About the Measuring of Information Security Awareness: A Systematic Literature Review

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

Abstract

To make employees aware of their important role for information security, companies typically carry out security awareness campaigns. The success and effectiveness of those campaigns has to be measured to justify the budget for example. Therefore, we did a systematic literature review in order to learn how information security awareness (ISA) is measured in theory and practice. We covered published literature as well as unpublished information. The unpublished information was retrieved by interviewing experts of small and medium-sized enterprises. The results showed that ISA is mostly measured via questionnaires. Round about 40 % of the questionnaires are based on the Knowledge-Attitude-Behavior-Model which is itself scientifically weak. According to studies measuring knowledge is not sufficient and,behavior has to be measured. Our results show that the answers of participants in questionnaires often differ from the truth due to wrong perception or social desirability bias. Therefore, behavior should be measured through behavior tests.

1. Introduction

In information security, humans play a central role. The behavior of workers at their workplace and at their home affects the confidentiality, integrity, and availability of sensitive corporate information. Risks can occur by a lost smartphone, a confidential document accidentally left on a desk, or a strange USB device used due to missing awareness of potential dangers. In addition, criminals exploit the "human factor" as a weak point with techniques such as phishing, malware, and social engineering [1]. Former social engineer Kevin Mitnick puts it this way: "Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk." [2] To make employees aware of their important role, companies typically carry out security awareness campaigns.

In order to determine the success, the effectiveness and the impact of such an awareness campaign, suitable measurement methods are required. In general, experiments or hypotheses cannot be verified without a suitable measurement method. For example, if a university aims to increase the information security awareness (ISA) of employees and students via an e-Learning campaign. To verify that the awareness indeed has increased, a suitable measurement method for security awareness is also required. The awareness level measured before the e-Learning campaign has to be compared with the awareness level measured after the campaign has been finished. In general, measurement results are required to justify the budget, to identify further opportunities for improvement, and to assess whether actions have been effective.

Moreover, the measuring of ISA is also important to determine the weak spots of the employees. Awareness trainings can only be effective and successful if they are not "one-size-fits-all", but individually address the weak spots [3]. Therefore, companies need a way to determine the ISA level of their employees. Since awareness campaigns are often iterative and aim at the continuous improvement of ISA the Deming circle can be applied. The Deming circle also known as plan-do-check-act, is an iterative four-step management method and requires measuring in order to check the effectiveness of activities [4].

We did a systematic literature review in order to determine the current state of the art about the measuring of ISA. Therefore, we analyzed published information about measuring as well as unpublished information of companies. We did some interviews with IT-security experts of small and medium-sized enterprises (SME).

At the beginning, we summarize the theoretical background. We cover three different definitions and models for information security awareness (ISA). Afterwards, we define our four research questions that we will answer within this paper. In Section "Research Approach" we describe our approach for this systematic literature review. In Section "Used Data Sources", we

URI: https://hdl.handle.net/10125/64540
978-0-9981331-3-3

present the journals, the digital libraries as well as our interview partners. Following the summary of used data sources, we gather the research results. The results are discussed in Section Results Discussion and we will answer our research questions. At the end, we will give a short summary of the paper and will conclude with an outlook and future work.

2. Theoretical Background

Security awareness targets the “human factor” and has established itself as a separate research area within information security. Moreover, security awareness focuses on how IT users can be brought to an information security-compliant behavior. IT users should be motivated to use their theoretical knowledge about information security in practice [5] and should be convinced of the importance of their actions. In practice, information security awareness campaigns mainly do one thing: In lectures, employees receive theoretical knowledge about information security. However, the actual behavior of an employee is hardly influenced by classical training.

Employees are believed to be important organizational assets and therefore, ISA is a critical factor on the overall information security of an organization. However, the employees require the ability to make decisive decisions regarding information security in certain situations. ISA can increase this ability [6].

According to both, Katsikas and Siponen the attention of individuals has to be directed to information security [7, 8]. Katsikas states that the individual has to realise the concern of information security [7]. Moreover, Siponen wants to ensure compliant behavior [8]. Al-Hamdani also agrees with Siponen but wants to ensure that users are accepting information security and can therefore respond accordingly [9]. De Maeyer has a slightly different definition for ISA: “an organized and ongoing effort to guide the behavior and culture of an organization in regard to information security issues” [10]. There are even more authors that define ISA as a direction of attention: Kritzinger and Smith, Tsohou et al., and Wilson and Hash [11, 12, 13]. Moreover, Kritzinger and Smith want to ensure that employees are not only aware about security awareness [11]. They need also to be aware of their role and responsibility.

There are other definitions of ISA besides the redirection of attention: Wolf et al. focus more on compliant behavior and state: “[ISA is] the effort to impart knowledge of or about factors in information security to the degree that it influences users behaviour to conform to policy” [14]. Bulgurcu et al. defined ISA as “an employees general knowledge about information security and his cognizance of the Information Security Policies of his organization” [15]. However, all mentioned definitions are not sufficient to describe ISA. ISA is a complex topic that requires whole models instead of short definitions. All definitions focus only on one single aspect of ISA. This is why, many models have been derived and will be presented in the following paragraphs.

Security Awareness was divided into three possible perspectives by Hänsch and Benenson [16]: “Perception”, “Protection”, and “Behavior”. “Perception” requires that employees know existing threats and are able to recognize them. If employees further know, how to protect themselves against threats, the perspective “Protection” is fulfilled. “Behavior” describes, that employees know what a threat is, what they can do about it and that they behave compliantly. However, only the perspective “Behavior” promises an actual increase in information security within the company. Regarding Hänsch and Benenson, raising ISA means that employees know how to behave in compliance with information security. Moreover, employees know what consequences non-compliant behavior has like loss of image and financial loss due to loss of customer data. Thus, the employees have to actually apply their knowledge in critical situations. However, the model of Hänsch and Benenson is only a summary of the previous ISA definitions their model lacks psychological aspects [16].

Hanus et al. did a structured literature review and defined a multidimensional model of security awareness [17]. Their model includes different factors like Information Security Policy Awareness, Previous Experience, Interest in Information Security and the Intention to Comply with Information Security Policies. Moreover, they defined six different hypotheses and did studies and tests against those hypotheses. Nevertheless, the model of Hanus et al. lacks also psychological aspects since the model is solely based on their literature review and the pre-existing definitions of ISA.

Since the previous definitions and models are not sufficient to define ISA, Schütz derived his own Integrated Behavorial Model (IBM) back in 2018 [3]. The IBM is based on the model of Montao and Kasprzyk [18]. The IBM describes how compliant behavior of employees is influenced by different factors. Those factors include knowledge, salience, habit, attitude, perceived norm, personal agency as well as environmental constraints.

3. Research Questions

Our research project focuses on methods to increase the ISA in small and medium-sized enterprises (SME). However, in order to determine if ISA has increased, we need measurements. Therefore, we are researching about the measurement of ISA and are executing this literature review. Moreover, we want to know if companies are already measuring the ISA of their employees.

Interviews and questionnaires are often used if a quantization of required information is hard to achieve. Using those approaches is fine but they require manual effort. Moreover, the use of questionnaires is affected by several response bias [19]. Regarding ISA the social desirability bias (SDB) is especially critical [20]. The employees could give answers different from truth during interviews or questionnaires if they believe the answer is viewed more favorably by others. Therefore, we aim to use an additional automated measuring system to detect the differences between the truth and the given answers. Moreover, if such an automated measuring system is possible, it has to be verified if it can successfully detect those differences.

Since our research project is focusing on ISA in SMEs, it is important to check whether such enterprises are already measuring ISA. Moreover, if those enterprises are already measuring ISA, we will research the techniques they use.

To sum up, within this literature review we will answer the following research questions:

Q1) What approaches are used in literature to measure ISA?

Q2) Are there any approaches for automated measuring of ISA?

Q3) Are SMEs already measuring ISA?

Q4) If SMEs are already measuring ISA, do they use any automation?

4. Research Approach

Table 1. Each keyword was AND concatenated with Information Security Awareness

Measuring	Metrics
Assessment	Assessing
Maturity Model	Adoption
Effectiveness	Training results
Success	Key Performance Indicators

In this section, we describe the approach for this structured literature review. We describe the identification and selection of relevant references. Therfore, we define the keywords for the search process and describe the coding used to filter the findings.

We used the proposed approach of Webster and Watson for the identification of relevant references [21]. The structured approach improves the search process, and the search process is fundamental for the quality of this literature review [22]. A thorough literature research must be valid and reliable according to Brocke et al. [22]. A valid literature research has to accurately uncover the sources the reviewer wants to collect [22, 23]. A reliable literature research has to be repeatable in order to allow other researchers to collect the same sources [22]. Therefore, we documented our research process:

According to Webster and Watson we started our search process by a keyword search using the pre-defined keywords shown in Table 1 [21]. All keywords were AND concatenated with the term ‘Information Security Awareness’. We limited our search to publications written in English. Moreover, we only used references that were published since 2000 to provide an up-to-date literature review. In order to filter publications that are not dealing with the topic of measuring security awareness we did a manual screening of all titles, abstracts and if neccessary of the full text. Afterwards, a backward as well as a forward search was carried out. Both searches were carried out manually.

In addition to the literature review we carried out several interviews with experts in order to retrieve unpublished approaches. The choice of interviewees determines the nature and quality of the results and must be included in the interpretation of the results. For this reason, the definition of an expert as well as the requirements should be clarified. After weighing definitions from other publications, Bogner et al. are defining an expert as persons able to structure a given field of action for others. They use their experience as well as their knowledge from practice [24]. Moreover, the chosen experts have to be representative for SMEs [25].

In the sense of the sample construction, a homogeneous targeted random sample was selected by theoretical considerations in order to answer the objectives. Characteristic of the homogeneous targeted random sample are few recruiting channels and a small sample. Initially, as recommended by Bogner et al., we defined the following requirements for the expert selection [24]: The experts should have been involved in the information security in an SME, either recently or in the past. Moreover, the experts should have initial experience in the areas of security awareness and information security measurement.

The experts were recruited by either snowball sampling [26] or targeted sampling [27]. Through our social network, the experts were recruited during the snowball sampling process. Since we could not recruit enough experts via snowball sampling, a modified variant of targeted sampling was used in addition. The Internet presence of companies working in the area of information security was scoured for typical certifications such as ISO27001 or Security Awareness as a service. Moreover, we tried to recruit experts geographically close to our research lab.

5. Used Data Sources

In this section we describe the used data sources and the papers found during the literature review. Moreover, we give an overview of experts chosen for our interviews. Based on our keyword search defined in Section 4 we found a total of 34 papers after removing the duplicates. Table 2 shows all used data sources and the number of hits during the search. Moreover, Table 2 shows how many papers were included and retrieved by forward and backward search. Table 2 is ordered by the order of searching the data sources. The numbers of included papers are without duplicates. Many of the digital libraries revealed the same papers. Therefore, the number of included papers was only increased if the data source revealed a new paper.

Since we started with IEEE Xplore Digital Library, we discovered the most relevant findings: 18 papers. The forward and backward search revealed two additional papers matching the inclusion criteria. The ACM Digital Library was searched afterwards and had 11 hits within the *ACM Full-Text Collection*. Therefore, we expanded our search to the *ACM Guide to Computing Literature* and got 95 hits. Since the *ACM Guide to Computing Literature* reveals also papers of other digital libraries, we had many duplicates compared to IEEE Xplore Digital Library. However, we could include additional 2 papers from the results and 1 additional paper via forward and backward search. The keyword based search on ScienceDirect revealed 216 hits. Based on the inclusion criteria we could include 3 of those papers.

Searching the Scitepress Digital Library and Springer Link did not result in new papers. Springer Link had 95,000 hits so we had to use additional filters: We used the Discipline Computer Science and Sub-Discipline Computer Science general which resulted in 648 hits. We could not include any additional paper after removing the duplicates.

After searching the digital libraries, we continued with manual searches within journals. Therefore, we chose journals, we already had papers included from. The journal *Review of Business Information Systems* resulted in 7 hits and 1 included paper. *Computers & Security* had the most results with 43 hits. We could include 2 papers and retrieved 2 additional papers via forward and backward search. All other journals covered did not uncover additional papers matching the inclusion criteria.

In addition to the journals we searched the conference proceedings of AIS conferences. Therefore, we used the AIS eLibrary. The AIS eLibrary had 235 hits but no additional paper was included after removing the duplicates. Last but not least, we used Semantic Scholar to cover other sources as well. The keyword search result had 222 hits and 3 papers matched our inclusion criteria. In addition we checked Github in order to reveal any open source tool for measuring ISA. However, we did not find any unpublished software dealing with our topic of interest.

Table 3 shows an anonymous list of companies we used for our interviews. We could recruit five experts for our interviews. The characteristics according to [24] are also shown in Table 3. We summarized the number of employees of the company, the position, age, and experience in years of our interviewee.

A partially or semi-structured interview should be used, if the expert interview is the method of choice in qualitative social research [24]. In the partially structured interview, the interviewer does not take a static role. This allows the interviewer to decide on the way the questions are to be discussed. Overall, new questions or a new question sequence can flexibly be used depending on the conversation situation. However, the partial or semi-structure of the interview is required due to the comparability of the results.

We transformed the objectives of our research into questions for the interviewee. After the interview, we evaluated the answers according to our objectives. The interview guideline combines open questions with narrative prompts and was designed according to the principles of communicative excitement [24]. The interview guideline was designed according to the presented methodology of Bogner et al. [24]. The questions have been split into key questions (S) and contingencies (E). The key questions are mandatory questions. The contingency questions have a supplementary character and are only used when points have not been answered by the key question.

We structered our interview guideline into the following six topics:

Table 2. Number of Search Hits and Included Papers per Data Source

Data Source	Hits	Included	Forward/Backward
IEEE Xplore Digital Library	648	18	2
ACM Digital Library	95	2	1
ScienceDirect	216	3	0
Scitepress Digital Library	2	0	0
Springer Link	648	0	0
Review of Business Information Systems	7	1	0
Computers & Security	43	2	2
Computers & Education	1	0	0
MIS Quarterly	1	0	0
Information Systems Research	3	0	0
International Journal of Computer Science and Information Security	0	0	0
Computer Fraud & Security	0	0	0
Information Systems Journal	2	0	0
AIS eLibrary	235	0	0
Semantic Scholar	222	3	0
Total Without Duplicates		**34**	

Table 3. List of Companies used for Interviews including number of employees, interviewee position, age of interviewee and experience in years of interviewee.

Company	Industrial Sector	# Employees	Interviewee Position	Age	Years
A	Offline & Online Shop	9	IT-Projectmanager	< 30	< 5
B	IT Service Provider	12	CEO	>= 50	>= 30
C	IT Service Provider	19	CEO	>= 50	>= 20
D	IT Service Provider	90	Data Security Officer	>= 30	>= 10
E	IT Service Provider	170	IS Manager	>= 30	>= 10

- Definition of Information Security Awareness (ISA)
- ISA within the company of the interviewee
- Requirements for Measuring ISA
- Requirements for Metrics
- Requirements for Performance Measurement Systems
- Closing Questions

6. Research Results

This section summarizes the research results of the literature review as well as the interviews.

6.1. Literature Results

The thematic analysis resulted in the mapping of nine categories. Table 4 shows the different categories and mappings of literature. Some of the papers were mapped to multiple categories if it was applicable. All categories are based on the used methodology to measure ISA. The objectives of the papers were not used for categorization since for our research it is not important why they wanted to measure ISA.

Table 4 shows that 31 of 34 papers are in a category that used questionnaires. However, some of them used additional measuring methods like behavior tests or benchmarks for example. In the following we discuss the different approaches in detail. Regarding the papers that only used questionnaires we will not discuss every single questionnaire in detail.

The category *Questionnaire & Survey* includes 16 papers. All of them are running questionnaires in order to determine the success of awareness campaigns or to assess the level of ISA of employees or students. Those questionnaires are executed over several weeks to gather enough participants. Some of the questionnaires are only knowledge-based, e.g., “What characters should a password contain?”. However, some contain questions about behavior or beliefs. Sari et al. checked whether measuring knowledge is significant and compared it to measuring behavior [40] The questionnaire of Fung et al. was very technical in contrast to other questionnaires [43]. Fung et al. focused mostly on knowledge about

Table 4. Categorization of found literature

Category	Found Papers
Questionnaire & Surveys	[28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43]
Questionnaire according to [44]	[45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57]
Interviews	[45, 32, 28]
Observation	[28]
Monitoring & Metrics	[31, 49, 58]
Benchmarks	[31]
Theory of reasoned action	[49]
Questionnaire & Behavior Tests	[59, 60]
Password Compliance	[14, 61]

security exploits

The category *Questionnaire according to [44]* includes 13 papers. Kruger et al. proposed a prototype for measuring ISA. They are splitting ISA in three factors: knowledge (K), attitude (A), and behavior (B). The idea of Kruger et al. was, that knowledge as well as the beliefs of the user (A) are influencing the behavior. They divided their questions in different areas of security, like passwords, email, and social engineering. Each area contains questions focusing on all three factors (KAB). This approach resulted in the KAB-model which is widely used in literature.

The category *Interviews* includes three papers. Parsons et al. are conducting a questionnaire according to the KAB-model [45]. Additionally, they interviewed the managers of the companies under test. They tried to determine if the managers have a good understanding of the ISA of their employees. Boujettif and Wang measured the ISA using a questionnaire and interviewed the Chief Information Officers (CIO) of the companies [32]. Marks et al. did also run additional interviews to retrieve more information about the ISA [28].

Only one paper was included in category *Observation*. Marks et al. explain that they observed the employees directly. During observation they gathered information about the behavior of employees and used that information to determine the ISA.

Three papers are included in the category *Monitoring & Metrics*. The proposed metrics are either collected automatically by monitoring mails, reports, networks, etc. or manually by the security group of the companies. Proposed metrics are the "number of help desk calls", "number of phishing mails", "number of accesses to intranet pages", and "number of accesses to unauthorized pages" [49]. Thomas is proposing additional metrics that are determined manually by the security group like "number of sensitive documents left in public areas" and "number of employees wearing their badges outside the building" [58].

One single paper was included in category *Benchmarks*. Scholl did a review on categories of measuring ISA and mentioned benchmarks [31]. Scholl mentions planned phishing attacks as example for benchmarks.

Khan used the KAB-model and extended it to a five-step ladder model [49]. His five-step ladder model uses the theory of reasoned action and theory of planned behavior. This is why we included his paper in the category *Theory of reasoned action*.

The category *Questionnaire & Behavior Tests* includes two papers. Both of them propose that knowledge tests are not enough to determine the ISA. They also propose to run behavior tests instead of asking questions about behavior due to the SDB [20].

The last category *Password Compliance* includes also two papers. Wolf et al. are measuring the quality of passwords multiple times [14]. Every test is executed a few days after awareness campaigns about password security. Eminağaoğlu is running multiple password strength audits to determine the ISA.

6.2. Interview Results

The current state of ISA within the companies was provided by the question about the implemented and planned security awareness programs. Moreover, we asked for possible approaches for measuring ISA. Subsequently, the motivation and the problems of measuring the ISA were revealed.

All companies had already established security awareness trainings. Four of the companies have gained additional experience through penetration tests in the area of ISA (B, C, D). Three of the companies carried out the ISO / IEC 27001 certification internally or at their customers (C, D, E). Two of the interviewees planned to introduce an awareness tool (D, E). On the one hand, the tool should be an awareness platform for the security awareness process including training of employees as well as measuring the success (D). On the other hand, the tool should be an awareness assessment tool for the employees (E). In order to reduce the number of security incidents, an extended version of seggregation of duties was introduced as method (B). In the event of a potential danger, colleagues as well as the Information Security Officer are contacted.

All companies are measuring ISA via metrics. Those metrics were called “soft values” (D). “Soft values” include number of trainings per employee (C, D, E), questionnaires to record compliant behavior and knowledge (B, C, E), number of employee interviews (B, E) and the degree of implementation of organizational measures (A, E).

No general statement can be made about the frequency of measurings. Two companies reported measuring before and after a training program (A, B). One company measures only during audits (D), and the other companies at quarterly or half-yearly intervals (B, E).

The main motivation for measuring ISA had been the measuring of success after awareness programs. The desire to measure success is due to both internal and external factors. The justification of the security trainings before the management is to be attributed to the internal factors. The customer was named as the driving external factor.

According to the experts, the problem of measuring is due to the abstract nature of ISA. In particular, quantifying human behavior and finding meaningful metrics has been cited as problematic.

7. Results Discussion

The results of the literature review as well as the interviews are used to answer our research questions proposed in Section 3. To answer Q1, we use the categories of the literature. ISA is currently measured either by questionnaires and surveys, questionnaires based on the KAB-model, interviews, observations, monitoring, metrics, benchmarks, and behavior tests. According to Scholl all categories can be grouped into the following three main areas: *Monitoring Security Procedures*, *Surveys*, and *Benchmarks* [62]. Therefore, the categories benchmarks, behavior tests and observations can be grouped together as well as the different categories for questionnaires and interviews. However, there are some issues with the current state-of-the-art of measuring ISA.

Round about 40 % use the proposed KAB-model of [44]. However, the scientific support for the knowledge component of the KAB-model is weak [63]. Baranowski states that within complex predictive models with very large samples, measures of knowledge were weakly related to physical activity behavior [63]. Moreover, Khan also extended the KAB-model into his five-step ladder model because of this weakness [49]. Sari et al. did also recognize that measuring knowledge has no significance only the measuring of behavior can be used to draw conclusions about the ISA [40]. Compliant behavior is the result of ISA and can, therefore, be used to draw conclusions about ISA according to Schütz [3]. Shepherd and Archibald measured behavior via questionnaires as well as via their firefox extension used by participants [60]. They discovered that all participants thought they revealed less privacy data than they actually did. Besides the SDB, the results of Shepherd and Archibald are another reason why measuring behavior via questionnaires is not sufficient and reliable.

The literature allows to answer Q2 as well. Automated measuring of ISA is always based on metrics or benchmarks. However, not all benchmark activities can be done automatically. The preparation and distribution of tests has to be carried out manually. Moreover, not all metrics can be supported by data automatically. However, literature shows that metrics can be measured automatically and that there exist already some tools to retrieve the required information. For example, the password strength audits can easily be automated. However, the password strength is not sufficient for an assessment of ISA but can be used to ensure the effectiveness of awareness programs [14]

To answer Q3 and Q4 we use the results of our interviews. The interviewed companies are already measuring ISA due to internal and external factors. They are using their measurements to ensure that awareness programs are successful and effective. Moreover, in case of ISO / IEC 270001 certifications they also need a way to measure their ISA. All companies argue that they are only measuring “soft values”. Their metrics are not able to draw scientific conclusions. Moreover, their metrics cannot be used to measure the ISA of their employees automatically. All companies are not measuring ISA automatically, yet, but would prefer an automated method.

According to the companies the main issue is the definition of metrics and the quantification of human behavior. Nevertheless, we learned during this literature review that the measurement of knowledge is not significant [40] and that the KAB-model is scientifically weak [63]. In order to achieve a significant way of measuring ISA, we have to measure the behavior of employees. Therefore, we have to define metrics, that allow us to quantify human behavior. Those metrics are required in research as well as in industry.

8. Conclusion

We carried out a systematic literature review to answer the research questions how ISA is currently measured in theory and practice and how it can be automated. To gather information about industry we carried out five interviews with SMEs. We discovered that measuring ISA is mainly achieved via questionnaires. Many of the questionnaires are based on the KAB-model, which is itself scientifically weak [63]. Moreover, measuring of knowledge was not significant in the research of Sari et al. [40]. Since compliant behavior is the result of ISA, the behavior has to be measured. However, many studies measure behavior via questionnaires which can lead to results different from the truth [60]. According to the interviewees the quantification of human behavior is the main issue in the field of measuring ISA.

In our future work we want to define metrics that allow to quantify human behavior. Moreover, the metrics should be measured automatically. This allows to create a dashboard with metrics than can easily be tracked on a day-by-day basis. Moreover, those metrics should adhere to the IBM model of Schütz [3].

Another research topic will be how to change behavior of employees. We assume that behavior is the result of ISA. Therefore, we have to increase the ISA of the employees in order to achieve a change in behavior. Since measuring behavior seems to be a promising way for measuring ISA, we could easily check the success of new methods.

Acknowledgements

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

References

[1] 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.

[2] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. New York, NY, USA: John Wiley & Sons, Inc., 2002.

[3] 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.

[4] P. J. Koiesar, "What Deming Told the Japanese in 1950," *Quality Management Journal*, vol. 2, no. 1, pp. 9–24, 1994.

[5] 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.

[6] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pp. 248–252, Dec. 2014.

[7] S. K. Katsikas, "Health care management and information systems security: awareness, training or education?," *International Journal of Medical Informatics*, vol. 60, pp. 129–135, Nov. 2000.

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

[9] W. A. Al-Hamdani, "Assessment of Need and Method of Delivery for Information Security Awareness Program," in *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, InfoSecCD '06, (New York, NY, USA), pp. 102–108, ACM, 2006. event-place: Kennesaw, Georgia.

[10] D. De Maeyer, "Setting up an Effective Information Security Awareness Programme," in *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference* (N. Pohlmann, H. Reimer, and W. Schneider, eds.), pp. 49–58, Wiesbaden: Vieweg, 2007.

[11] E. Kritzinger and E. Smith, "Information security management: An information security retrieval and awareness model for industry," *Computers & Security*, vol. 27, pp. 224–231, Oct. 2008.

[12] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "Investigating Information Security Awareness: Research and Practice Gaps," *Inf. Sec. J.: A Global Perspective*, vol. 17, pp. 207–227, Jan. 2008.

[13] M. Wilson and J. Hash, "SP 800-50. Building an Information Technology Security Awareness and Training Program," tech. rep., National Institute of Standards & Technology, Gaithersburg, MD, United States, 2003.

[14] M. Wolf, D. Haworth, and L. Pietron, "Measuring An Information Security Awareness Program," *Review of Business Information Systems (RBIS)*, vol. 15, pp. 9–22, July 2011.

[15] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, pp. 523–548, Sept. 2010.

[16] 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.

[17] B. Hanus, J. C. Windsor, and Y. Wu, "Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order," *SIGMIS Database*, vol. 49, pp. 103–133, Apr. 2018.

[18] 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.

[19] D. L. Paulhus, "Measurement and control of response bias," in *Measures of personality and social psychological attitudes*, Measures of social psychological attitudes, Vol. 1., pp. 17–59, San Diego, CA, US: Academic Press, 1991.

[20] 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.

[21] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002.

[22] J. v. Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven, "Reconstructing the giant: On the importance of rigour in documenting the literature search process," in *ECIS*, 2009.

[23] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' Information Security Awareness and Behavior: A Literature Review," in *2013 46th Hawaii International Conference on System Sciences*, pp. 2978–2987, Jan. 2013.

[24] A. Bogner, B. Littig, and W. Menz, eds., *Interviewing Experts*. ECPR Research Methods, Palgrave Macmillan UK, 2009.

[25] U. Flick, *An Introduction to Qualitative Research*. SAGE, 2014. Google-Books-ID: o5l7DwAAQBAJ.

[26] L. A. Goodman, "Snowball Sampling," *The Annals of Mathematical Statistics*, vol. 32, pp. 148–170, Mar. 1961.

[27] J. K. Watters and P. Biernacki, "Targeted Sampling: Options for the Study of Hidden Populations," *Social Problems*, vol. 36, no. 4, pp. 416–430, 1989.

[28] A. Marks and Y. Rezgui, "A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing," in *2009 International Conference on Management and Service Science*, pp. 1–7, Sept. 2009.

[29] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A survey of cyber-security awareness in Saudi Arabia," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 154–158, Dec. 2016.

[30] G. Kiss and A. Szasz, "Analysing of the information security awareness of the economic information technology students," in *2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI)*, pp. 000213–000218, Nov. 2016.

[31] M. Scholl, K. Leiner, and F. Fuhrmann, "Blind spot: Do you know the effectiveness of your information security awareness-raising program?," in *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, pp. 361–366, 2017.

[32] M. Boujettif and Y. Wang, "Constructivist Approach to Information Security Awareness in the Middle East," in *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, pp. 192–199, Nov. 2010.

[33] T. Velki, K. Solic, and H. Ocevcic, "Development of Users' Information Security Awareness Questionnaire (UISAQ) Ongoing work," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1417–1421, May 2014.

[34] L. Li, W. He, L. Xu, A. Ivan, M. Anwar, and X. Yuan, "Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study," in *2014 Enterprise Systems Conference*, pp. 169–173, Aug. 2014.

[35] N. Innab, H. Al-Rashoud, R. Al-Mahawes, and W. Al-Shehri, "Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh," in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, pp. 1–5, Apr. 2018.

[36] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security*, vol. 29, pp. 432–445, June 2010.

[37] N. Waly, R. Tassabehji, and M. Kamala, "Improving Organisational Information Security Management: The Impact of Training and Awareness," in *2012 IEEE 14th International Conference on High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems*, pp. 1270–1275, June 2012.

[38] Z. A. Alzamil, "Information Security Awareness at Saudi Arabians Organizations: An Information Technology Employees Perspective," *International Journal of Information Security and Privacy (IJISP)*, vol. 6, no. 3, pp. 38–55, 2012.

[39] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 352–359, Aug. 2015.

[40] P. K. Sari, Candiwan, and N. Trianasari, "Information security awareness measurement with confirmatory factor analysis," in *2014 International Symposium on Technology Management and Emerging Technologies*, pp. 218–223, May 2014.

[41] A. P. Filippidis, C. S. Hilas, G. Filippidis, and A. Politis, "Information security awareness of greek higher education students #x2014; Preliminary findings," in *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, pp. 1–4, May 2018.

[42] G. Kiss and A. Szasz, "Level of the information security awareness of the mechanical engineering students," in *2016 15th International Conference on Information Technology Based Higher Education and Training (ITHET)*, pp. 1–6, Sept. 2016.

[43] C. C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, and P. Boonbrahm, "Raising information security awareness in digital ecosystem with games - a pilot study in Thailand," in *2008 2nd IEEE International Conference on Digital Ecosystems and Technologies*, pp. 375–380, Feb. 2008.

[44] H. Kruger and W. Kearney, "A protoype for assesing information security awareness: A West Africa gold mining enviroment case study," *Computers and Security*, vol. 4, no. 25, 2006.

[45] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations," *Information Management & Computer Security*, vol. 22, pp. 334–345, Oct. 2014.

[46] M. Hassanzadeh, N. Jahangiri, and B. Brewster, "Chapter 6 - A Conceptual Framework for Information Security Awareness, Assessment, and Training," in *Emerging Trends in ICT Security* (B. Akhgar and H. R. Arabnia, eds.), pp. 99–110, Boston: Morgan Kaufmann, Jan. 2014.

[47] T. Gundu, S. Flowerday, and K. Renaud, "Deliver Security Awareness Training, then Repeat: Deliver; Measure Efficacy," in *2019 Conference on Information Communications Technology and Society (ICTAS)*, pp. 1–6, Mar. 2019.

[48] K. Parsons, A. McCormac, M. A. Butavicius, M. R. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165–176, 2014.

[49] Bilal Khan, "Effectiveness of information security awareness methods based on psychological theories," *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, vol. 5, Oct. 2011.

[50] T. Gundu and S. V. Flowerday, "Ignorance to Awareness: Towards an Information Security Awareness Process," *SAIEE Africa Research Journal*, vol. 104, pp. 69–79, June 2013.

[51] D. D. H. Wahyudiwan, Y. G. Sucahyo, and A. Gandhi, "Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, pp. 654–658, Oct. 2017.

[52] A. Kusumawati, "Information Security Awareness: Study on a Government Agency," in *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, pp. 224–229, Nov. 2018.

[53] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, "Measurement of Employee Information Security Awareness Using Analytic Hierarchy Process (AHP): A Case Study of Foreign Affairs Ministry," in *2018 International Conference on Computing, Engineering, and Design (ICCED)*, pp. 52–56, Sept. 2018.

[54] P. K. Sari and C. Candiwan, "Measuring Information Security Awareness of Indonesian Smartphone Users," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 12, pp. 493–500, June 2014.

[55] A. Cindana and Y. Ruldeviyani, "Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm," in *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, pp. 289–294, Oct. 2018.

[56] I. Veseli, "Measuring the Effectiveness of Information Security Awareness Program," Master's thesis, Gjøvik University College, 2011.

[57] A. Gandhi, "Quantitative Assessment of Information Security Awareness on Informatics Students in a University," in *Proceedings of the 2017 International Conference on Information Technology*, ICIT 2017, (New York, NY, USA), pp. 346–350, ACM, 2017. event-place: Singapore, Singapore.

[58] V. Thomas, "Chapter 13 - Measuring Effectiveness," in *Building an Information Security Awareness Program* (B. Gardner and V. Thomas, eds.), pp. 119–124, Boston: Syngress, Jan. 2014.

[59] H. A. Majid, M. A. Majid, M. I. Ibrahim, W. N. S. W. Manan, and M. R. Ramli, "Investigation of security awareness on e-learning system among lecturers and students in Higher Education Institution," in *2015 International Conference on Computer, Communications, and Control Technology (I4CT)*, pp. 216–220, Apr. 2015.

[60] L. A. Shepherd and J. Archibald, "Security awareness and affective feedback: Categorical behaviour vs. reported behaviour," in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1–6, June 2017.

[61] M. Eminağaoğlu, E. Uçar, and Ş. Eren, "The positive outcomes of information security awareness training in companies A case study," *Information Security Technical Report*, vol. 14, pp. 223–229, Nov. 2009.

[62] M. C. Scholl, F. Fuhrmann, and L. R. Scholl, "Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 2235–2244, 2018.

[63] T. Baranowski, K. W. Cullen, T. Nicklas, D. Thompson, and J. Baranowski, "Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts?," *Obesity Research*, vol. 11, no. S10, pp. 23S–43S, 2003.