Effective Cybersecurity Awareness Training for Election Officials

Carsten Schürmann(✉), Lisa Hartmann Jensen, and Rósa María Sigbjörnsdóttir

IT University of Copenhagen, Copenhagen, Denmark
carsten@itu.dk, lisaha85@gmail.com, rosa.sigbj@gmail.com

Abstract. Cybersecurity awareness training has a bad reputation for being ineffective and boring [21]. In this paper, we show the contrary, namely that it is possible to deliver effective cybersecurity awareness training using e-learning. We provide a general methodology on how to create cybersecurity awareness training and evaluate it based on Kirkpatrick's model of evaluation [22]. We have conducted a pilot study of the methodology in context of the European Parliament election 2019.

Keywords: Cybersecurity awareness training · E-learning · Human factors · Attack trees · Election officials

1 Introduction

Organizations rely on their staff for protection of their assets. No matter how many security polices are put in place, security always comes down to how the individual employee behaves. In March 2016, for example, the personal Google mail account of John Podesta, a former White House chief of staff and chair of Hillary Clinton's 2016 U.S. presidential campaign, was compromised in a data breach accomplished via a spear-phishing attack allegedly carried out by foreign Nation State. Allegedly, Podesta's assistant, following the advice of a security technician, complied and followed the instructions contained within the phishing mail [20].

Therefore, to protect an organization from security breaches, it is vital to protect the technical and organizational infrastructure including sensitive data *and* prepare users, employees, consultants, and guests to recognize and defend against cyberattacks. In this paper, we focus on the human factor. Social engineering attacks, where an adversary exploits human traits, such as modesty, altruism, empathy, and diligence of a victim to gain access to restricted resources, steal secrets, or causes other kinds of havoc. It seems natural that the only way to protect an organization against this kind of attack is by sharpening a user's common sense and the ability to recognize, react, and mitigate an imminent attack, and to install a designed behavior in connection with security [15]. Therefore, education is an important part of creating a security culture in organizations [6]. However, cybersecurity awareness training has the reputation of being ineffective [2].

R. Krimmer et al. (Eds.): E-Vote-ID 2020, LNCS 12455, pp. 196–212, 2020.
https://doi.org/10.1007/978-3-030-60347-2_13

Not wanting to accept this conclusion, we set out in this work to demonstrate that cybersecurity awareness training for short-term retention of knowledge, for example for election officials, *can be made* effective. The hypothesis of our work is that one of the reasons for the perceived ineffectiveness is that cybersecurity training is often unspecific, explaining concepts abstractly, such as confidentiality, integrity, and availability that are good to know, but often not directly relevant and difficult to translate into practice. Instead such training must be methodologically relevant, consistent, role-based and continuously adopted to an ever-evolving threat landscape [21].

As a corollary, effective cybersecurity awareness training can only take place, after a rigorous security analysis of the attack surface, the entire security context, and the security background of the target audience, i.e. users and course participants, has been conducted. These findings must inform the learning objectives of the cybersecurity awareness training, not more and not less. Concretely, in this paper, we develop a methodology consisting of a few easy to follow steps to prepare tailored security training for a particular target group to be deployed in a well-defined security context.

We evaluate this methodology empirically, in the context of the European Parliament election 2019, held in Denmark. In close cooperation with Copenhagen municipality, we conducted a security analysis of the voter identification system, deployed in each of the 53 polling stations in Copenhagen, and prepared an e-learning course for 53 election officials, the digital election secretaries, responsible for all technical equipment used in the polling station. The course was organized in modules, each tailored to the security needs of the election officials. All participants had to take an entry exam before the training and a final exam after the training. We could demonstratively measure a significant increase in cybersecurity preparedness for this limited target group election officials.

The cybersecurity awareness training was administered as part of the general training of election officials, who are recruited within the municipality, some having served in this role already several times before. Election officials have to undergo training before each election, and the knowledge gained in the training is usually necessary only for the day of the election. In general, election officials were grateful to have the opportunity to learn about the attack surface. Long-term retention of knowledge was not measured. To our knowledge this is the first systematic study of e-learning with the short-term retention of cybersecurity knowledge.

The literature [21] defines three levels of security awareness: perception, comprehension, and projection. Perception is to be aware of that there are potential security risks. Comprehension is to understand and assess the dangers of security risks. Projection is to be able to anticipate future situations and how to act on potential security attacks. Based on our pilot training and the evaluative statistical analyses we conclude that cybersecurity awareness training for short-term retention delivered on all three levels of security awareness.

This paper is structured as follows. In Sect. 2, we discuss human factors in cyber security. In Sect. 3, we then design a methodology for designing cyberse-

curity awareness training to be delivered through e-learning. Next, we present a pilot study for the European Parliament election 2019 and an evaluation in Sect. 4 before we conclude and assess results in Sect. 5.

2 The Human Factor

The attack surface of any system includes technical as well as human components. No system is stronger than its weakest component [5], and arguably, human performance is recognized as a critical part of securing critical infrastructure [5]. Depending on the adversary's objective, social engineering will always be considered as one way to achieve the goal: As opposed to technical cyberattacks that exploit vulnerabilities and always leave traces in log files or other media, social engineering is considered a viable alternative which allows adversaries to break a perimeter and operate somewhat undetected. In general, it is also more difficult to attribute a social engineering attack to an adversary. Therefore, measures to prevent or decrease the negative impacts of cybersecurity breaches must include all processes, policies and actors involved [7]. Technology alone cannot create a secure environment, since human factors are an integral part of any system, for example, during configuration, operation, or use. According to 2020 Verizon Data Breach Report social attacks are used in 22% of all cases recorded. These attacks are almost evenly split into phishing and pretexting attacks [4].

There are many factors that influence the security behavior of users i.e. the user's respective rank in an organization, their respective personal values, and their common sense regarding security [15]. Users are often not aware or do not consider the vulnerabilities in an organization, they make mistakes or are tricked into giving away sensitive information [1]. Therefore, common sense regarding security in an organization must be taught [15] and training in cybersecurity awareness is an important part of creating a security culture [1].

However, there seems to be a problem with existing cybersecurity awareness training as it does not change behavior as expected [2]. There are several reasons that this is the case. Firstly, cybersecurity awareness training is often designed as too general without a clear target group in mind, leading to users not finding it relevant. Secondly, incorrect assumptions about the targeted users and their skills and motivation tend to make cybersecurity awareness training too general.

3 Training Design Methodology

Next, we describe a methodology for how to create cybersecurity awareness training that avoids the above mentioned factors by tailoring training to a well defined target group and focusing the training content on what the target group need to know and nothing else. The methodology consists of five steps, which are summarized in Fig. 1.

1. Target group
   - Define the target group, target setting, tasks, and responsibilities
2. Risk assessment
   - Define the adversarial environment
   - Define assets, including physical and logical, and processes
3. Threat modeling and risk analysis
   - Model the entire socio-technical system using CORAS/attack trees
   - Derive and prioritize potential attacks
   - Derive the attack surface and tailor it for the target group.
4. Training materials
   - Base training on knowledge gained from (1.-3.)
   - Create an e-learning platform
   - Consider using videos, audio, games as part of the training
5. Evaluate training

Fig. 1. Training design methodology

3.1 Target Group

The first step of creating good cybersecurity awareness training is to identify and characterize the target group, the target setting, and the target group's tasks and responsibilities in this setting. This can be achieved by ethnographic studies, long-time observation of work practices, and study of available procedures and documents. Usually, it is not sufficient to base this analysis only on printed materials, as common work practices often deviate from the described processes. A target group must be homogeneous, meaning all members should be assigned the same tasks and the same responsibilities. Heterogeneous target groups are not considered in this paper.

3.2 Risk Assessment

The next step is to identify assets and processes that are at risk, and define the security policies that should be enforced [3]. A good starting point for the risk assessment is to explore notions such as confidentiality, integrity, and availability, and refine them on demand. It is absolutely crucial that the target group identifies with this assessment. The cybersecurity training must be perceived as relevant by the target group for it to be effective.

A part of the risk assessment is the attack surface of the infrastructure, for which cybersecurity assessment training is to be offered. This presupposes a clear picture of the adversary's capacity and the adversary's objective. The attack surface includes all aspect of the infrastructure to be protected, including technology, networked computing equipment, air-gapped equipment, access control, cryptographic key distributions, physical access etc.

With the risk assessment in place, the next step is then to identify the weak points in the infrastructure that an adversary could exploit and to define the

role of the human to detect attacks and protect assets and processes. These insights and this knowledge form the basis of understanding of the infrastructure and feeds into the design process of the training materials, of which attacks participants should learn to spot, and which procedures they should learn follow to neutralize threats effectively.

3.3 Threat Modeling and Risk Analysis

In our experience, modern threat modeling tools, such as CORAS [16], attack trees [17] or even attack-defense trees [14] are useful tools to explore the threat model of any socio-technical system in a systematic and complete way. The CORAS method is a defensive risk analysis approach where the Unified Modeling Language (UML-diagrams) is used to model the target of the analysis. Unwanted behaviors are drawn as threat scenarios. The CORAS method comes with tool support, in particular, there exists a tool that supports drawing and analyzing diagrams. Alternative ways of conducting security analyses and modeling threats are described in this survey article [11]. In this paper, however, we focus on attack trees as a modeling tool.

An attack tree is a mathematical tree-like structure that organizes threats and attacks against a system. The root of the tree comprises the goal for the adversary, and the leaf nodes denote the different actions an adversary can execute to achieve this goal. Each node in a tree can be seen as a subgoal. The disjunctive "OR"-node represents alternatives, i.e. if *one* of the subtrees is successful then so is the subgoal. In contrast, the a subgoal rooted in a conjunctive "AND"-node is successful if an only if *all* subtrees are successful. There are also other variants of attack trees, that could in theory be considered, for example those supporting sequential conjunctions. The methodology presented here applies as well. The visual representations of "OR"-nodes, "AND"-nodes and leaf-nodes are depicted in Fig. 2.

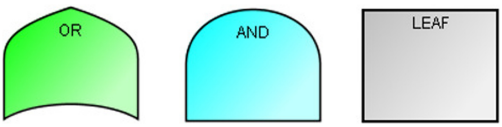

Fig. 2. Explanation of nodes in attack tree

Attack trees are known for their ability to express socio-technical systems and model human factors. We will be using them as well in our pilot study for securing polling stations during the European Parliament election 2019 that we describe in the Sect. 4.

3.4 Training Materials

Next, we identify the critical elements of the analysis and translate the attack tree into suitable training materials. We proceed in four steps, tagging, normalizing, prioritizing, and finalizing.

Tagging: When normalizing an attack tree, all information about the structure of the inner nodes, i.e. OR and AND nodes is lost. In practice, however, it is useful, to tag such inner nodes with keywords that help structure the content of the training materials, and collect them during the normalization procedure. Possible tags include, for example, social engineering attacks, man in the middle attacks, attacks against air-gapping, SQL-injection attacks, cross-site scripting attacks, buffer overflow attacks, and so on. An example of tagging can be seen in Fig. 3.

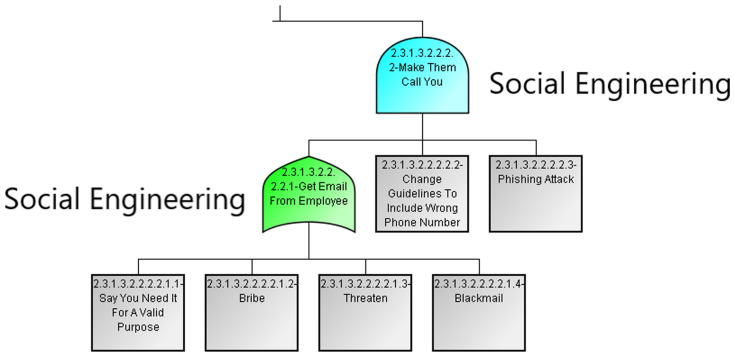

Fig. 3. Example of tagging sub-trees

Normalizing: Hereafter, the attack tree is normalized as to create a list of attack-chains in plain text. Attack-chains only include leaf nodes. Correspondingly the normalization procedure is augmented, to derive an additional tag-chain, of all of the tags that were encountered while constructing the attack chain. Below A and T are normalized attack-chain/tag-chain pair displaying the fragments derived from the attack tree depicted in Fig. 3:

$A = \{\ldots$
Say You Need It For A Valid Purpose,
Change Guidelines To Include Wrong Phone Number,
Phishing Attack
$\ldots\}$

$T = \ldots$, Social Engineering, $\ldots$

The above step should result in a number of attack/tag-chains pairs. Duplicate attack chains should be removed while their tag-chains should be merged.

Prioritizing: Next, we identify precisely the topics that should be covered in the training materials. We therefore correlate the attack-chains with the tasks the target group is in charge of to determine what parts of the attack-chain, if not all, need to be included. It is critical for the training to be effective to educate the target group exactly in the topics they need to know - nothing more and nothing less. We use the tag chains as a guide to structure and organize the material.

Finalizing: In this last step, we create new or update existing training materials to create a consistent product. Recall that the success of effective training is to make sure the target group attains three levels of awareness of security risks, namely perception, comprehension and projection [21]. We propose to use e-learning as platform for the training, since interactive and adaptable material i.e. videos, also called hyper media-based material, can lead to effective cybersecurity training [21] and motivation for learning through such a platform tends to be high. Prior research has shown that video-based training is preferred over other methods and yields better results [1,18]. The length of the video is important to get the participants engaged, and a study shows that videos that are 0–3 minutes have the highest engagement [9]. The training videos developed should train the target group to observe, identify, react, and defend against the individual steps laid out in the attack chains. Training material can be rearranged and reused for other target groups.

3.5 Evaluating E-learning

The final step of our methodology is that of evaluation. It is good practice to document the effects of security awareness training, to analyze the training objectively, and to measure the efficiency and effectiveness of it. Evaluation can help create a common understanding about the human factor defense capabilities, which areas of understanding among the target group are sufficient, and identify weaknesses that need to be strengthened [8].

Choosing an evaluation model to evaluate e-learning is dependent on the scale and the time frame of the e-learning. The state of the art is described in an article by Tripathi et al. [23] where four different evaluation models are described in depth. We found that more models could be used in our case, and many of the models don't differ that much when measuring short-term effects, as we do. If we had to measure long term, we would have to go back and look at the evaluation models again. The two best models for our purpose are CIRO or Kirkpatrick's model of evaluation.

The CIRO model does not take the behavior of the learners into account and is, therefore, thought to be better suited for management focused training rather than for people working on lower levels of organizations [23,24], therefore we chose to use Kirkpatrick's model of evaluation.

Kirkpatrick's model of evaluation was introduced in 1959. The model evaluates outcomes of training programs at four levels: reaction, learning, behavior and results. *Reaction* addresses how the participant felt and reacted to the training experience. *Learning* measures to which extent knowledge has increased

and how intellectual capability has changed from before the training. *Behavior* measures how the participant has changed behavior and applied the learning. *Results* addresses how the improved performance of the participant affect organizations [13].

Kirkpatrick's model is applied after training. The model is popular and still widely used among organizations. The main strength of the model is the focus on behavioral outcomes of the participants [13,23].

Quizzes can be used to measure learning in Kirkpatrick's model. A quiz can be thought of as a survey, i.e. a quantitative method to collect data. The quiz, which must be taken both before and after training, consists of closed-ended questions. Participants can choose from a set of answers, where either one or more are correct. Participants can answer closed-ended questions fast and they can get instant feedback when they have taken the quiz. Another reason for using this type of question is that it is easy to analyze [19]. The quiz must be constructed in such a way that it measures the three levels of security awareness.

A survey can also be used to measure reaction in Kirkpatrick's model. The survey to measure this level consists of questions answered by a likert-scale and open questions. The likert-scale questions should give an indication of how relevant the participants find the e-learning. The open questions can help to discover unforeseen findings, and are essential to understand how the target group perceive the training [19].

4 Pilot Study: Digital Election Secretaries in the Election Context

In connection with the European Parliament election conducted in Denmark on 26th May, 2019, a group of election officials employed by Copenhagen municipality, called digital election secretaries, partook in cybersecurity awareness training. The staff at each polling station includes one *digital election secretary*, who is responsible for all computer equipment that is used in a polling station, that is, a digital voter identification system and a digital results transmission system. In Denmark, ballots are not interpreted and stored digitally, only the result of precinct-level tabulation is. The scope of our pilot was limited to cybersecurity awareness training with respect to the digital voter identification system. It was the first time that election officials had received any role-based cybersecurity training to recognize and act on attacks happening at the polling stations. The objective of our pilot study was to measure the improvement of their cybersecurity awareness.

4.1 Target Group

Copenhagen municipality has 53 digital election secretaries, one for each polling station. The main responsibilities of this group is to secure the equipment at the polling station and the electoral register including all the data in the above mentioned register. The digital election secretaries are recruited within the workers

of the municipality and differ in age and background. Some have served in the role of digital election secretary several times before. Despite the demographic differences, the group is highly homogeneous in the tasks they perform on election day. They will spend election day in similar environments, the different polling stations, and work with the same kind of election technologies, including the electoral register.

4.2 Risk Assessment

We conducted a detailed risk assessment of the processes connected with the digital election secretaries on election day, and identified a set of potential objectives of a hypothetical adversary. We consider confidentiality, integrity, and availability in turn.

Confidentiality: We consider an attacker who aims to get unauthorized access to information. If published by the attacker, it would weaken the trust in the security of the election and violate this security goal. It is the digital election secretaries' responsibility to protect voters' data at the polling stations and will, therefore, be considered in our cybersecurity awareness training.

Integrity: We consider an attacker who could try to violate election integrity by voting multiple times with the goal to change the election result in his or her favor. This is very difficult achieve given the organization of a Danish national election as several checks and balances were put in place for this not to happen. For example, every voter receives a voting card in the mail which they will have to bring to the polling station. All voting cards will be kept until the end of voting day and then counted to validate the number of votes cast. Once a voter is identified in the polling station, the physical poll book or in the electoral register will be updated, the former only if the electoral register fails. However, it is the digital election secretary's responsibility to ensure that no one voted more than once, and will hence be considered in our cybersecurity awareness training.

Availability: The attacker's objective could be to weaken public confidence in the voting process, by trying to make headlines in the press or on social media. To succeed, the attacker would have to break one or more security goals, for example, by rendering the electoral register at a polling station unavailable/unusable. To protect this asset, again, lies within the responsibilities of the digital election secretary and will hence be considered in our cybersecurity awareness training.

4.3 Threat Modeling

Based on the analysis in the previous section, we focus on all security goals, in particular an attacker's intent to weaken public confidence. We exclude insider attacks from our threat model. To succeed, the attacker would have to break one or more security goals, and it does not matter which one(s). With this objective

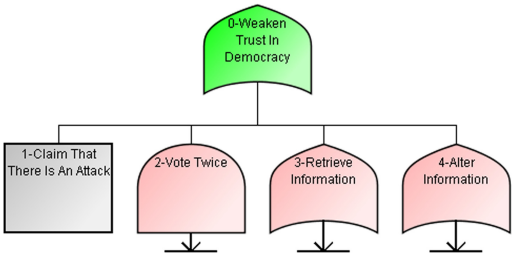

Fig. 4. Root and first level of the attack tree (Color figure online)

in mind, we develop an attack tree of the election system from the vantage point of a digital election secretary.

Together with election experts from Copenhagen municipality, we identified 88 possible attack scenarios leaving us with an attack tree too large to include in this paper. The full attack tree can be found on the project's homepage[1]. Figure 4 depicts the top two levels of the attack tree. The leftmost singleton subtree (shaded in grey) states that a possible attack would be an attacker crying wolf and claiming that the election is under attack. Clearly, the digital election secretaries cannot stop people from lying, but still, such circumstances may arise, and the digital election secretary would need to know how to react. Hence, this must be a part of the cybersecurity awareness training.

The other three subtrees, describe ways on how an attacker could conceivable vote twice, gain access to privileged information, or alter the information stored in the electoral register. In the interest of space, we comment only the second subtree that is depicted in Fig. 5. In our estimation, this attack is highly hypothetical and very difficult to execute. The nodes of the subtree are largely self-explanatory, except perhaps the unit that is called PCA, which refers to the laptop named "A" that contains the binding version of the digital electoral roll. In general, the polling place consists of several (through wired Ethernet) networked laptops. This network is not connected to other networks including the Internet during operation, but has been during configuration.

4.4 Training Materials

In our pilot study, we considered the entire attack tree[1], tagged the inner nodes, normalized to obtain attack/tag-chain pairs, prioritized them, and used this knowledge as input for the design of training materials. The training materials, which were created throughout a two months period, consist of an e-learning website with several modules and videos. The course page is online an can be accessed under https://valgsikkerhed.dk.[2] All 53 digital election secretaries were

[1] See https://www.demtech.dk/training/.

[2] The website is online, and anyone interested can make an account and access the teaching materials. Note, that the website is only in Danish.

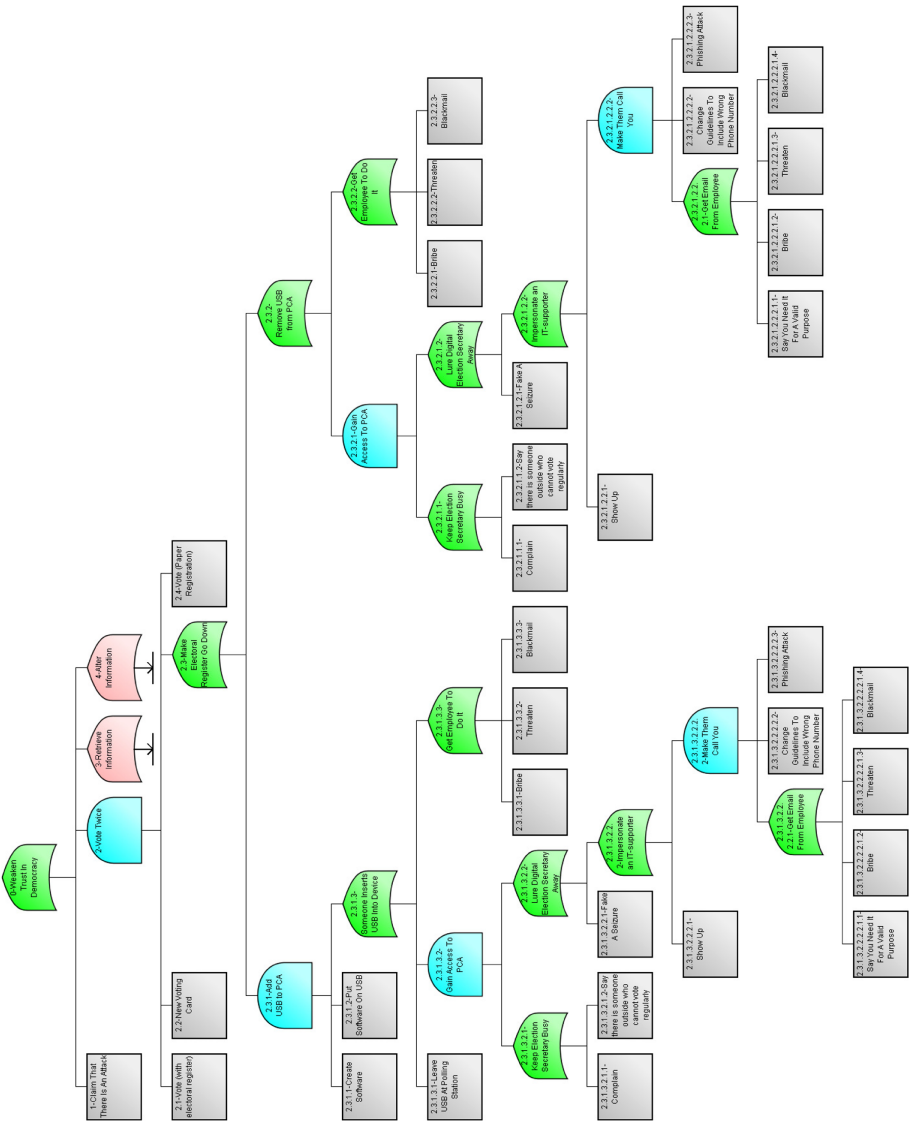

Fig. 5. Subtree 2: vote twice

invited to complete the e-learning course at their own pace and in their own time. Participating in the training was not mandatory.

All potential attacks are based on social engineering techniques aiming to coerce employees to retrieve desired confidential information or execute an attack on behalf of the adversary. Some potential attacks include also elements of man-in-the-middle attacks. Our training material therefore includes modules aimed to explain both, social engineering and man-in-the-middle attacks. The video on man-in-the-middle discusses devices that should not be present at polling stations, and how to react if they are spotted. The social-engineering videos focus on attacks that could be conducted before election day or at polling stations, i.e. exploiting common human traits resulting in that employees give access to confidential information to people with authority, follow instructions in phishing e-mails or gain access to any of the networked PCs in particular PCA, by creating a distraction. The training materials even include guidelines on how to calm worried voters in the case of an imminent cyberattack.

4.5 Evaluating E-learning

Learning Outcome. To evaluate if the digital election secretaries had gained cybersecurity awareness, they were tested both before and after the training with the same questionnaire.

The questionnaire was designed in such a way that each level of awareness was covered by more than one question. It is designed with reaction and learning levels from Kirkpatrick's model in mind. Since we are not measuring long term effects, there is no reason to evaluate the participants changed behavior nor how their changed behavior affect the organizations they work for.

77.4% of the target group signed up to the platform but only 71.7% completed the e-learning training. That means that 92% of those who started the e-learning finished it. The distribution of the grades can be seen in Fig. 6.

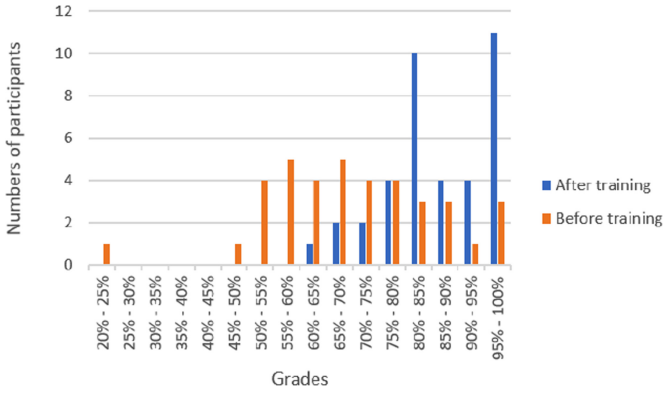

Fig. 6. Distribution of the grades before and after training.

A paired t-test can be used to check if the learning is effective by comparing before and after observations. This is done to show that there is statistical evidence that the difference of the means between the paired samples is significantly different from zero [12].

In order to do a paired t-test on this small data set, one need to make sure that the data is normally distributed. This was tested with a Q-Q Plot, that can be seen in Fig. 7. It shows that the data is, indeed, normally distributed.

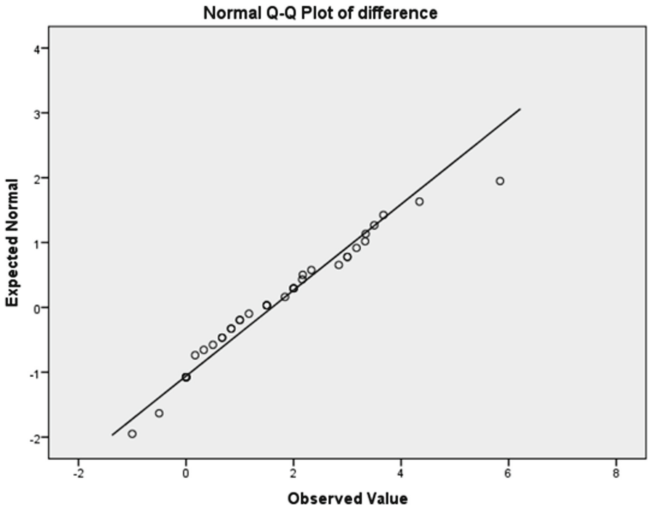

Fig. 7. Q-Q plot of data.

The t-test is run with the following hypotheses:

$$H_0 : \mu_d = 0 \tag{1}$$

$$H_1 : \mu_d \neq 0 \tag{2}$$

In other words, H_0 assumes that the security awareness training has no effect on the mean and the alternative hypothesis, H_1 assumes that there is a difference.

The grades before and after were used to run the paired t-test. Since the participants can also score less than before we do a two-tailed test.

SPSS is a widely used statics application created by IBM [10] and was used to run the paired t-test. The test was run with $\alpha = 0.05$. The result of the test is shown in Fig. 8. As can be seen in the figure the digital election secretaries score, on average 1.6 points higher in the latter quiz. It also shows that the Sig. (2-tailed), also called the p-value, is much smaller than α. This means that we can reject the null-hypothesis.

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	before - after	-1.59789	1.50898	.24479	-2.09388	-1.10191	-6.528	37	.0000001217

Fig. 8. Paired t-test results

To evaluate the awareness layers, as mentioned in [21], they are translated to this specific context. Perception is getting the digital election secretaries recognizing and understanding potential security risks in an election. Comprehension is to teach them to take in information from multiple sources, interpret them and be able to pass on information that can help others actors in the election. Projection is for them to be able to prevent future attacks.

The results in Table 1 shows that all the three levels of successful security awareness training was reached for the election officials that participated in the e-learning training.

Table 1. Table of scores for the three levels of security awareness

Awareness level	Before	After	t(37)	p
Perception	M = 1.45, SD = 0.57	M = 1.64, SD = 0.49	−2.113	0.041
Comprehension	M = 2.24, SD = 0.75	M = 2.237, SD = 0.41	−4.112	0.00209
Projection	M = 3.3, SD = 0.89	M = 4.15, SD = 0.59	−5.929	0.0000007835

An analysis on the time spent on the quizzes, shows that the participants spend on average 4 min less on the latter quiz. However, we can not draw any conclusion by that in itself as we decided to give the participant the freedom to do the training at their own pace. Hence we have not measured the individual questions in the quizzes and, therefore, do not know how which questions they spend less time on in the latter quiz. We leave this to future work.

Participant Evaluation. 52.6% gave feedback on their experience of the e-learning. 85% said that they felt they had either gained new knowledge or refreshed knowledge they already had. 85% also said that they thought the content of the e-learning was good and relevant for their duties as digital election secretaries.

5 Conclusion

This paper provides a methodology for designing and delivering cybersecurity awareness training for short-term retention. The methodology was tested on 53 digital election secretaries who were deployed to 53 polling stations in Copenhagen municipality during the European Parliament election in 2019. We have evaluated the training using Kirkpatrick's model of evaluation found it to be effective. We are certain that our methodology carries over directly to the other 97 Danish municipalities, as their elections are organized in a manner similar to those in Copenhagen. We also believe that it is applicable beyond Denmark, as other European countries use digital voter identification and results transmission systems. The training material must be updated and adjusted to the respective target audiences and the specific technologies in use in a particular location.

Through understanding of the target group, the adversarial environment and the attack surface it was possible to create training materials tailored toward the job of the digital election secretaries. The training was delivered through a custom-made e-learning platform, containing short videos to deliver individual modules derived from potential attacks identified using attack trees. After training, we demonstrated that the target group reached all levels of successful security awareness: perception, comprehension and projection. In addition, a training evaluation showed that (1) the digital election secretaries perceived the training to be both good and relevant for their work on election day and (2) they also felt that they gained or at least refreshed their cyber security knowledge.

In future work, we would like to collect more evidence that this is a sustainable methodology to design and conduct cybersecurity awareness training. Firstly, we would like to compare a group that has been trained with a group that has not been trained to identify the difference, if any. Secondly, it would be interesting to analyze time spent on each task and correlate with retention of the concepts associated with each task. Hence do a more granular evaluation of the cyber security awareness training. Thirdly, we would like to conduct similar awareness training with the same group of digital election security at future elections to identify trends in the evaluation data. Fourthly, we would like to broaden the pilot to the whole of Denmark to examine if we can reproduce our results. Lastly, we believe that it would be interesting to apply the same methodology to elections in other countries and/or broaden cybersecurity awareness training beyond the elections to other sectors as well to study the robustness of the methodology.

Acknowledgments. We would like to thank the employees Copenhagen municipality's election office, the Ministry of Social and Internal Affairs, and KL, the association and interest organization of the 98 Danish municipalities.

References

1. Abawajy, J.: User preference of cyber security awareness delivery methods. Behav. Inf. Tech. **33**(3), 237–248 (2014)
2. Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672 (2019)
3. Basin, D., Schaller, P., Schläpfer, M.: Applied Information Security: A Hands-on Approach. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24474-2
4. Bassett, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S.: 2020 verizon data breach report (2020)
5. Boyce, M.W., Duma, K.M., Hettinger, L.J., Malone, T.B., Wilson, D.P., Lockett-Reynolds, J.: Human performance in cybersecurity: a research agenda. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 55, pp. 1115–1119 (2011)
6. Dhillon, G.: What to do before and after a cybersecurity breach? American University, Washington, DC, Kogod Cybersecurity Governance Center (2015)
7. Dutton, W.H.: Fostering a cybersecurity mindset. Internet Policy Rev. **6**(1), 110–123 (2017)
8. Eminağaoğlu, M., Uçar, E., Eren, Ş.: The positive outcomes of information security awareness training in companies-a case study. Inf. Secur. Tech. Rep. **14**(4), 223–229 (2009)
9. Guo, P.J., Kim, J., Rubin, R.: How video production affects student engagement: an empirical study of mooc videos. In: Proceedings of the First ACM Conference on Learning@ Scale Conference, pp. 41–50. ACM (2014)
10. Hinton, P.R., McMurray, I., Brownlow, C.: SPSS Explained. Routledge, London (2014)
11. Hussain, S., Kamal, A., Ahmad, S., Rasool, G., Iqbal, S.: Threat modelling methodologies: a survey. Sci. Int. (Lahore) **26**(4), 1607–1609 (2014)
12. Kent State University: SPSS tutorials: Paired samples T test (2019). https://libguides.library.kent.edu/spss/pairedsamplesttest
13. Kirkpatrick, D., Kirkpatrick, J.: Evaluating Training Programs: The Four Levels. Berrett-Koehler Publishers, San Francisco (2006)
14. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack–defense trees. In: Degano, P., Etalle, S., Guttman, J. (eds.) FAST 2010. LNCS, vol. 6561, pp. 80–95. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19751-2_6
15. Leach, J.: Improving user security behaviour. Comput. Secur. **22**(8), 685–692 (2003)
16. Lund, M.S., Solhaug, B., Stlen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12323-8
17. Mauw, S., Oostdijk, M.: Foundations of attack trees. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 186–198. Springer, Heidelberg (2006). https://doi.org/10.1007/11734727_17
18. Merkt, M., Weigand, S., Heier, A., Schwan, S.: Learning with videos vs. learning with print: the role of interactive features. Learn. Instr. **21**(6), 687–704 (2011)
19. Neuman, W.L., Robson, K.: Basics of social research: qualitative and quantitative approaches. Power **48**, 48 (2007)
20. Sciutto, J.: How one typo helped let Russian hackers. In: CNN, 27 June 2017

21. Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.J.: The impact of information richness on information security awareness training effectiveness. Comput. Educ. **52**(1), 92–100 (2009)
22. Topno, H.: Evaluation of training and development: an analysis of various models. J. Bus. Manage. **5**(2), 16–22 (2012)
23. Tripathi, J., Bansal, A.: A literature review on various models for evaluating training programs. IOSR J. Bus. Manage. **19**(11), 1 (2017)
24. Warr, P., Bird, M., Rackham, N.: Evaluation of management training: a practical framework, with cases, for evaluating training needs and results. Gower Press, London (1970)