Measuring the Impact of E-Learning Platforms on Information Security Awareness

Tobias Fertig(✉), Andreas E. Schütz, Kristin Weber, and Nicholas H. Müller

Faculty of Computer Science and Business Information Systems,
University of Applied Sciences Würzburg-Schweinfurt,
Sanderheinrichsleitenweg 20, 97074 Würzburg, Germany
{tobias.fertig,andreas.schuetz,kristin.weber,nicholas.mueller}@fhws.de

Abstract. Humans play a central role in information security. The behavior of workers at their workplace affects the confidentiality, integrity, and availability of sensitive corporate information. In addition, attackers exploit the "human factor" as a weak point with techniques such as phishing, malware, and social engineering. Exploiting the lack of awareness is often an easy task with minimal risk. To make employees aware of their important role, companies typically carry out security awareness campaigns. Our university created an e-Learning Platform (eLP) to support our awareness campaigns. In order to determine the success, the effectiveness and the impact of such an awareness campaign, suitable measurement methods are needed. A common approach to measure the success of eLPs is to run surveys and questionnaires with the learners. Since the manual evaluation of those surveys and questionnaires is a time-consuming task, we are researching how a possible automation can be achieved. Moreover, the effectiveness is often evaluated through quizzes or knowledge tests. Since knowledge by itself does not improve the behavior of people, the compliant-behavior has to be measured, too. We derived metrics for success and effectiveness but recognized that success can hardly be measured automatically. To reduce the manual effort we decided to only measure the effectiveness automatically. Therefore, we are measuring the behavior and determine if the security-compliance has increased.

Keywords: Information security awareness · Measuring · e-Learning Platforms · Success · Effectiveness · Automated measuring

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

P. Zaphiris and A. Ioannou (Eds.): HCII 2019, LNCS 11590, pp. 26–37, 2019.
https://doi.org/10.1007/978-3-030-21814-0_3

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 [12]. 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 [18]." To make employees aware of their important role, companies typically carry out security awareness campaigns [11,27].

In order to determine the success, the effectiveness and the impact of such an awareness campaign, suitable measurement methods are needed. In general, experiments or hypotheses cannot be verified without a suitable measurement method. For example, our university aims to increase the information security awareness 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 needed to justify the budget, to identify further opportunities for improvement, and to assess whether actions have been effective.

In order to increase the information security awareness of employees and students, our university created an e-Learning Platform (eLP) about information security to run e-Learning campaigns. The eLP was created as part of a research project and contains slides, lectures and information about security issues and possible attack vectors. Moreover, the platform provides quizzes and other knowledge tests.

Based on related work on measuring the success of eLP, metrics were derived to provide information on whether the participants' security awareness has increased. The derived metrics and results of our research will be used to answer the following research questions:

(Q1) How is the success and effectiveness of eLPs measured in general?
(Q2) How can the impact of eLPs on information security awareness be measured?
(Q3) Is it possible to automate the measurement of success and effectiveness impact?

At the beginning, we summarize related work on security awareness, measuring success and effectiveness of eLPs, and measuring security awareness. In Sect. 3, we evaluate existing metrics to measure the success and effectiveness of eLPs and group them into categories. This evaluation of metrics is based on a literature review. In Sect. 4 we introduce our project in which the eLP and the measuring was executed. Afterwards, we discuss the advantages and disadvantages as well as the limitations of our approach. Finally, we give a short summary of the paper and describe our future work.

2 Related Work

2.1 Security Awareness

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 [2] and should be convinced of the importance of their actions [9]. 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 [28].

An additional aspect of information security awareness is organization, which was described by Helisch and Pokoyski [11]. They mention that the organization ensures that employees in the company are able to behave in compliance with information security. Therefore, the organization ensures that no barriers exist, which are in conflict with compliant behavior. For example, a hidden password change link within the depths of the company intranet can be such a barrier. Additionally, organizational measures, such as increasing the usability of applications, can support information security and lead to greater acceptance. The acceptance will then increase the compliant behavior of employees. Information security awareness is thus an interaction of cognition (understanding of the problem and the knowledge to solve it), intention to act (will of the employee to behave in accordance with information security) and the organization [11].

Since the three interactions are not sufficient to define information security awareness, we derived our own Integrated Behavorial Model (IBM) [22]. Our IBM is based on the model of [20]. The IBM describes how compliant behavior of employees is influenced by different factors. Those factors include the knowledge, salience, habit, attitude, perceived norm, personal agency as well as environmental constraints. Using an eLP to increase the information security awareness has to cover the different factors in order to establish a holistic approach.

2.2 Measuring Success and Effectiveness of E-Learning Platforms

The definition of metrics is a prerequisite for measuring the success and effectiveness of eLPs. The metrics are needed to compare the current state with the desired target state. Figure 1 shows the IT controlling cycle of [15]: First, a goal has to be defined - secure behavior of stuff members. Then the metrics for measuring the goal are identified and defined, target values are set. Subsequently, the current state is measured and compared with the target state. In an analysis, conclusions are drawn about actions that are to be implemented to achieve the goal.

There are mainly two different types of metrics for eLPs: those for success and those for effectiveness. Metrics that are focusing on success are often derived from the DeLone and McLean model of information systems success (D&M model)

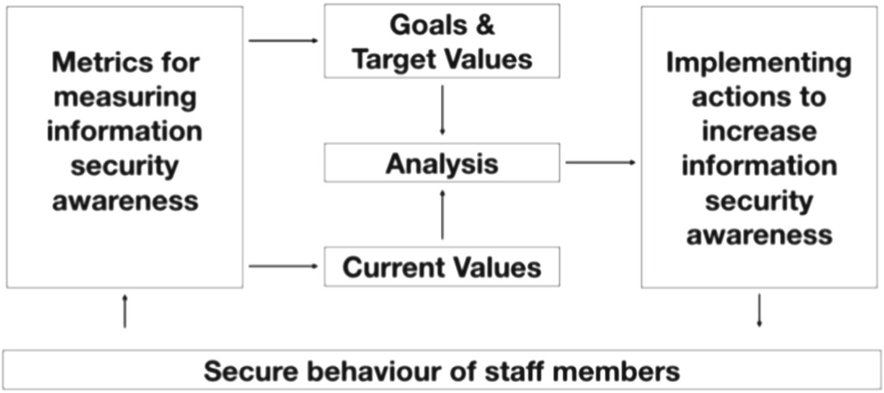
Metrics for measuring information security awareness
Goals & Target Values
Analysis
Current Values
Implementing actions to increase information security awareness
Secure behaviour of staff members

Fig. 1. Controlling cycle for secure behavior [15].

[5]. The derived models focus on the satisfaction of learners besides the other categories. Mainly, because the satisfaction will lead to a better adoption of the eLP by the learners. Adoption means that the learners accept the eLP as a tool to acquire knowledge. The adoption will than generate impact on the outcomes of the e-learning campaign [6,10,16,26]. However, measuring the adoption itself does not necessarily change the behavior of the learners. The Kirkpatrick Evaluation Method describes four levels of learning evaluation [14]. The first level focuses also on learner's satisfaction, whereas the other three levels focus on the results and outcome. Therefore, the Kirkpatrick Evaluation Method can also be divided into the evaluation of success and effectiveness: Satisfaction is part of the success measuring, whereas results and outcome are part of the effectiveness measuring.

The effectiveness of eLPs has to be measured separately to ensure that the adoption of the eLP leads to an improvement of skills. Noesgaard et al. clustered a total of 92 papers according to the definition of effectiveness described within those papers [21]. They distinguish between the effectiveness measured for higher education and for work-related learning. Work-related learning in this case means, that the learners train their knowledge required to fulfill their work or required by their organization. Papers targeting the higher education focused on the learning outcome and compared the grades of e-learners and traditional learners. Papers focusing on work-related learning always defined the effectiveness based on the application to practice.

2.3 Measuring Awareness

We proposed our process to determine how aware the employees are in [22]. Before companies can start influencing the behavioral factors of their employees within the context of an information security awareness campaign, they must carry out an as-is analysis. The aim of this analysis is to find out how strong the individual factors are and which emotions or beliefs prevail in the company regarding information security-compliant behavior. For example, the employees could believe that security is not an issue in their case, because they do not have critical information on their computers. Another example could be that the security is only overhead for employees so that they are not willing to act security-compliant. Montaño and Kasprzyk [20] recommend carrying out a qualitative study in form of interviews. The interviews identify the most salient problems. 15–20 employees of each target group, that has to participate on the eLP, should be interviewed to obtain the following information [20]:

- Experiential attitude: What positive or negative emotions exist regarding the behavior?
- Instrumental attitude: Which positive or negative attributes or outcomes result from the behavior?
- Normative influencers: Which influential individuals or groups support the behavior or are against it?
- Control beliefs and self-efficacy expectations: What situational barriers or supportive factors hinder or support the behavior.

From the findings gathered in the interviews, a questionnaire for a quantitative evaluation can be prepared [13]. A large portion of the employees within the company should answer it. To compose the questionnaire, the beliefs collected in the first step are generalized, transformed into questions and assigned to the four factors knowledge and skills, salience, habit and intention [13]. A question about the normative beliefs could be: “My manager influences me in my working with USB flash drives”. A behavioral belief might look like this: “Locking my screen is unnecessary because I have no important data on my computer.” Employees respond to a five-point scale ranging from “I disagree” to “I agree” or similar [19]. It is also possible to query the factors knowledge and skills as well as habit (e.g., through the “Self-Report Habit Index” [25]). In order to be efficient, the survey should be computer-aided, and employees should handle it within a reasonable time (e.g., 15 to 20 min). The computer-aided analysis of the survey results provides information about the manifestation of the respective behavioral factors in the company.

3 E-Learning Metrics

Several sources have been reviewed to gather metrics for the success of eLP. Figure 2 shows the updated D&M model [4,5], which is often derived by approaches for measuring the success of eLPs. However, there exist also approaches that are independent of the D&M model. In the following, we will first analyze the approaches that extend the D&M model. In addition, we examine independent approaches to define additional metrics. All approaches are working with questionnaires to obtain the actual values for each metric.

Manisi et al. have produced a literature review summarizing the categories of the D&M model [17]. [16] and [26] both used the D&M model as a basis and defined various metrics for all categories. The first category is ‘Intension to

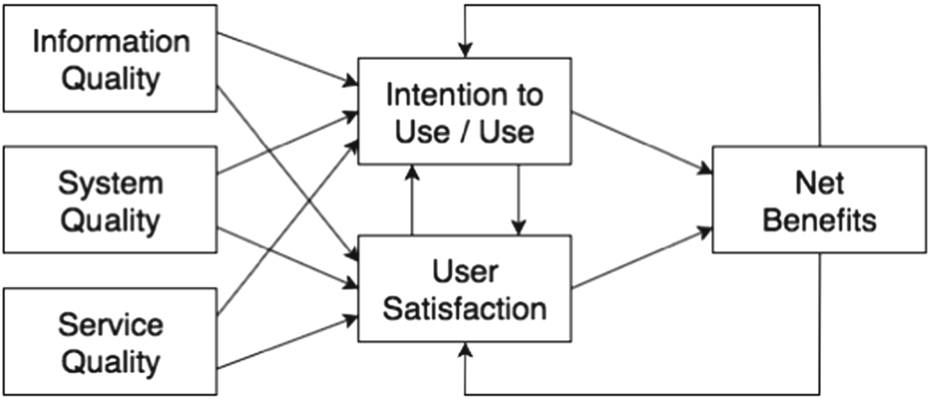

Fig. 2. Updated D&M model based on [5]

Use/Use'. [17] and [10] mention here that the intention of the user can already exist before the actual usage. From a student's point of view, usage also depends on how useful it appears [7,24]. In this category, [26] measures how often the eLP is being used, whether it is voluntary and whether the user depends on the system. [16] additionally measure the intension of the user: Is the eLP useful and if the user would recommend the eLP to others. In addition, interpersonal statements are also tested: e.g. Users use the eLP to receive rewards. [6] proposed an approach independent from the D&M model. They ask the users about future use.

The next category is 'User Satisfaction'. The D&M model describes the satisfaction of the user after interacting with the system. In addition, [17] and [24] explain that the expectations of the user and the usefulness for the core business also play a role. [16] and [26] each ask three questions about how satisfied the user is with the system, its information, and the interaction. Also, [6] ask questions about the overall satisfaction of the user.

The next category is 'System Quality'. The quality of the eLP depends on the quality of its hardware and software [24]. However, reliability, response time and ease of use are also critical for the System Quality, according to the D&M model. [16] ask questions to get information about reliability, response time and ease of use. [26] extend these factors to include personalized information presentation and attractive features. Moreover, the independent approach of [6] covers the complexity of the eLP within their survey.

The category 'Information Quality' is defined by [10] as the overall quality of the output of the eLP. According to [7], however, security should also be taken into account when measuring information quality. Users are asked if the eLP information is correct, if relevant information is being taught in the lessons, or if the information is up to date [16]. In addition, [26] checks whether the information is communicated at the right time and whether the information is understandable enough. The independent approach considers Authentic Learning, which can be assigned to the category Information Quality [6].

The 'Service Quality' category, according to [10], analyzes the effectiveness and efficiency of the technical support provided to the eLP. This category plays a very important role in the success of the eLP as technically ineligible users could be intimidated by the eLP. These users would then, with dislike, use the eLP and not achieve the desired learning success [23]. In [16], this category is interpreted a little differently and also checks the response time or whether information is correct. However, [26] ask questions about online assistance and support. There is also an analogy in [6] for this category: Technical support.

The last category is 'Net Benefits'. Here, it should be checked whether the eLP has really brought any benefit to the user. According to [1] the satisfaction of the learners plays a central role. Both [26] and [16] ask the user if he can apply the learned knowledge. In addition, [6] queried the age of the users to determine if it had an impact on individual impact.

Another approach that does not depend on the D&M model was shown in [3]. There, both students and staff were interviewed about the eLP. All asked questions can be classified in one of the categories described above and thus no additional metrics result.

4 Project Background

With the widespread use of new, digital services, the importance of information security is increasing. The University of Applied Sciences Würzburg-Schweinfurt has to protect their infrastructure, privacy data, research data and financial data against possible attacks. Moreover, a new e-governance law as well as a new data privacy policy was released. Therefore, our university launched an information security project to increase the security awareness of employees and students. Within the project, the university wants to train security-compliant behavior and to increase the knowledge about security-related topics. To support the project an eLP was created. The purpose of the eLP is to inform users to security risks, and to train them such as being able to better recognize phishing mails. As the creation and management of an eLP requires many resources, the university wanted to know if learners' information security awareness really improved.

Since our research project focuses on the human factor and security awareness in an organizational environment, we are focussing on work-related learning. We try to improve the security awareness so that the learning outcomes can be applied to the practice. Therefore, within our project the effectiveness of eLPs is defined as transfer described by Noesgaard et al. [21]. In order to measure the application to practice, we have to measure the security awareness before the e-learning campaign and afterwards. We can than determine the impact of the eLP on security awareness. However, we have to measure the success of our eLP also, in order to determine if the learners have used the eLP.

5 Research Results

In order to determine if the learners' information security awareness really improved, we had to answer research question Q1 and evaluate how success and effectiveness of eLPs is measured. The literature review showed that many universities and also companies are measuring the success and effectiveness of eLP. Most of the measurements of success are based on the D&M model or can at least be derived from it [5]. Even the proposed models that are not directly based on the D&M model cover related categories with their metrics. All reviewed papers are using surveys or questionnaires in order to determine the success of their eLP. Some researchers are even evaluating the success by interviews. However, many questions rely on the knowledge of the learners, like for example "The information provided by eLP is accurate" [16]. In our opinion, the information quality cannot be measured based on the answers to this questions. A learner who is new to the topic cannot decide properly whether the information is accurate.

Many researchers use surveys and questionnaires also regarding the effectiveness of eLP. The results are then analyzed and evaluated based on different definitions for effectiveness. Companies are defining the effectiveness mainly as the ability to apply the knowledge in practice or transfer of knowledge. Whereas, universities define effectiveness based on the improved grades of their students [21]. In our case, we are not interested in grades of the learners since we want to increase the information security awareness. Therefore, we are defining our effectiveness as transfer of knowledge. However, the general approach to measure the success and effectiveness manually per surveys and questionnaires does not meet our requirements.

Research question Q2 focused on the effectiveness of eLP on information security awareness. In order to measure the effectiveness on information security awareness we need to know the current state of our learners. Therefore, we have to measure the information security awareness of staff and students of our university, which is itself a challenging task. According to our process in Sect. 2.3 we first interviewed about 30 employees for the qualitative analysis. To accomplish the quantitative analysis we run a survey on all our employees and students. The evaluation of results has to be done manually. In order to determine the effectiveness of our eLP, we had to repeat this process. Afterwards, we could determine if the awareness has increased. Nevertheless, a better solution is required, since we defined the effectiveness as application to practice. Based on the answers of our learners we could only draw conclusions about the knowledge but not really about their ability to apply the learned knowledge to practice.

Since measuring the success and the effectiveness manually is a time consuming task, we tried to automate the measuring. Therefore, we determined if the metrics in Sect. 3 are able to be automated for measurement. The first category 'Intention to Use/Use' can be measured automatically. Therefore, the online times of our learners have to be tracked. However, the intention to use itself cannot be measured automatically since the users have to be asked about their intentions. The 'User Satisfaction' cannot be measured without assumptions or without asking the users for their satisfaction. An overall rating could be gathered easily, but no further information about the learners' expectations.

The 'System Quality' which was defined by the reliability, response time and ease of use can also not be measured automatically. A monitoring system could send requests to the eLP to measure the response time, but the ease of use has to be measured by surveys or questionnaires again. The second dimension of 'System Quality' focuses on data accuracy and completeness which is also not possible to measure automatically. In order to measure the 'Information Quality' the learner has to be asked to answer all questions concerning the learners' needs, understandings and requirements. Moreover, metrics focusing on relevance and actual information cannot be gathered automatically. 'Service Quality' is the third quality criteria focusing on online assisstance and support. To measure the satisfaction an overall rating can also be collected automatically. However, for detailed analysis surveys and questionnaires are required also.

The last category of 'Net Benefits' can be measured by measuring the effectiveness of our eLP. An impact during the e-Learning campaign is not expected and therefore, it is sufficient to measure the impact and effectiveness afterwards. To sum up, we can answer question Q3 so that an automated measuring of success is not sufficient since only few aspects can be measured. The effectiveness however, can be measured automatically by measuring the information security awareness before and after the e-Learning campaign. In order to do so, we created a prototype for a monitoring tool. The monitoring tool tracks the behavior of employees and creates anonymous reports within a dashboard.

The prototypical approach was chosen because it helps to formulate the requirements for an information system more precisely and to prove the technical feasibility. Basically, it reduces the number of uncertain assumptions in a software project. Therefore, an explorative prototype was created in the context of our project. The requirements for the prototype were defined within the exploratory preparatory work. In addition, the privacy of personal data introduced further requirements. The prototype tests the measurability of metrics and proves the general feasibility of the approach, including data privacy compliance. For this purpose, a client-server application was developed: The server manages indicators and events that the client has previously collected. The client collects security-relevant data on the workstations of the employees and sends them pseudonymous to the server for evaluation and anonymization by grouping. To enable a pseudonymous login, departmental logins are used. All clients of a department use the same login for authentication. The larger the departments are chosen, the higher the degree of anonymity. By configuring a measurement interval, the metrics are always randomly measured. A complete record of the activities of a person is thus, for privacy reasons, not possible.

An IT admin can configure the login data. The configuration used for the survey is initially downloaded from the server. In a pre-defined interval, the client application now checks to see if thresholds of the active measures have been exceeded. The server refreshes the list of recent events and increases the value of non-critical events as a whole. The server includes a dashboard that provides a quick overview of the number of critical or non-critical incidents. The dashboard also shows a temporal course of the incident frequency in the last week.

The following list summarizes a few of the metrics our prototype can cover:

- The time of inactivity without a locked screen.
- The time interval from receiving an email until opening the attachments.
- The frequency of password changes.
- The installed software. And the installed unauthorized software.
- The amount of external USB devices used.

The combination of metrics can be used to decide whether an event is critical or not: An installation of disallowed software is more critical if an email attachment was opened before. Moreover, if external USB devices have been connected, the installation is also more critical.

We decided to only measure the effectiveness of our eLP, since the effectiveness is the more relevant information to us. Moreover, the effectiveness is part of the success within the category 'Net Benefits'. Therefore, we can reduce the efforts by discontinueing the manual measurements for the success of our eLP. Hagen et al. described that eLP has to be used repetitive in iterations so that the learners' do not forget the security details [8]. The reduced effort is even more helpful if we run repetitive e-Learning campaigns.

However, we have some limitations with this approach. The measuring of effectiveness can only be done before and after the e-Learning campaign. If assumptions about the success should be made, metrics are required, that can be determined during the campaigns. Another drawback is that, the metrics should not be used in isolation. A single metric can improve even if the learners did not use the eLP. Therefore, some usage statistics should be collected to verify that the eLP is useful.

6 Conclusion and Future Work

Our goal was to measure the success, impact and effectiveness of eLP on information security awareness. We evaluated several metrics and determined which metrics can be measured automatically and which require manual efforts. Afterwards, we decided to only measure the effectiveness and the impact of our eLP. Therefore, we can use our prototype that gathers random data about the behavior of our learners.

Our next goal is to run repetitive campaigns and check whether the information security awareness can be steadily increased. Those repetitive campaigns will also help to ensure that the knowledge of our learners becomes stable in the long-term. Moreover, we will run some empirical studies about the impact of eLPs based on the collected data.

Another goal is to evaluate gamification concepts. We assume that it would be easier to derive metrics for the success of our eLP based on the gamification concepts. For example, the character level or the user's achievements can be used. Based on those metrics, we can then verify if a successful campaign will lead to higher impact and effectiveness.

References

1. Aparicio, M., Bacao, F., Oliveira, T.: Cultural impacts on e-learning systems' success. Internet High. Educ. **31**, 58–70 (2016). https://doi.org/10.1016/j.iheduc.2016.06.003. http://www.sciencedirect.com/science/article/pii/S1096751616300367
2. Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: why do they fail to change behaviour? In: Global Cyber Security Capacity Centre: Draft Working Paper, pp. 188–131 (2014)
3. Bell, M., Farrier, S.: Measuring success in e-learning-a multi-dimensional approach. Electron. J. e-Learn. **6**(2), 99–110 (2008). https://eric.ed.gov/?id=EJ1098718
4. DeLone, W.H., McLean, E.R.: Information systems success: the quest for the dependent variable. Inf. Syst. Res. **3**(1), 60–95 (1992). https://doi.org/10.1287/isre.3.1.60. http://pubsonline.informs.org/doi/abs/10.1287/isre.3.1.60
5. DeLone, W.H., McLean, E.R.: The DeLone and McLean model of information systems success: a ten-year update. J. Manage. Inf. Syst. **19**(4), 9–30 (2003). https://www.jstor.org/stable/40398604
6. Fleming, J., Becker, K., Newton, C.: Factors for successful e-learning: does age matter? Educ. + Training **59**(1), 76–89 (2017). https://doi.org/10.1108/ET-07-2015-0057. http://www.emeraldinsight.com/doi/10.1108/ET-07-2015-0057
7. Freeze, R.D., Alshare, K.A., Lane, P.L., Wen, H.J.: IS success model in e-learning context based on students' perceptions. J. Inf. Syst. Educ. **21**, 13 (2014)
8. Hagen, J., Ole Johnsen, S., Albrechtsen, E.: The long-term effects of information security-learning on organizational learning. Inf. Manage. Comput. Secur. **19**(3), 140–154 (2011). https://doi.org/10.1108/09685221111153537. https://www.emeraldinsight.com/doi/full/10.1108/09685221111153537
9. Harich, T.W.: IT-sicherheit im Unternehmen. mitp Professional, mitp-Verlags, Frechen, [Germany], 1. auflage edn. (2015)
10. Hassanzadeh, A., Kanaani, F., Elahi, S.: A model for measuring e-learning systems success in universities. Expert Syst. Appl. **39**(12), 10959–10966 (2012). https://doi.org/10.1016/j.eswa.2012.03.028. http://www.sciencedirect.com/science/article/pii/S0957417412004988
11. Helisch, M., Pokoyski, D.: Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Vieweg+Teubner Verlag/GWV Fachverlage GmbH Wiesbaden, Wiesbaden (2009). https://doi.org/10.1007/978-3-8348-9594-3
12. ISACA: State of Cybersecurity 2017. Part 2: Current Trends in Threat Landscape. Technical report, Information Systems Audit and Control Association, ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA (2017). http://www.isaca.org/Knowledge-Center/Research/Documents/state-of-cybersecurity-2017-part-2_res_eng_0517.pdf
13. Kasprzyk, D., Montaño, D.E.: Application of an integrated behavioral model to understand HIV prevention behavior of high-risk men in rural Zimbabwe. In: Ajzen, I., Albarracin, D. (eds.) Prediction and Change of Health Behavior: Applying the Reasoned Action Approach, pp. 145–168. Psychology Press, London (2007)
14. Kirkpatrick, D.L.: Evaluating Training Programs: The Four Levels. Berrett-Koehler, Oakland (1994)
15. Kütz, M.: Kennzahlen in der IT: Werkzeuge für Controlling und Management. dpunkt-Verlag (2007). Google-Books-ID: bkbXGAAACAAJ
16. Lin, H.F.: Measuring online learning systems success: applying the updated DeLone and McLean model. CyberPsychol. Behav. **10**(6), 817–820 (2007). https://doi.org/10.1089/cpb.2007.9948. https://www.liebertpub.com/doi/abs/10.1089/cpb.2007.9948

17. Manisi, P., Jantjies, M., Kimani, L.: A conceptual integrated model for measuring the success of elearning in developing countries: literature review. In: 2018 IST-Africa Week Conference (IST-Africa), pp. 1–9, May 2018
18. Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security. Wiley, New York (2002)
19. Montaño, D.E., Kasprzyk, D.: Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In: Glanz, K., Rimer, B.K., Viswanath, K. (eds.) Health Behavior, pp. 95–124. APA PsycNet, Washington, DC (2015)
20. Montaño, D.E., Kasprzyk, D.: Theory of reasoned action, theory of planned behavior, and the integrated behavior model. In: Glanz, K., Rimer, B.K., Viswanath, K. (eds.) Health Behavior and Health Education, pp. 67–96. APA PsycNet, Washington, DC (2008)
21. Noesgaard, S.S., Ørngreen, R.: The effectiveness of e-learning: an explorative and integrative review of the definitions, methodologies and factors that promote e-learning effectiveness. Electron. J. e-Learn. **13**(4), 278–290 (2015). https://eric.ed.gov/?id=EJ1062121
22. Schütz, A.E.: Information security awareness: it's time to change minds! In: Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development - ICDD 2018. Sibiu, Romania (2018)
23. Sun, P.C., Tsai, R.J., Finger, G., Chen, Y.Y., Yeh, D.: What drives a successful e-learning? An empirical investigation of the critical factors influencing learner satisfaction. Comput. Educ. **50**(4), 1183–1202 (2008). https://doi.org/10.1016/j.compedu.2006.11.007. https://linkinghub.elsevier.com/retrieve/pii/S0360131506001874
24. Tate, M., Sedera, D., McLean, E., Burton-Jones, A.: Information systems success research: the "20-year update?" Panel report from PACIS, 2011. Commun. Assoc. Inf. Syst. **34**(1) (2014). https://doi.org/10.17705/1CAIS.03466. https://aisel.aisnet.org/cais/vol34/iss1/63
25. Verplanken, B., Aarts, H.: Habit, attitude, and planned behaviour: is habit an empty construct or an interesting case of goal-directed automaticity? Eur. Rev. Soc. Psychol. **10**(1), 101–134 (1999). https://doi.org/10.1080/14792779943000035
26. Wang, Y.S., Wang, H.Y., Shee, D.Y.: Measuring e-learning systems success in an organizational context: Scale development and validation. Comput. Hum. Behav. **23**(4), 1792–1808 (2007). https://doi.org/10.1016/j.chb.2005.10.006. http://www.sciencedirect.com/science/article/pii/S0747563205000890
27. Weber, K., Schütz, A.E.: ISIS12-Hack: Mitarbeitersensibilisierenstatt informieren. In: Drews, P., Funk, B., Niemeyer, P., Xie, L. (eds.) Multikonferenz Wirtschsinformatik 2018, vol. IV, pp. 1737–1748, Lüneburg, Germany (2018)
28. Wolf, M.: Von security awareness zum secure behaviour. Hakin9 Extra **5**, 18–19 (2012)