JAIST Repository
https://dspace.jaist.ac.jp/

Title	Assessment and Improvement of Security Awareness Training Methodologies [Project Paper]
Author(s)	Yuan, Liangwen
Citation	
Issue Date	2020-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/16382
Rights	
Description	Supervisor: Beuran Razvan Florin, 先端科学技術研究科, 修士（情報科学）

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

Assessment and Improvement of Security Awareness Training Methodologies

IBM 2016 study of the cost of data breach for the USA found that the total cost of data breaches had increased 7% by an average. Some companies affected by a serious security incident lose not only the trust of their customers but also their entire business after a major data breach. The average data breach incidents are 29,611 records, a cost of $221 each. It means during an accident, there is an estimated loss of $6,544,000. What's more, not only data breaches, but also other security problems, like Viruses, Worms, Trojan horses and so on, are taking place which cause serious problem. Security awareness training is considered to be one of the main factors in reducing the risks of data breach and other security problems.

Security awareness training approach aims to teach people multiple layers of protection on the computer, network, program or data they intended to protect. There are a lot security awareness training programs and systems nowadays. We want to figure out whether they can be improved or not.

In this report, we introduce the security awareness training programs within four categories. The first category is e-learning training programs. When the interactive whiteboard appeared on the training site, it was big news because it replaced the old chalk and rags as a key tool for education. Today, online learning tools may make traditional classroom training a thing of the past. The second category is video training programs. Traditional training makes it difficult to measure the effectiveness of training. With video, the training can be done on the road or at home. The more readily training are available, the more likely they are to be studied. It's safe to say that trainees prefer fast, engaging videos to other time-consuming training tasks. The third category is reading material training programs. When trainees have a chance to select their reading content, they have more ownership in education. Trainees must read at their own reading level and cannot rely on other's support to understand the materials. The fourth category is focus on technology training and practice. Technology training is critical to providing individuals with the computer tools they need to protect themselves from attacks. Common training content in technology training systems points to web security but also includes firewalls, DNS filtering, malware prevention, antivirus software and email security solutions.

For those security awareness training programs/systems categories introduced, we make a questionnaire to evaluate them. The questionnaire includes two parts, one is security knowledge quiz questions and the other is the actual assessment criteria. The main purpose of assessment criteria is to see whether it meets its objectives or not. Therefore, we gather feedback and data on how participants feel about the training will enable us to identify ways to improve. This applies to any other area. Trainers can contribute to the company by developing the improvements we offer to conduct an effective training. In security knowledge quiz questions, we prepare 8 questions and participants don't know the difficulty and this part is not counted into the evaluation of

training programs/systems. Participants can provide feedback on the concept of the question, the level of knowledge required to answer, the range of possible answers. It is the process of informal testing questionnaire for potential respondents. For example, if we find out a strange value for a participant in the assessment criteria, we can use his or her score of the security knowledge quiz questions to help us figure the reason whether the content is too difficult for him or her.

In assessment criteria, we create 9 close-end questions and 3 open-end questions depending on opinions from three experts in cyber security field. The 9 close-end questions are presented by Likert Scale. Some people advocate a 7-point or 9-point scale to add granularity. Sometimes using a 10-point (even number) scale to generate a forced choice measurement in which case there are no unrelated choices. However the most common scale is 5-point which is “Strongly agree”, “Agree”, “Neutral”, “Disagree” and “Strongly Disagree”. In our report, we use the common 5-point scale to measure the assessment criteria.

About calculation for the assessment criteria (Likert scale), we found a new method to measure discreteness that is expressed as agreement and disagreement. This measurement based on the recognized Shannon entropy utilizes the probability distribution and the distance between categories to generate a value spanning the unit interval. With this measurement, ordinal scale’s data can be assigned a dispersion value which is logically and theoretically reasonable.

We select 6 representative participants among the original 25 participants to conduct our assessment criteria of three e-learning training programs, four video training programs and three advanced training systems. From the outcome, we want to improve the gamification and practicality(be practical or easy to apply) to e-learning training program; the learning environment, gamification, addressing real security threats and engagement to video training program; engagement and practicality(be practical or easy to apply) to advanced training system. Therefore, in the overall proposed improvements, we propose the detailed improvements which seems possible.

With 9 close-end questions and 3 open-end questions in this report, we can easily weed out old and ineffective training methods and find better ones. The more appropriate a safety awareness solution is to the unique needs of social organization, the more effective it will be in reducing violations, building a strong security culture, and providing positive experiences for trainees.