Blind Spot: Do You Know the Effectiveness of Your Information Security Awareness-Raising Program?

Margit SCHOLL
Department Business, Computing, Law, Technical University of Applied Sciences Wildau
Wildau, 15745, Germany

K. Benjamin LEINER
Department Business, Computing, Law, Technical University of Applied Sciences Wildau
Wildau, 15745, Germany

Frauke FUHRMANN
Department Business, Computing, Law, Technical University of Applied Sciences Wildau
Wildau, 15745, Germany

ABSTRACT

Information and IT security awareness-raising measures and the evaluation of these measures are an indispensable part of today's information and knowledge society. While the number of firms that apply such measures is increasing, surveys of corporations show that it is unusual for these measures to be accompanied by specific in-depth evaluations of their effectiveness. Since these awareness-raising measures demand resources such as time, money, and the willingness of employees, every organization should have an interest in assessing their effectiveness. To support organizations in discovering the evaluation methods and metrics that meet their individual needs, an overview of current measures for assessing effectiveness is presented in this paper. Their advantages, disadvantages, and appropriate application are discussed. At the end of the paper suggestions are given as to what direction might be taken going forward.

Keywords: information security, awareness-raising measures, evaluation, effectiveness, metrics, methods

1. INTRODUCTION

Companies and organizations are increasingly becoming victims of cyber-attacks. For example, in November 2016 hundreds of thousands of Deutsche Telekom customers suffered an outage of their internet routers [5] and the login credentials of almost seventy million Dropbox customers were stolen in 2012, which became public in August 2016 [13]. To cope with the growing challenge of how to safeguard sensitive information and the IT infrastructure and to implement appropriate protective measures, 27,536 organizations in 150 countries have been certified to the standard 27001 "Information Security Management Systems" (ISMS) of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) [9]. According to ISO/IEC 27001, organizations are required to systematically implement an ISMS; as part of this, they are obliged to sensitize their employees to information security and to evaluate the effectiveness of their awareness-raising programs. In many cases the greatest risk to an organization's information security is not a weakness in the technology control environment but a mishandling of its information and data protection. "Employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success" [14].

In Germany, enterprises and public administrations have been able to apply for ISO 27001 IT protection certificates at the Federal Office for Information Security (BSI) since 2006 [3]. This is particularly interesting for internationally active German institutions. The concrete IT basic protection approach—together with the IT basic protection catalogues and the recommendations for standard security measures—is a practical de facto standard for IT security. According to the IT Baseline Protection of the BSI, the procedure corresponds to ISO/IEC 27002 "best practice" [8]. However, a survey of 424 German organizations shows that only 63 % perform measures to raise information security awareness [1] and 40.5 % of these organizations do not measure the effectiveness of their trainings. In an international survey with 369 respondents (70 % from US-based organizations and 30 % from outside the United States) 26.6 % indicated that they do not use any metrics to measure their awareness program [15]. Since the number of participants in these surveys is far smaller than the number of certified organizations (for example, 994 certificates in Germany and 1,247 in the United States [9]) it may be assumed that the share of organizations that do not perform awareness-raising measures and corresponding evaluations is far greater.

In order to secure sensitive information—a key resource for a long-term and successful presence in today's information and knowledge society—behavioral awareness for all employees and self-responsibility for information security are essential. However, to determine the appropriate awareness-raising program and, more importantly, to assess the effectiveness of the program applied, it is necessary to specify metrics and corresponding methods that provide information on how well sensitive information is secured.

However, the first step is to define the meaning of information security awareness. It may be understood as "the extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly" [11]. This definition combines three aspects that are accepted as essential elements of information security awareness: knowledge about information security, the willingness to protect sensitive information, and the possibility to do so [12]. A suitable methodological approach for the sensitization of information security that covers these three aspects is our "awareness training 3.0" [16], which combines knowledge transfer, marketing-oriented elements to arouse emotions, and employee involvement as well as systematic social participation in a communicative team process. The aim of this awareness training is to increase staff competence, willingness, and the self-responsibility to behave in such a way that sensitive information is secured [16]. To implement this awareness training 3.0 for employees or students, analogue and digital serious games are being developed and evaluated in the current research project "SecAware4job" at the Technical University of Applied Sciences Wildau [17].

If an organization is to be given a high degree of security awareness in its daily work, then awareness should be implemented as a continuous program to ensure that education and knowledge in information security are not simply viewed as a single annual activity [14]. Existing awareness-raising programs in the institutions must be evaluated with regard to their effectiveness in achieving lasting information security awareness and producing the corresponding behavior in employees. The aforementioned definition of information security awareness reveals that information security awareness is not simply an employee attribute that can be measured directly. Accordingly the challenge in measuring the effectiveness of awareness-raising programs is to cover the three aspects of knowledge, willingness, and possibility. But before appropriate measures for assessing the effectiveness of information security awareness-raising programs can be chosen, organizations should consider which metrics they would like to use to monitor the effectiveness of the programs applied.

2. METRICS

Metrics are parameters that enable the quantitative assessment of processes within a corporation—e.g., "percentage of budget spent on awareness training" or "number of security incidents." They can stand alone or be interdependent with other parameters. The importance of metrics can be seen in the "Security Awareness Maturity Model" developed by SANS, which is used to identify the current stage of a security awareness program [15]. While the model's developers explicitly state that metrics are important through all stages of the model, their high value is made clear by the name given to the highest level of a security awareness program: "Metrics Framework" (see Illustration 1).

According to the international survey, the most common metrics are "phishing assessments" (43.9 %), "security violations" (33.8 %), and "infected devices" (32.8 %), followed by "no metrics" (26.6 %)—multiple answers were allowed [15]. In a survey of 424 German organizations, about 25 % of the organizations stated that they use the participation quota of information security awareness training as a measure of the training's success (while 40.5 % said that "there was no measurement conducted") [1]. While this information is easy to obtain, it is not recommended that it be used for awareness measurement. The fact that an employee attended a training that may have been mandatory does not mean that he/she also paid attention to it or is willing to behave in such a way that sensitive information is secured. In contrast, a quota for successful completions of an awareness training that is finished with a test can be a useful metric.

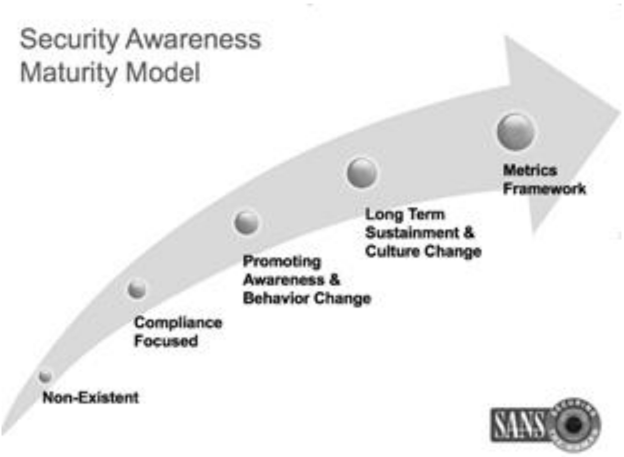
Security Awareness Maturity Model
Metrics Framework
Long Term Sustainment & Culture Change
Promoting Awareness & Behavior Change
Compliance Focused
Non-Existent
SANS

Illustration 1: The Security Awareness Maturity Model by SANS [15]

To successfully evaluate a corporation's awareness program, it is necessary to find out the current situation of the organization. As an example, the German Federal Ministry of the Interior recommends replying to the following questions as an indicator of the goals of the program and its evaluation [4]:

- Where is sensible information stored? / Are there areas or departments of special importance for information security?
- What are the biggest problems for the information security of the corporation?
- What kind of problems have arisen in the recent past? / Were the problems caused by employee deviance? If yes, by whom?
- What kind of malpractice is the most frequent?
- How significant are the differences in competency inside the corporation when it comes to information security?
- Will there be technical or organizational changes in the near future?

The answers to these questions can serve as a basis for the evaluation of the employees' information security awareness, including the three aspects of knowledge, willingness, and possibility. They can also help to phrase questions like "How do you dispose of documents with sensitive information?" or "What will you do if you lose your password?" Organizing the staff in groups with different responsibilities or functions can help to formulate suitable questions, especially in larger organizations.

3. METHODS TO MEASURE EFFECTIVENESS

The methods that can be used to measure the effectiveness of information security awareness programs are numerous and differ widely in their suitability and applicability for evaluating knowledge, willingness, and/or possibility. In the following, the most common methods will be presented and their advantages and disadvantages will be discussed.

Monitoring Security Procedures
A very easily applicable method is to monitor the appearance of security incidents—e.g., helpdesk reports or the results of virus scans. The type and amount of information that can be gathered by this method depends to a large degree on the internal procedures of an organization. While it can provide useful hints on a lack of awareness, it is often abandoned due to other factors that can be the cause of the increase in observed data [6]. For example, the notification of more virus infections can be due to a new, more sophisticated virus, while the level of awareness remained unchanged.

Metrics gathered with these methods do not provide information about a specific employee's awareness, but they can still be helpful. For example, the number of security incidents due to human behavior has proven to be very effective at measuring the overall success of security information awareness activities [6].

Surveys
Conducting surveys is a very common method for evaluating the awareness of an organization's staff. They can be done with either standardized questionnaires or qualitative interviews. Standardized surveys have clear questions with a predefined selection of answers to choose from. This facilitates analysis and allows comparisons to be made of the collected data. This kind of survey offers a suitable way of measuring knowledge. In contrast, interviews offer the possibility of receiving a range of different answers, delve deeper into interesting issues, and can be adapted to suit the questions to the participant. In this way, an insight into different perspectives can be gained and the two aspects of willingness and possibility can be better assessed. For example, an employee may describe how to handle a given situation. The advantages that questionnaires have in comparison to interviews are re-usability, a simple procedure, and the possibility of anonymity. On the other hand, interviews offer more flexibility and additional information can be gleaned through the interviewees' behavior. A practicable approach might be the use of surveys in general and supplemental interviews for employees with especially significant tasks.

Regardless of the kind of survey that is used, it is always important to carefully phrase the questions in a neutral and easily understandable way that does not lead to misinterpretations [10]: as a well-known maxim already states, what you ask is what you get.

Security Benchmarks
Security Benchmarks are the most exhaustive and extensive method of evaluation. For these benchmarks, attacks on the organization are simulated and the staff's behavior is observed. These observations can be done secretly, or alternatively the staff is informed in advance. Naturally, the most realistic results are produced with hidden observations, but they probably lead to a more paranoid atmosphere when conducted multiple times.

A very common and easily conducted benchmark is the phishing assessment, which was used by 49 % of the 369 international organizations surveyed [15]. Phishing is an attempt to get sensitive information like login data for a bank account using manipulative e-mails. To evaluate employees' awareness of this method, fictitious phishing mails are sent to all employees, and the rate of successful frauds is measured. Repeating this process, usually coupled with increasing professionalism in the phishing mails' design, should reveal changes in awareness. Since the click rate on the links provided in these e-mails depends largely upon the professionalism with which they are designed, and because phishing is only one of many risks organizations are confronted with in relation to the protection of sensitive information, fictitious phishing mails do not provide a meaningful indicator of the information security awareness levels of employees.

Thus, other security benchmarks also include the introduction of infected data storages, illegal intrusion into corporate facilities by unauthorized personnel, the search for valuable information that has been thrown away (dumpster diving) or different forms of social engineering [7]. Social engineering is a more and more frequent form of attack that focuses on the human side of information and IT security. A social engineer often uses a fake identity or simulates a sense of urgency to address natural human characteristics such as gullibility, helpfulness, or curiosity in order to get hold of sensitive information [6].

The obvious advantage of getting direct results from employee behavior in the workplace, however, is counterbalanced by certain difficulties. Besides the relatively high degree of effort involved in preparing the tests and monitoring them, legal questions may also need to be clarified—e.g., when personal data is involved. In respect of privacy laws, the works council or other employee representatives should always be included before any action is conducted. It might also be necessary to inform employees themselves, which would influence the measurement's results. A thorough explanation about the legal aspects is given by Boehm, Hey, and Ortner [2].

To reduce legal work and avoid the risk of disturbing the organization's workflow, security benchmarking can be performed in a more controlled environment, via role playing, for example. While the only major trade-off is the fact that the observed persons are aware of their evaluation, controlled environments offer a number of benefits besides the aforementioned reasons:

- High-risk situations can be simulated without endangering the organization's security;
- No real company data needs to be used; this can be an important factor, since third parties are often involved when security benchmarking is conducted;
- The more structured nature of these environments allows easier analysis of the results.

Because the digital world offers a controlled environment that can easily be adapted to individual requirements, serious games that combine information, learning, and entertainment are a further means of creating possible security benchmarks. Digital benchmarks also have the advantages of reusability and scalability, especially when a modularized approach is taken, and once they are created, they are always available. Since information security is a mainly digital sector, and younger generations are for the most part used to playing video games, the drawback of not being a "real-life-environment" is minimal.

In conclusion, security benchmarks offer excellent insight into the behavior of employees and hence the aspects of willingness and possibility. While real penetration tests and benchmarks inside an organization probably provide the best information about the level of awareness, the costs are high and in many cases off-budget. A cheaper way is offered by digital benchmarks, which can be easily adjusted to the budget and are likely to have a better price-performance ratio.

4. DISCUSSION AND CONCLUSION

As a first step in the development of a formal security awareness program, best practices in organizational security awareness indicate the assembling of a security awareness team with different responsibilities, representing a cross-section of the organization [14]. The goal of the second step is to build a reference catalogue of various types and depths of trainings in order to deliver the right training to the right people at the right time [14]. For this purpose, the team needs to determine security awareness roles for the organization relative to the depth of security awareness training. PCI [14] proposes the following classification:

- *low-level depth trainings for all personnel* to help “recognize threats, see security as beneficial enough to make it a habit at work and at home, and feel comfortable reporting potential security issues”
- *medium- to high-level depth trainings for management and specialized roles* to help “focus on the individual’s obligation to follow secure procedures for handling sensitive information and recognize the associated risks if privileged access is misused”

Moreover, “the management needs to understand the organization’s security policy and security requirements enough to discuss and positively reinforce the message to staff, encourage staff awareness, and recognize and address security related issues should they occur.”

In the third step, according to PCI [14], metrics can be an effective tool to measure the success of a security awareness program. They can also provide valuable information to keep the program up to date and effective. However, the individual measures used to measure the success of such a program vary for each organization and/or the type of training.

Current surveys show that many organizations still struggle in their efforts to deploy an efficient measure of the success of information security awareness programs. The main reason here seems to be the lack of suitable metrics for the rating of each of the three aspects of information security awareness.

Even though the metrics that are currently in use offer insight into the overall improvement of a corporation’s security awareness, they cannot help in the search for reasons why programs do or do not improve the security awareness of employees. Finding appropriate metrics that reflect the value of information security awareness programs and their different aspects will be an important task for the future.

Other factors that can impede the proper realization of information security awareness training courses and their evaluation can be an organization’s budget, the support for awareness, and communication inside the corporation. According to the international survey, 30.4 % of the 369 people surveyed reported that they have a budget of less than $5,000 for security awareness programs while another 25.8 % did not know their budget [15]. While $5,000 might be sufficient for small organizations, this sum was also stated in larger companies with several thousand employees. This shows that many organizations still do not recognize the importance of information security awareness or the efforts that must be conducted to achieve it. In the same report, the more than 35 % who stated that they have less than optimal executive support [15] strengthens this assumption.

But even when awareness programs are to be implemented, internal communication seems to be a major problem and was stated as the biggest impediment in the international survey [15]. Therefore, it is very important to involve everyone in the procedures of awareness programs by at least informing them about the importance of taking measures and explaining their use. Instilling a sense of responsibility for an organization’s sensitive information in its employees is also a very important part of a successful information security awareness program. When evaluating the program, it should be ensured that daily work life is not interrupted too frequently or more than necessary. Employees should be motivated to take part instead of being annoyed by constant measuring.

There are plenty of options when it comes to measurement methods. The overview has shown that different methods are appropriate for different aspects of information security awareness and different questions. It also became obvious that there is no single method that can provide all the answers. A practical solution would be a combination of methods, where the monitoring of security procedures used to identify issues and security benchmarks is coupled with surveys that provide information with regard to the awareness aspects. To what extent the different methods are implemented largely depends on the size and structure of the organization being evaluated and the available budget.

One method that should be highlighted is the digital benchmark. Even though digital benchmarks for information security awareness are still in their infancy and simulations have limited possibilities, the prospects for future development are huge. As mentioned in the previous section, the benefits of digital benchmarking are already numerous, and improvements in technology like virtual and augmented reality will further mitigate the differences to “real-life” evaluations. Surveys can easily be implemented in the form of quizzes, and with the right ideas the person involved will not even notice that they are being evaluated (and therefore not falsify the results)—for example, if they are playing a game whose goals are ostensibly other than to assess information security awareness.

5. OUTLOOK

To overcome the lack of metrics that provide meaningful information about the effectiveness of awareness-raising measures, we are planning a research project with organizations that integrates innovative measures for sensitization and for quantifying the awareness level and thus the effectiveness of the applied sensitization measures. As a basis for the training and subsequent evaluation measurement, competence profiles should be formulated to determine the learning topics that are relevant for different employee groups.

According to the competences formulated, the employees firstly work in a team to complete a “Security Arena,” which consists of learning stations with analogue serious games on a variety of information security issues (for example, Security on the Go, Social Engineering, Internet Services) [16, 17]. Afterwards, the employees figure out vulnerabilities in the organization’s information security system in a digital serious game or in a role play. Since every organization has different weaknesses, our method needs to be exactly tailored to the organization’s needs.

Furthermore, no matter how well a serious game is designed and what possible scenarios are considered, they cannot anticipate all the possible threats to different organizations. Besides this learning and detecting game, we are considering developing another more entertaining game whose primary focus does not lie in information security but rather where playing it consistently recalls information security issues in order to internalize them. Evaluation measures that can be easily integrated during role plays or digital (serious) games include observations and (eye-) tracking procedures. After such innovative trainings for employees using analogue/digital methods and possible technical and organizational improvements in the respective institution, on-site inspections or penetration tests can round off the awareness measurements.

In this manner, sensitization measures, which should be an ongoing process because of the rapid developments of new challenges and attacks, can be effectively interlinked with measures evaluating the employees' awareness level. We consider that this will be an innovative approach to measuring the effectiveness of awareness-raising measures in the future.

6. REFERENCES

[1] Alliance for Cyber Security (Allianz für Cyber-Sicherheit), **Awareness-Umfrage 2015**, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/awareness-umfrage-2015.pdf?__blob=publicationFile&v=5, 2015, accessed December 1, 2016.

[2] F. Boehm, T. Hey, and R. Ortner, "How to Measure IT Security Awareness of Employees: A Comparison to E-Mail Surveillance at the Workplace", **European Journal of Law and Technology**, Vol. 7, No. 1, 2016, pp. 1-15.

[3] BSI (Federal Office for Information Security), **Self-Declaration and IT-Grundschutz Certificate**, https://www.bsi.bund.de/EN/Topics/ITGrundschutz/IT-GrundschutzCertification/OrganisationofCertification/organisationofcertification_node.html, accessed December 1, 2016.

[4] Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV**), Sensibilisierung für die Informationssicherheit in der öffentlichen Verwaltung – Der Leitfaden**, Brühl, 2016.

[5] G. Chazan, "Deutsche Telekom Outage Blamed on Possible Cyber Attack", **Financial Times,** November 28, 2016, https://www.ft.com/content/c4779f86-7a2b-3480-96e4-878cf2bd73cb, accessed December 7, 2016.

[6] ENISA (European Network and Information Security Agency), **The New Users' Guide: How to Raise Information Security Awareness**, Heraklion, Greece, 2010.

[7] HvS-Consulting AG., **Messen Sie die aktuelle Security Awareness in Ihrem Unternehmen** [online], 2016, https://www.is-fox.de/security-awareness-tools/awareness-messung/, accessed December 1, 2016.

[8] ISO/IEC 27002:2013, **Information technology – Code of practice for information security controls**, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533, accessed December 11, 2016.

[9] ISO Survey, **The ISO Survey of Management System Standard Certifications (2006–2015): ISO/IEC 27001 – Information Technology – Information Security Management Systems – Requirements, ISO/IEC 27001:2013/Cor 2:2015,** 2015, http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF, accessed September 28, 2016.

[10] M. Kaya, "Verfahren der Datenerhebung (Procedure of Data Collection)", in S. Albers, D. Klapper, U. Konradt, A. Walter, and J. Wolf, **Methodik der empirischen Forschung (Methodology of Empirical Research)**, 2nd ed. Wiesbaden: Gabler, 2007, pp. 49-64.

[11] B. Khan, K.S. Alghathbar, S.I. Nabi, and M.K. Khan, "Effectiveness of Information Security Awareness Methods Based on Psychological Theories", **African Journal of Business Management**, Vol. 5, No. 26, 2011, pp. 10862-10868.

[12] H.A. Kruger, and W.D. Kearney, "A Prototype for Assessing Information Security Awareness", **Computers & Security**, Vol. 25, No. 4, 2006, pp. 289-296.

[13] D. Meyer, "How to Check If You Were Caught Up in the Dropbox Breach", **Fortune**, August 31, 2016, http://fortune.com/2016/08/31/dropbox-breach-passwords/, accessed December 7, 2016.

[14] PCI Security Standards Council / Security Awareness Program Special Interest Group, **PCI Data Security Standard (PCI DSS)**, Version 1.0, October 2014, https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf, accessed December 11, 2016.

[15] SANS Securing The Human, **Security Awareness Report: Awareness Is Hard: A Tale of Two Challenges**, 2016, https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2016.pdf, accessed December 4, 2016.

[16] M. Scholl, F. Fuhrmann, and D. Pokoyski, "Information security awareness training 3.0 for young professionals", **Proceedings of Conference on ENTERprise Information Systems/International Conference on Project MANagement/Conference on Health and Social Care Information Systems and Technologies**, CENTERIS/ProjMAN / HCist 2016, 2016, pp. 433-436.

[17] SecAware4job, **Information Security Awareness for the Career Entry**, http://secaware4job.th-wildau.de (English), 2017, accessed September 4, 2017.