway”). The other part locks sensitive documents in a cabinet. But not everyone has this option.

6. Quantitative Phase

The quantitative analysis was carried out with an online questionnaire. The questionnaire was designed on the basis of the previous interviews. For this purpose, the described findings were reformulated into assumptions, which in turn were used to formulate the questions. With this we wanted to investigate whether the insights gained were also an important topic in the university as a whole. The questions were grouped into the different topic blocks. In addition to the usual topics, we also asked for statistical data. The response options for the questions were individually adapted to the character of the question. Most of the questions could be answered on a Likert scale for measuring personal attitudes. Participants had five possible answers: “I fully agree”, “I rather agree”, “I neither agree nor disagree”, “I rather disagree”, and “I strongly disagree”. Alternatively, for some questions a sixth answer possibility was given with “Don’t know”. Some questions could also be answered with “Yes” or “No” or with different answer options to query knowledge. The statistical data also asked about the age group and the employee group. The staff groups were divided into scientific staff, technical staff, administrative staff and other. For each topic block, the participants also had the opportunity to leave comments in a text field.

The employee survey started on December 13, 2017 and was available until December 22, 2017. In advance, all employees were invited to take part in the survey

Table 1. Results of the quantitative Analysis (5 = I fully agree, 1 = I strongly disagree)

ID	Statement	5	4	3	2	1	Don't know	Yes	No
P1	It is important for me choosing secure passwords for all applications I use within the university. (n = 331)	50%	41%	3%	4%	1%	1%	-	-
P2	I know the password policy of the university. (n = 330)	-	-	-	-	-	1%	30%	69%
P3	I'm still using the password, I received at the beginning of my studies for university applications. (n = 331)	-	-	-	-	-	2%	16%	82%
P4	I change my university password regularly (e.g., once a year). (n = 237)	10%	26%	13%	36%	15%	-	-	-
P5	I think it is difficult to remember new passwords. (n = 330)	26%	33%	13%	18%	10%	-	-	-
P6	I would appreciate support regarding the memorization of passwords. (n = 331)	-	-	-	-	-	14%	35%	51%
P7	I know how to change my university password. (n = 330)	-	-	-	-	-	23%	60%	17%
M1	I check the e-mails of my university address with my private smartphone / tablet. (n = 312)	-	-	-	-	-	-	62%	38%
M2	I secure all my mobile devices (whether business or private) with a PIN, password, fingerprint or Face ID. (n = 247)	-	-	-	-	-	-	83%	17%
I1	I use USB drives/external hard drives that belong to other persons at my workplace. (n = 319)	12%	23%	10%	29%	26%	-	-	-
I2	I don't have issues with using USB drives/external hard drives other persons gave me. (n = 319)	4%	16%	11%	34%	35%	-	-	-
I3	I use the university cloud to store and exchange data. (n = 318)	17%	19%	10%	15%	39%	-	-	-
E1	I'm sure that malicious e-mails are recognized by my anti-virus programme. (n = 315)	11%	41%	19%	20%	9%	-	-	-
E2	I examine unexpected mails for signs of being potentially harmful. (n = 315)	73%	23%	1%	2%	1%	-	-	-
E3	I know that I can encrypt e-mails with a certificate. (n = 315)	11%	12%	11%	27%	39%	-	-	-
E4	I have requested a certificate for encrypting / signing e-mails. (n = 71)	-	-	-	-	-	1%	30%	69%
W1	I always lock my screen, even if I leave my workplace only for a short period of time. (n = 313)	42%	25%	7%	14%	11%	1%	-	-
W2	Locking the screen,is unnecessary to lock the screen, because nobody has access to the office. (n = 313)	6%	13%	10%	19%	52%	-	-	-
W3	Locking the screen is unnecessary because I don't have any important data on my computer/ notebook. (n = 313)	1%	4%	9%	21%	65%	-	-	-
W4	I always lock documents with important / sensitive information in a closet when leaving my workplace. (n = 313)	38%	26%	16%	15%	5%	-	-	-
W5	I do not have the option to lock documents away. (n = 63)	-	-	-	-	-	-	29%	71%

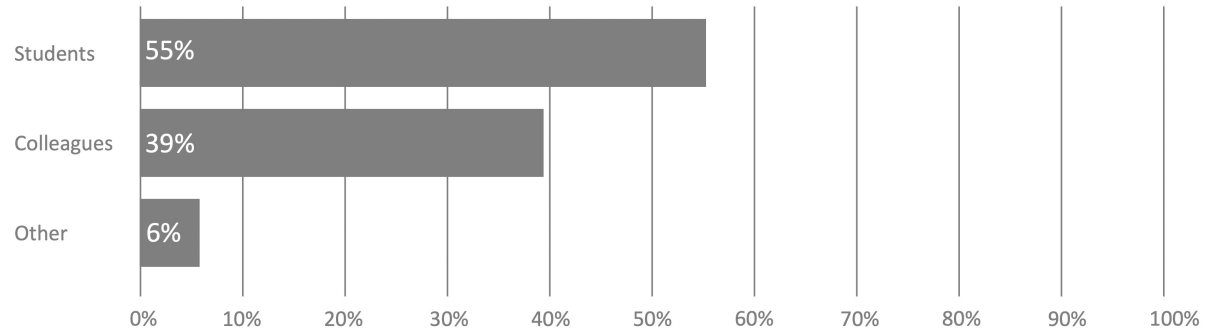

Figure 4. The USB drives / external hard drives predominantly belong to.

by e-mail. The deans of the faculties were contacted separately by the information security officer in order to encourage their employees to take part. 305 surveys were completed in full and 47 in part. With a total of 352 people, this corresponds to a response rate of 32.62 %. The detailed results of the survey are shown in Table 1. The following text refers to the ID of the respective statement.

The questionnaire confirmed that employees value secure passwords. 91 % of the participants agreed (P1). In addition, a large proportion of the questionnaires were able to identify passwords that comply with the current password rules (cf. Figure 3). In the questionnaire, 69 % gave an negative answer to the question of whether the employees knew the university's specifications for passwords (P2). In addition, 16 % of the employees still used their initial password (P3). But even for employees who have changed their initial password, it is rather unusual to change their password regularly afterwards. Only 36 % said they would become active here (P4). 60 % also said that they know where to change their password (P7). 59 % of employees said they had trouble remembering a password (P5). However, only 35 % require assistance with this (P6).

In the area of mobile devices, 62 % of employees used private devices to retrieve business e-mails (M1). 17 % of employees do not secure their mobile devices with an authentication method (M2).

In the area of information exchange, 69 % of employees have concerns about using removable media from other people (I2). 35 percent stated that they regularly use removable media from other people (I1). As seen in Figure 4 in most cases the flash drives belong to students (55 %), but also to other employees (39 %). The university's own alternative to data exchange (cloud solution) is used by 36 % of the participants (I3).

In the e-mail sector, 52 % of employees rely on anti-virus software to detect malicious e-mails (E1). As seen in Figure 5 a large proportion identified files ending with *.exe (90 %) and *.zip (77 %) as potentially dangerous attachments for e-mails. However, only 45 % consider *.doc to be dangerous. With 96 percent a a large proportion of the staff agrees, that they examine unexpected mails for signs of being potentially harmful (E2). In addition, only 23 % of employees know that a certificate for e-mails can be applied for to encrypt e-mails (E3). However, only 30 % of these people actually applied for a certificate to encrypt e-mails (E4).

While in the qualitative analysis only about half of the respondents stated that they lock the screen of their computer, 67 % said in the questionnaire that they lock the screen when leaving their workplace for a short time (W1). The conviction gained from the qualitative analysis "The locking of the screen is unnecessary because nobody but me and my office colleagues comes to my workplace anyway" is only agreed by 19 % of the respondents (W2). The conviction "The locking of the screen is unnecessary, because I have no important data on my computer" was agreed by only 5 % of the participants (W3). In the questionnaire, 20 % of respondents said they did not lock sensitive documents away (W4). Only 30 % of this group said they have no cabinet to lock them away (W5).

7. Discussion

The analysis could provide valuable insights for the development and design of awareness measures for the university. Surprising was that many of the behaviors investigated could be improved by organizational and technical solutions. The IBM shows that barriers at the workplace can have an effect on the intention to behave in terms of behavior (cf. [9]). In the area of passwords, it was shown that most employees are familiar with the recommendations for password design and that it is, therefore, not necessary to prioritize the

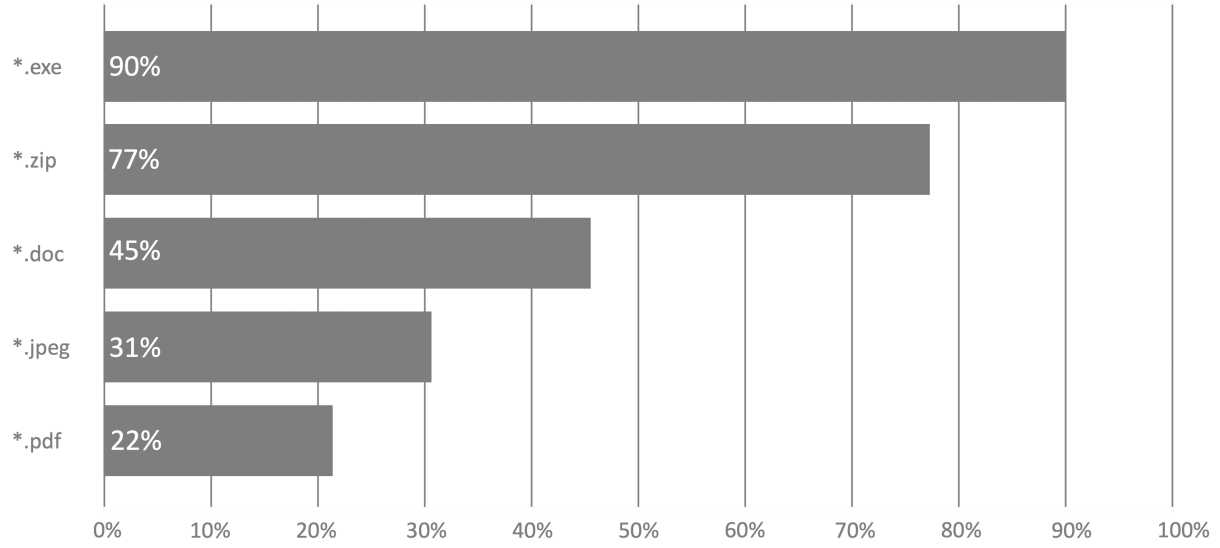

Figure 5. E-mail attachments with the following endings are potentially dangerous and should not be opened without hesitation. (Multiple answer allowed.)

topic passwords. Since, not any university specifications were known, the development of guidelines should be initiated. It could be helpful to orient on the new recommendations for passwords of the National Institute of Standards and Technology (NIST) [16]. Following the recommendations, newly selected and existing passwords are compared with a blacklist of insecure passwords. This investigation can also be used to check whether initial passwords are still being used. If the respective password appears in the list, the user receives a message asking him to change the password. In order to facilitate the password change, the necessary steps to change the password can be explained to the user in the message. Since some employees had requested assistance in remembering passwords, a password manager should be procured for voluntary use. Barriers were identified when reviewing the certificate application process following the survey. Instead of asking users to identify themselves at a central location away from the employees' workplaces, on-site appointments could be arranged where several employees can confirm their identity at once. In addition, additional cabinets should be bought to lock documents away for those who need it.

In the case of some types of behavior, the potential danger of noncompliance must be pointed out in order to influence the employees' intention to behave. Employees must be convinced of the relevance of business e-mail addresses in order to secure access to private mobile devices. The outgoing dangers of exposed documents and removable media like USB flash drives must also be clarified in order to influence the intention to behave. The cloud is already a technical solution for bypassing removable media. This solution is accessible not only to employees but also to students. In order to make this service salient, advertising for the cloud should be intensified in the future. In the area of e-mail, the main aim is to increase knowledge. Although the employees told us that they investigate suspicious e-mails, our analysis did not ask for any characteristics they check. Various incidents of phishing attacks in the time after the analysis showed success with only a few employees, but had major consequences. For this reason, employees need to be trained in this topic. Knowledge must also be imparted with regard to the process of integrating a certificate for secure e-mail communication. A simple manual could be designed for this purpose, which is now made available to the employees. Why the employees do not use a screen lock could not be determined in the analysis and will have to be determined in the future. For this behavior it is also a good idea to practice the habit of locking the screen with shortcuts on the keyboard.

The division of the analysis into a qualitative and a quantitative part has proved its worth. On the one hand, the real urgency of a topic could be determined. On the other hand, the quantitative part also showed differences to the findings of the qualitative part. While the employees strongly demanded a password manager in the interviews, only a small part of the employees asked

for help in the questionnaire. In addition, the interview participants were significantly more active in locking mobile devices than the questionnaire participants. Moreover, the quantitative analysis did not confirm the convictions expressed in the interviews as to why employees do not lock their screens. In addition, the lack of lockable cabinets was not reflected as much in the quantitative analysis as the interviews suggested.

Overall, the approach provided many clues for the design of ISA measures. The analysis also provided very targeted and individual insights, which can be used specifically in the context of the university. Otherwise, increasing knowledge might have been the only measure taken. However, the results show how diverse the reasons for a behavior can be. The use of IBM also made it possible to classify the various factors influencing human behavior. The involvement of employees in the topic also created an advertising effect for information security at the university and increased interest. However, there were also some weaknesses. On the one hand the analysis is very time-consuming, since the interviews must be accomplished and terminated. In addition it happened that important questions were not questioned in the quantitative analysis, because they were not considered necessary by the qualitative analysis. After the interviews, for example, it was assumed that mobile devices would be widely locked with authentication methods. Therefore, we never asked for reasons for not using authentication methods in the questionnaire. In the case of computer screen locking, beliefs gained in the interviews were not confirmed later in the quantitative analysis. Therefore, we never asked for other beliefs towards the behavior.

8. Outlook

The methodology presented in this paper describes the first practical trial of our approach to preparing a tailor-made ISA training. Many useful lessons have been learned for planning such actions. Whether these measures also promise the hoped-for success, must be examined in our further research. A good way of doing this is by taking a second survey after the measures have been completed. Future analyses should focus on gaining even more insights for the reasons of the performance of a certain behavior. Due to the broad range of behaviors, this was not possible in depth here. In addition, it will be necessary to examine whether participants in interviews or surveys are trying to be particularly exemplary. This could lead to distorted response tendencies (cf. [17]. This is only possible if the findings are substantiated with further key figures. Such an indicator could, for example, be a supplementary check of the password database to determine how many initial passwords are actually contained. In addition, research should be conducted into how the cost of qualitative analysis could be reduced in the future. By repeatedly using the interviews in different companies, it might be possible to generate a catalogue of different beliefs that would minimize the search for causes in the interviews in the future.

9. Acknowledgments

Andreas E. Schütz and Tobias Fertig were supported by the BayWISS Consortium Digitization.

References

[1] G. C. Kane, D. Palmer, A. Phillips, D. Kiron, and N. Buckley, "Strategy, not Technology, Drives Digital Transformation, Becoming a digitally mature enterprise.," Tech. Rep. 57181, Deloitte University Press, 2015.

[2] P. Blase and A. Rao, "Information as an asset," Dec. 2013.

[3] L. Hirshfield, P. Bobko, A. J. Barelka, M. R. Costa, G. J. Funke, V. F. Mancuso, V. Finomore, and B. A. Knott, "The Role of Human Operators' Suspicion in the Detection of Cyber Attacks:," *International Journal of Cyber Warfare and Terrorism*, vol. 5, pp. 28–44, July 2015.

[4] B. Semba and T. Eymann, "Developing a Model to Analyze the Influence of Personal Values on IT Security Behavior.," in *Tagungsband Multikonferenz Wirtschaftsinformatik 2016*, (Ilmenau), pp. 1083 – 1091, TU Ilmenau, 2016.

[5] ISACA, "State of Cybersecurity 2017. Part 2: Current Trends in Threat Landscape," tech. rep., Information Systems Audit and Control Association, 2017. Published: ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA.

[6] A. für Cybersicherheit, "Awareness-Umfrage 2015," tech. rep., Bundesamt für Sicherheit in der Informationstechnik, Bonn, May 2016.

[7] M. Siponen, "Five Dimensions of Information Security Awareness," *SIGCAS Comput. Soc.*, vol. 31, pp. 24–29, June 2001.

[8] D. E. Montaño and D. Kasprzyk, "Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavior Model," in *Health Behavior and Health Education* (K. Glanz, Rimer, Barbara, K., and K. Viswanath, eds.), pp. 67–96, APA PsycNet, 2008.

[9] A. E. Schütz, "Information Security Awareness: Its Time to Change Minds!," in *Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development - ICDD 2018*, (Sibiu, Romania), 2018.

[10] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," *Global Cyber Security Capacity Centre: Draft Working Paper*, pp. 188–131, 2014.

[11] N. Hänsch and Z. Benenson, "Specifying IT Security Awareness," in *2014 25th International Workshop on Database and Expert Systems Applications*, pp. 326–330, Sept. 2014.

[12] M. Helisch and D. Pokoyski, *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*. Wiesbaden: Vieweg+Teubner Verlag / GWV Fachverlage GmbH Wiesbaden, 2009.

[13] H. A. Kruger and W. D. Kearney, "A Prototype for Assessing Information Security Awareness," *Comput. Secur.*, vol. 25, pp. 289–296, June 2006.

[14] B. Khan, K. S. Alghatbar, S. I. Nabi, and M. Khan, "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management*, vol. 26, no. 5, pp. 10862–10868, 2011.

[15] Bayerisches IT-Sicherheitscluster, *Handbuch zur effizienten Gestaltung von Informationssicherheit für den Mittelstand*. Regensburg: Bayerischer IT-Sicherheitscluster e. V., version 1.7 ed., 2014.

[16] P. Grassi, R. Perlner, J. Fenton, W. Burr, and J. Picher, "Digital Identity Guidelines - Authentication and Lifecycle Management," NIST Special Publication 800-63B, U.S. Department of Commerce, 2017.

[17] A. L. Edwards, *The social desirability variable in personality assessment and research*. The social desirability variable in personality assessment and research, Ft Worth, TX, US: Dryden Press, 1957.