Exploring Experiences of Using SETA in Nordic Municipalities

Aous Al Salek, Joakim Kävrestad, Marcus Nohlberg

Exploring experiences of using SETA in Nordic municipalities

Aous Al Salek[1][0000−0002−7462−1809], Joakim Kävrestad[1][0000−0003−2084−9119], and Marcus Nohlberg[1][0000−0001−5962−9995]

[1] University of Skövde, Sweden aous.al.salek@gmail.se
[2] University of Skövde, Sweden joakim.kavrestad@his.se
[3] University of Skövde, Sweden marcus.nohlberg@his.se

Abstract. User behavior is a key aspect of cybersecurity and it is well documented that insecure user behavior is the root cause of the majority of all cybersecurity incidents. Security Education, Training, and Awareness (SETA) is described by practitioners and researchers as the most important tool for improving cybersecurity behavior and has been for several decades. Further, there are several ways to work with SETA found in academic literature and a lot of research into various aspects of SETA effectiveness. However, the problem of insecure user behavior remains revealing a need for further research in the domain. While previous research have looked at the users' experience of SETA, this study looks at SETA adoption from the perspective of the adopting organization. For this purpose, a survey was sent out to all Nordic municipalities with the intent of measuring if and how SETA is conducted, and how the respondents would ideally like to conduct SETA. The results show that a majority of the participating organizations use SETA and that e-learning is the most common delivery method. However, the results also show that gamification and embedded training is seldom used in practice nor a part of the participants' picture of ideal SETA.

Keywords: SETA · awareness training · user awareness · adoption · organizations

1 Introduction

Cybersecurity is a domain that is socio-technical by its nature [18]. While the technical part of cybersecurity is certainly important it has been made evident that human behavior is a key factor in the majority of security incidents today [6, 7]. In essence, attackers have realized that exploiting user behavior is a feasible way to launch attacks against individuals as well as against organizations [13]. Improving user behavior, with regards to security, is one of the most pressing matters in cybersecurity [10]. The most commonly suggested, and adopted, means to this ends is SETA, Security Education, Training and Awareness, which commonly attempts to educate users on correct behavior and make them aware of the risks associated with insecure behavior [17].

SETA has been discussed in scientific literature for at least two decades [20]. Further, there is a multitude of methods by which SETA can be delivered discussed in previous research, with different benefits and drawbacks. Current methods of SETA delivery include:

- *Instructor led training* where participants are thought in the format of a lecture [24, 22]. This method is often appreciated by participants but the participants may not retain the acquired knowledge over time.
- *E-learning* where participants are sent, or given access to, digital training material [21]. A benefit of this training is that participants are able to access the SETA on-demand, but a consequence of that is that some users in the organization may not use the training.
- *Gamified training* is similar to e-learning but the learning modules are delivered as games [9, 12]. Gamified training is often motivated by the use of game mechanics to improve the learning process and has been shown to be appreciated by its users but suffer from the same potential shortcomings as e-learning.
- *Embedded training* where SETA is delivered to users in a situation where the training is of direct relevance [14, 16]. This is argued to add an awareness increasing mechanism and make the users more likely to participate in the training since it is presented to the user in a situation where it is of relevance. A potential drawback is that it may be seen as bothering by the users and that it is inherently more complex to deploy than the other described methods.

While neither the importance of user behavior nor the need for SETA is unknown, and while organizations do spend time and money on SETA efforts, the problem of insecure user behavior persists suggesting a need for continued research into the domain [2, 5]. A lot of previous research have studied SETA from a user perspective and there are several promising methods for SETA delivery discussed in scientific literature. However, how organizations procuring or developing SETA methods select and perceive different SETA methods is an underresearshed perspective. This paper addresses that perspective through a survey targeting Nordic municipalities. The survey intends to measure to what degree the participating municipalities employ SETA, and how they do it. The study will also investigate the participants' perception of ideal SETA with the intent of analyzing if there is a gap between the current and ideal practice. The study will complement existing research into SETA with an organizational perspective that can help researchers and practitioners understand the organizational effects of various SETA methods and the driving factors behind a decision to implement a certain SETA method.

2 Research approach

The intent of this study it to generate results representative for the municipalities in the Nordic countries; Sweden, Denmark, Norway, Finland and Iceland. There

are 1123 municipalities in total in these countries and a survey was considered a feasible way to give all of them a chance to participate in the study. Furthermore, surveys are often considered to make it easier for the respondents to provide information on sensitive topics, such as cybersecurity [8]. A survey with two question blocks was developed by the research team. The first block of questions intended to measure the proportion of municipalities that use SETA, what type of SETA they use and the perceived effect of SETA. The questions in this block were quantitative and designed to capture the proportion of the respondents that selected a certain option. As such, the results from the first block are reported as frequencies with corresponding margins of error, given a confidence level of 95%, as suggested by [26]. The second block intended to capture data about the participants' perception of ideal SETA including how SETA should be delivered and what content it should cover. To ensure that the participants were not biased by pre-decided answers, those questions were designed as free-texts answers. The data collected was therefore qualitative in nature, and analyzed using content analysis with the aim of summarizing the general opinions of the respondents [3, 15]. The answers were analyzed by one researcher with the intent of identifying themes discussed under each question, and the prevalence of each theme. During this process, each answer was coded as one or more themes. the coding was then reviewed by the rest of the research team and differences of opinions were discussed to form a common view.

3 Results and analysis

One of the major concerns of a web based survey methodology is to ensure that the participants correctly understand the questions [4]. In this case, the survey was sent to respondents in several countries, and a multilingual survey was developed to ensure that the respondents could answer the survey in their native language. The survey was developed in English and translated to the languages of the Nordic countries after development, by the company TransPerfect. Further, the survey was subjected to pretesting before and after translation in order to ensure its quality, as follows:

1. The survey was developed by the research team.
2. The survey was reviewed by two persons who were not IT-professionals, one of whom was an expert in statistics.
3. The survey was answered by an IT-professional during a think-aloud session.
4. The survey was translated and sent to 7 respondents from the various Nordic countries with additional questions requesting feedback on the survey itself.

The survey was distributed using e-mail and the tool Limesurvey. E-mail addresses to the Nordic municipalities were acquired from public list, except for the Norwegian municipalities were a list had to be procured. The survey was open for three weeks and a reminder was sent out after a period of two weeks. The survey was completed by 96 participants. Several municipalities have joint IT-department. Therefore, the 96 participants are representing 136 municipalities. Table 1 reflects the number of participants per country.

Country	Municipalities	Participants	Municipalities covered
Sweden	290	70	89
Norway	356	10	23
Iceland	69	3	3
Denmark	98	7	7
Finland	310	6	14
Total	1123	96	136

Table 1. Participants per country.

The first question in block one intended to measure how many municipalities that currently use, or previously used SETA. The respondents were asked "Does your organization currently offer information security awareness training for users?" and respodents who answered "no" were also asked "Has your organization had information security awareness training for users in the past?". The responses are presented in Table 2.

Answer	Proportion	Margin of error
Yes - now	71%	8.7%
Yes - in the past	14.6%	
No	14.6%	

Table 2. Prevalence of SETA

Table 2 shows that a vast majority of the participants' municipalities are offering SETA, or has offered SETA to users in the past. The next question asked the participants that currently used SETA what type of SETA they used. The answer options and proportion of respondents picking each option is presented in Table 3, note that the participants were asked to select all answers that applied to them. Table 3 shows that online training is the most common type of SETA used by the participating municipalities followed by written or oral information. Gamified or embedded training is only used by a small proportion of the respondents.

Answer	Proportion	Margin of error
Oral informative (lecture or personal)	54.4%	11.5%
Written information	52.9%	11.5%
Promotional	10.3%	7.3%
Online	80.9%	9%
Gamified	4.4%	5.3%
Embedded	11.8%	7.7%
Other	10.29%	7.3%

Table 3. Use of SETA types

The third question intended to analyze how frequently the users in the municipalities were subjected to SETA and was "How often do users receive information security awareness training?". The answer options and proportion of respondents selecting each answer are shown in Table 4, which demonstrates that while the frequency of SETA varies quite a lot, a majority of the participants report subjecting users to SETA annually or less frequently.

Answer	**Proportion**	**Margin of error**
Daily	2.9%	4.6%
Weekly	5.9%	5.9%
Monthly	14.7%	8.2%
Quarterly	8.8%	6.9%
Semi-annually	2.9%	4.6%
Annually	35.3%	11%
Less frequently	27.9%	10.3%

Table 4. SETA frequency

The final question in block one asked the participants "What is the general attitude of trainees towards information security awareness training?". 61.8% responded that the trainees are positive to the SETA while 32.6% perceived them as indifferent. Only 1.5 % of the respondents perceived the trainees as negative towards SETA.

The second block of the survey contained three open questions that intended to capture the respondents perception of how SETA should ideally be carried out and what it should result in. Those questions were answered by all respondents, regardless of their responses to the previous questions. The data was analyzed using a content analysis approach. The analysis was carried out in four steps:

1. Each answer was analyzed and the themes described in the answer were recorded by the lead researcher.
2. The coding was reviewed by the rest of the research team.
3. The themes were summarized by the lead researcher.
4. The summaries were reviewed by the rest of the research team.

The first question was *What are the most important key factors regarding the design of information security awareness training? (e.g., frequency, length, cost, users covered, being mandatory).* The themes identified in the responses to this questions were:

- It should be mandatory - 18 mentions.
- It should be easy to consume, require little time and be easy to access - 45 mentions.
- It should be re-occurring - 25 mentions.
- It should be appreciated by users - 3 mentions.
- It should be possible to adapt the material - 8 mentions.

- It should not be costly - 10 mentions.
- Management must be openly positive towards it - 3 mentions.
- The information should be easy to understand and relevant for the users - 31 mentions.

The identified themes reveal a user centered pattern where the two most prevalent themes describe that the participants think that SETA must be easy to access for users, and not require a lot of time to consume. This is motivated both in terms of not consuming too much of the users' work-day and with the notion that users will not bother if the training is too time-consuming. The respondents also describe that the training should be relevant and at a level that is easy to consume. Some respondents explicitly mention that the material should not be too technical. A further pattern is that the respondents argue that the training should be re-occurring so that the training is reinforced and to ensure that the users are provided with up-to-date information.

The second question was *What is the information security awareness training delivery method or combination of methods that suites your organization the most?* The themes identified in the responses to this questions were:

- Instructor led training - 26 mentions.
- Training via e-mail - 5 mentions.
- Nanolearning - 12 mentions.
- E-learning - 44 mentions.
- Written guides - 1 mention.
- Tests including knowledge tests and attack simulations (such as phishing resilience tests) - 5 mentions.
- Embedded - 2 mentions.

In response to this question, the respondents mention e-learning using videos or interactive content. Some respondents also mention sending training via e-mail or using nanolearning and it is hard to differentiate between those themes and e-learning. However, the analysis clearly shows that a majority of the participants favour using a digital form of training that the users can consume in their own time. Instructor led training is also a common theme and several respondents describe that instructor led training is given during staff meetings and/or on-boarding of new employees and then combined with digital re-occurring training. It is further noticeable that embedded training is only mentioned by two respondents and gamified training is not mentioned at all. The results are also in line with what training methods that are actually used in the respondents organizations, as displayed in Table 3. Several respondents mention that a reason for using e-learning is that it is cost efficient and easy to distribute to the users continuously. However, a few participants also mention that a drawback of e-learning is that it is hard to ensure that all users are participating.

The last open question was *What are the results expected from information security awareness training?* The themes identified in the responses to this question were:

- A higher level of security - 5 mentions.
- Less security incidents - 26 mentions.
- Adherence to organizational policies - 1 mention.
- Improved security culture - 52 mentions.

The pattern that emerges in response to the last question is that improved security culture and less security incidents are expected outcomes of SETA. Those are mentioned in combination by several respondents suggesting that the respondents perceive improved security culture as a precursor to less security incidents.

4 Discussion and conclusion

The intent of this paper is twofold. The first aim was to measure if and how Nordic municipalities provide SETA for their users. The study was carried out as a survey among Nordic municipalities and the first block of the survey contained quantitative questions aimed towards this first research aim. The results show that a majority of the participants' organizations (about 85%) used SETA now or in the past. While this is not surprising, given the impact that user behavior has on cybersecurity and how commonly SETA is described as a key factor for influencing user behavior, it suggests that the Nordic municipalities are well aware of this fact and that actions for improved user behavior are on their agenda. The results further show that e-learning, instructor led training and written information are the most common forms of SETA employed and other methods are only used in a few of the participants' organizations. E-learning is described as cost efficient and easy to distribute and its popularity is therefore not surprising. A result that was a bit more surprising was that gamification, despite its common occurrence in recent research [23, 1, 11], was used by less than 5% of the participants' municipalities. Finally, the results show that only about 40% of the participants' municipalities distribute SETA more frequently than once a year.

The second aim was to research the participants' perception of ideal SETA through the use of open ended questions. The intent was further to compare the participants' perception of ideal SETA to the current practice. The results in this part highlight that the participants perceive user behavior as a key part of cybersecurity. The participants describe that SETA should be easy to consume and relevant for the users. Several participants highlight that getting users to participate in SETA is a challenge and that could explain why they stated that SETA should be re-occurring and mandatory to participate in. On that note, it is interesting to see that a common perception is that SETA should be a natural and re-occurring part of cybersecurty practices while only about 40% of the participants' municipalities employ SETA more than once a year. The participants further describe that e-learning and instructor led training are the delivery methods best suited for their organizations. These results are well in line with the results showing that those are the most frequently used delivery methods in practice. It is, however, noticeable that embedded training is only mentioned by two

respondents and gamified training is not mentioned at all. Given the pedagogical benefits attributed to gamification [12], and the re-occurring nature of embedded training [14], the low prevalence of those methods is noticeable. Whether these results reflect that the participants prefer e-learning, are unaware of embedded training and gamification, or something else is beyond the scope of this study and an interesting area for future research.

The target population of this survey was Nordic municipalities. The survey was completed by 96 participants but covered 136 municipalities since several respondents worked in IT-organizations responsible for two or more municipalities. The survey covered about 12% of the population, which is common for web based surveys [19, 25]. Further, the response rate between the Nordic nations was uneven with the survey covering 31% of the Swedish municipalities but only a few percentages of the municipalities in the other Nordic countries. A possible explanation for this can be that the research team is based in Sweden and the Swedish municipalities are aware of the research institutions, whereas the other municipalities are not. The distribution of respondents could mean that the results are primarily valid for Swedish municipalities and the results should be interpreted with that in mind. A further possible limitation of this study is self-reporting bias that is always a risk with survey based studies. It is possible that respondents refrain from disclosing security sensitive data and this survey could be interpreted as such. It is further well known that respondents tend to portrait a positive image of themselves and that could lead to results that are more favourable than what is actually the case. Self-reporting bias was counteracted in this study by guaranteeing the anonymity of the respondents and by translating the survey to the respondents native language to make the respondents more comfortable with the survey. Allowing the respondents to answer the survey in the native language was also intended to increase the understandability of the survey.

This study concludes that a majority of the Nordic municipalities use SETA on a regular basis and that e-learning alone or in combination with written guides and/or instructor led training are the most common delivery methods for SETA. A second conclusion is that SETA is deployed in a multi-faceted way and it would be interesting for future studies to compare the effects of different deployment strategies. The study further concludes that the participants perceive that effective SETA should be easy for users to participate in meaning that the material should be relevant and the effort needed to participate minimized. SETA should also be a regular occurrence and the study suggests that the participants believe that SETA should be more regular than what is currently the case.

This study was limited to Nordic municipalities and the results should be interpreted in that context. A given direction for future work would be to research similar topics in the private sector and in public sector organizations outside of the Nordic region. Further, this study identifies that gamified and embedded SETA is only used by a small portion of the study's respondents. Further, those methods are not included in what the participants perceive as ideal SETA. Given

the prevalence of those methods in research, and the positive aspects attributed to them, the reason for why they are not adopted should be further researched.

References

1. Aldawood, H., Skinner, G.: Educating and raising awareness on cyber security social engineering: A literature review. In: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). pp. 62–68. IEEE (2018)
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. Berelson, B.: Content analysis in communication research. Content analysis in communication research., Free Press, New York, NY, US (1952)
4. Berndtsson, M., Hansson, J., Olsson, B., Lundell, B.: Thesis projects: a guide for students in computer science and information systems. Springer Science & Business Media (2007)
5. de Bruijn, H., Janssen, M.: Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly **34**(1), 1–7 (2017)
6. Cybint: 15 alarming cyber security facts and stats. (2020), https://www.cybintsolutions.com/cyber-security-facts-stats/
7. EC-Council: The top types of cybersecurity attacks of 2019, till date (2019), https://blog.eccouncil.org/the-top-types-of-cybersecurity-attacks-of-2019-till-date/
8. Fowler Jr, F.J.: Survey research methods. Sage publications (2013)
9. Gjertsen, E.G.B., Gjaere, E.A., Bartnes, M., Flores, W.R.: Gamification of Information Security Awareness and Training. Icissp 2017
10. Hadlington, L.: Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon **3**(7), e00346 (2017)
11. Handayani, V., Budiono, F.L., Rosyada, D., Amriza, R.N.S., Masruroh, S.U., et al.: Gamified learning platform analysis for designing a gamification-based ui/ux of e-learning applications: A systematic literature review. In: 2020 8th International Conference on Cyber and IT Service Management (CITSM). pp. 1–5. IEEE (2020)
12. Huynh, D., Luong, P., Iida, H., Beuran, R.: Design and Evaluation of a Cybersecurity Awareness Training Game, Lecture Notes in Computer Science, vol. 10507, pp. 183–188
13. Joinson, A., van Steen, T.: Human aspects of cyber security: Behaviour or culture change? Cyber Security: A Peer-Reviewed Journal **1**(4), 351–360 (2018)
14. Kävrestad, J., Nohlberg, M.: Contextbased microtraining: A framework for information security training. In: International Symposium on Human Aspects of Information Security and Assurance. pp. 71–81. Springer (2020)
15. Krippendorff, K.: Reliability in content analysis: Some common misconceptions and recommendations. Human Communication Research **30**(3), 411–433 (2006). https://doi.org/10.1111/j.1468-2958.2004.tb00738.x, https://doi.org/10.1111/j.1468-2958.2004.tb00738.x
16. Lim, I.K., Park, Y.G., Lee, J.K.: Design of security training system for individual users. Wireless Personal Communications **90**(3), 1105–1120

17. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS quarterly pp. 757–778 (2010)
18. Safa, N.S., Von Solms, R.: An information security knowledge sharing model in organizations. Computers in Human Behavior **57**, 442–451 (2016)
19. Sauermann, H., Roach, M.: Increasing web survey response rates in innovation research: An experimental study of static and dynamic contact design features. Research Policy **42**(1), 273–286 (2013)
20. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security (2000)
21. Takata, T., Ogura, K., Ieee: Confront Phishing Attacks - from a Perspective of Security Education, pp. 10–13. International Conference on Awareness Science and Technology (2019)
22. Taneski, V., Heričko, M., Brumen, B.: Impact of security education on password change. pp. 1350–1355
23. Tchakounté, F., Wabo, L.K., Atemkeng, M.: A review of gamification applied to phishing (2020)
24. Van Rensburg, W.J., Thomson, K.L., Futcher, L.: An Educational Intervention Towards Safe Smartphone Usage. HAISA 2018 (2018)
25. Walston, J.T., Lissitz, R.W., Rudner, L.M.: The influence of web-based questionnaire presentation variations on survey cooperation and perceptions of survey quality. Journal of Official Statistics **22**(2), 271 (2006)
26. Wheelan, C.: Naked statistics: Stripping the dread from the data. WW Norton & Company (2013)