Extracting Guidelines for Security Education, Training and Awareness Programme from the Literature

Olivier de Casanove, Florence Sèdes

Extracting Guidelines for Security Education, Training and Awareness Programme from the Literature

Olivier de Casanove[1] and Florence Sèdes[1]

IRIT, Université Toulouse III - Paul Sabatier,
118 route de Narbonne 31062 CEDEX 9 Toulouse
{olivier.decasanove,florence.sedes}@irit.fr

Abstract. Security standards help to create security policies, but they are often very descriptive, especially when it comes to security awareness. Information systems security awareness is vital to maintain a high level of security. SETA programmes (Security Education, Training and Awareness) increase information systems security awareness and play an important role in finding the strategic balance between the prevention and response paradigms. By reviewing the literature, we identify guidelines for designing a SETA programme following a PDCA (Plan Do Check Adjust) cycle.

Keywords: Prevention · PDCA · information systems security · Awareness · SETA · Guidelines · Review

1 Introduction

Defining security awareness is a challenging task. Tsohou et al. [36] even conclude their paper saying that the absence of concrete definition creates frustration among security experts; this could be a reason why security awareness remains an issue. In this paper we will consider that the objective of security awareness is to reduce the share of security incidents caused by humans.

To decrease the proportion of security incidents caused by well-meaning users, we need to educate them. As stated in [38] "Accountability must be derived from a fully informed, well-trained and aware workforce." Some information system security standards define objectives to promote a security culture and to raise awareness. Some of the most famous standards addressing this concern is the ISO/IEC 27000 family [18] and COBIT [17]. These standards often follow a Plan Do Check Adjust (PDCA) cycle. PDCA is a method for control and continuous improvement of processes or tools. As the IT world is ever-evolving, a continuous improvement method such as PDCA is suitable for information systems security. Unfortunately, information system security standards are very descriptive [4]. They set goals to reach but rarely provide process or methodology on how to reach them; there is a need for guidelines.

In this paper we will review the literature to identify guidelines to promote a security culture and raise awareness thanks to security education, training

and awareness programmes (SETA programmes). It should be noted that some authors disagree with considering education and training as security awareness [36]. These guidelines are presented in four sections, each section corresponds to a step in the PDCA cycle. Then, we discuss the future of SETA programmes and security awareness. Finally, we conclude.

2 Plan the SETA programme

A SETA programme is designed to make people adopt safe behaviours. People will still make mistakes even if they behave safely, but if we are successful, they will make fewer. The most effective way to change security behaviours is to make people adopt a security culture [34]. To adopt a new culture, it is advised to generate an intrinsic motivation [33]. In other words, SETA programmes should increase empowerment, which is a strong lever to increase security awareness [13]. A SETA programme designed to generate intrinsic motivation is more likely to be successful over a long period of time. To design such a programme we need to identify four elements: the source of the message, the type of message, the media of the message and the target of the message.

2.1 The source

First, we need to understand who is the source of the message [34]. Depending on its hierarchical level, the programme will not have the same degree of complexity. For example, if the message is from executives, the objective will be to teach non-technical ideas, for example *how to have good digital hygiene?* As executives have less understanding of the production environment than team leaders, their messages should not be about technical matters. It is the role of the team leaders to translate the non-technical messages into technical messages that are relevant to what their team is facing. For example, the team leader can turn the previous non-technical message into *How to use the shared mailbox safely?*

2.2 The type of message

There are two forms of communication that the SETA programme should adopt [33][38]:

- *Persuasive communication/education:* it answers the question "why" in the user's mind. It should increase people's insight and motivation.
- *Active participation/training:* it answers the question "how" in the user's mind. It should develop skills and competence.

Both are equally important; people will not be satisfied if the only reason given for improving security is "just do it" and they cannot do anything if they do not know how. A good programme is a combination of active training and persuasive communication [33] There are five themes to conduct a security awareness campaign [20]: deterrence, morality, regret, incentive or feedback. They are defined as follows:

- *Deterrence messages* associate sanction to a bad action. This assumes that people are rational and will choose the best option for them, which will not be the one with the expected penalty. Empirical evidence that SETA programmes are suitable for deterrence messages can be found in [9]. This finding is confirmed by the literature review [1]. Deterrence messages can also be considered in the literature as fear messages. Fear is one of the most used messages in the industry.
- *Morality messages* attempt to evoke our own moral principles to avoid bad decisions. Empirical evidence that moral reasoning has an impact on security behaviour can be found in [28]. The authors also argue that appropriate punishment activities are important for moral reasoning to be effective. Punishment activities obviously cannot be carried out during a SETA programme.
- *Regret messages* assume that people can anticipate the emotional consequences of their choices before making a decision. This anticipation would encourage people to make the right choice. Empirical evidence of the positive effect of regret on security behaviour is found in [8] but is not distinguished from deterrence or morality. No significant evidence is found in [41].
- *Incentive messages* assume that giving rewards for doing the right thing helps people improve their behaviour. This can be seen as the opposite of regret messages. Empirical studies show that rewards for compliance with security policies and procedures are not associated with the individual's perceived mandatoriness of the established set of policies and procedures [7] or with compliance [30]. A survey also concludes that rewards do not directly influence security behaviour [1]. However, [3] finds theoretical evidence of positive effects on security behaviour and [8] finds empirical evidence that the incentive has a positive effect. Financial rewards also have a positive effect on security behaviour according to [15].
- *Feedback messages* assume that people will change their behaviour if they receive feedback on their actions, this can be positive or negative reinforcement. In [37], West explains that classical feedback mechanisms do not work in information systems security; the consequence of a bad action is often delayed, and the consequence of a good one is not to be under attack, in other words, nothing happens. Reinforcement learning is therefore not effective in this context.

In [26], the authors compared the effectiveness of different themes for a password policies awareness campaign to a control group and they found no significant difference between the groups' willingness to comply. They suggest that, on a motivate public, theme does not matter.

2.3 The media

There are different media for conveying a SETA programme and choosing the right one is an important decision. The choice of media depends on multiple factors, seven have been identified in [38]:

- *The population we are targeting:* as mentioned in the previous section, there is little literature about developing a SETA programme for a specific population.
- *The why or the how:* some media are more suited for persuasive communication, and others for active participation. [38] lists the possible media according to the question they answer. [2] suggests that video-based communication is more effective than text-based communication to answer the question "why" (the objective of the study was motivating users to adopt password managers)
- *The price:* [38] details which media are cheap and which are expensive.
- *Ease of use:* How easy is it to access, deploy, update and maintain the SETA programme?
- *Scalability:* Can the material be used for different sized audiences and in different locations?
- *Support:* Will support for the programme be internal or external ? Is it easy to find help to use the material?
- *Accountability:* Which statistics can be used to measure the effectiveness of the programme ? How comprehensive are these measures?

As mentioned in the previous section, we need to use media that allow us to answer the question of how (active training) and why (persuasive communication).

2.4 The target

Finally, a SETA programme should be audience-specific. Unfortunately, little work has been done to study the relationship between public types and other factors, such as the theme of a SETA programme. However, one paper finds that there might be a correlation between personality traits and the effectiveness of a theme [20]. The most relevant advice found regarding the public is to divide the population by groups of interest. This recommendation is found several times in the literature, regardless of the study publication date [6][35][38].

Summary To plan a SETA programme we should assess available resources, understand who is the source of the message, what message we want to communicate, how we want to promote it and who is the target.

3 Do the SETA programme

Information system security, and particularly prevention, is sometimes seen as a constraint and a loss of time for the attendees. To fight this idea we need to have as little impact as possible on their daily work; therefore we should communicate the plan to all stakeholders [1][38]. This means the people we are training, but also their immediate superior and other people they work with who are not involved in the programme. During the session, the trainees will not be able to maintain production; everyone working with them must be prepared

for the consequences. In addition, the SETA programme should be organised in short sessions [35][24]. Providing social interactions during a session increases the effectiveness of the SETA programme and triggers positive changes in security behaviour [1][10][21][11][34]. The direct implication of this is that e-learning and other MOOCs (Massive Open Online Course) are not relevant for our needs. At the end of the programme, giving goodies is a good way to spread our message and reinforce the commitment [35]. When we carry out the programme, the most important thing is the public's willingness to participate [21]. To increase the public's willingness to participate it is tempting to use gamification [12], yet as shown by [29] gamification in the context of security awareness does not always hit.

Summary Attendees' coworkers should be warned that attendees will not be available to maintain production. A programme without social interaction is designed to fail.

4 Check the SETA programme

The check step is important for the continuous improvement of the SETA programme. In order to evaluate our programme, we will need to collect data. They can be feedback, questionnaires or notes taken during the session. We identified three types of evaluation in the literature:

- *Measure of behavioural intention:* This is the most represented type of evaluation in the literature. The assumption behind this type of evaluation is that system, method or tool use can be estimated using many other measures, and that the behavioural intention to use is a good estimator of actual usage. For example, if we run a campaign to promote password managers, the higher the user's intention to use them, the more successful the campaign is.
- *Knowledge oriented:* People who have less understanding of security concepts are more likely to be victims of an attack. Therefore, assessing the knowledge gained after the SETA programme can be an indicator of the effectiveness of the programme.
- *Ulterior incident rate:* This method consists of measuring the incident rate ulterior to the campaign. For example, if we run a campaign against bad password management and the rate of incidents related to bad password management decreases after the campaign, we can consider the campaign successful.

Regardless of the solution we choose to evaluate our programme, we need to think about automating the evaluation [38][22]. Some SETA programmes can be huge; the process of collecting the data and then interpreting it can be time consuming. Obviously, some types of data are better suited for automation than others. Hand notes of the session, open-ended questions and oral feedback need a human to interpret them; therefore this is difficult to process automatically. On the other hand, online questionnaires or at least multiple-choice questionnaires are easier to process automatically.

Table 1. Frequency of Special Characters

Evaluation method	References
Measure of behavioural intention	[16][19][25]*[32]
Knowledge test	[14][22][23][27]
Ulterior incident rate	[38]

* is a literature review about behavioural intention in information systems security.

Summary At this step, we need to choose a way to evaluate our programme. As the SETA programme will grow, it will be harder to evaluate it without automation. Some evaluation methods are most suited for automation than others; this should be taken into consideration when choosing the method to evaluate our programme.

5 Adjust the SETA programme

The adjust step will improve the programme for a future iteration. By using PDCA, we prevent flows from occurring in our SETA programmes in the first place, or once they do, we stop them from continuing.

After improving our programme based on the feedback we collected at the check step, we should verify if the campaign is consistent with the new policies and environment. The IT environment is an ever-evolving place, it is important to check if the messages provided are not obsolete. If so, we will need to update them or add new ones if we have new technology in our environment.

Once we have our new programme, we should consider launching a new campaign. This cycle is the single-loop learning of the prevention paradigm described in [5]. Since we are considering SETA programme as a continuous process, a new campaign should be launched on a regular basis. Exactly as it seems obvious to everyone to update their antivirus software, security culture must also be updated.

Summary The improvement process is in two parts: first improve the programme based on the feedback, second verify if the messages are still up to date. A new campaign must be planned at the end of the previous one.

6 Discussion

Prevention is an important aspect of security. It differs from other aspects of security by putting the user back at the centre of the information system. Some tools for security, like intrusion detection systems, are designed with theoretical assumptions and do not take final users into account, resulting in not that good performance in real application. Thanks to SETA programmes, people adopt a safer behaviour and a more coherent with the expected behaviour, which results in a diminution of false positive raised by detection systems. Putting the

user back in the centre of the information system is associated with the field of "Human-Centred Security & Privacy" (HCSP), see [31] for a brief overview of this field.

The theme of deterrence is dominant in security awareness, probably because of the relationship between information systems security and criminology. Other themes and how they interact with other variables, like the target of a campaign, is not well studied in the literature. Khan et al. [21] identify that information systems security awareness lags behind other domains such as ecological or public health awareness. They propose to imitate techniques from other fields to improve information systems security awareness. For example, in public health, a reference model is the EPPM (Extended Parallel Process Model) [39][40]. This model works well with messages fear-based (or deterrence messages), which are effective for SETA programmes. Developing such a model for information system security could be useful. This model also has the advantage of explaining why some campaigns may backfire.

Another problem with current security awareness is the lack of datasets. Many models are compared to find out which one is the best to explain the studied population behaviour, but none of them were compared with the same dataset. As a result, it is difficult to conclude that one model is better or worse than any other. In addition there is a need for reproducibility since the datasets are not public.

While many tools in information system security are automated, non-technical security measures are exceptions to this rule. The PDCA cycle permits at least to create a clear process which will facilitate the creation of a SETA programme. We used the PDCA cycle because it is a widely used tool in the industry, but other controls and continuous improvement of process tools should be studied, or created if needed, to better suit the needs of information system security.

7 Conclusion

Security awareness is a major concern in information system security. To promote awareness, we use SETA programmes which should be considered as a part of a security culture. However, there is a lack of methodology on how to implement them in the state of the art. This is the problem we try to address in this paper. By reviewing the literature, we identify guidelines for designing a SETA programme following a PDCA cycle. The PDCA cycle allows us to be prescriptive and not just descriptive as many current standards does. In addition PDCA facilitate the continuous improvement of awareness campaign which, as every security tool, should stay updated.

We believe this work can help information system security actors to design better prevention programmes but not only. This work can also be used by researchers who want to study the various topics related to prevention. They can find in this paper guidelines to create effective programmes to convey messages, leading to more efficient prevention campaign and more significant results.

References

1. Abraham, S.: Information Security Behavior: Factors and Research Directions. In: AMCIS - 2011 Proceedings - All Submissions. p. 462 (2011)
2. Albayram, Y., Liu, J., Cangonj, S.: Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager. In: European Symposium on Usable Security 2021, pp. 89–104. Association for Computing Machinery, New York, NY, USA (Oct 2021)
3. August, T., Tunca, T.I.: Network Software Security and User Incentives. Management Science **52**(11), 1703–1720 (2006)
4. Barlette, Y., Fomin, V.V.: The Adoption of Information Security Management Standards: A Literature Review, pp. 69–90. IGI Global (2010). https://doi.org/10.4018/978-1-61520-965-1.ch104
5. Baskerville, R., Spagnoletti, P., Kim, J.: Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management **51**(1), 138–151 (Jan 2014). https://doi.org/10.1016/j.im.2013.11.004
6. Bauer, S., Bernroider, E.W.N., Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' noncompliance with information security policies in banks. Computers & Security **68**, 145–159 (Jul 2017). https://doi.org/10.1016/j.cose.2017.04.009
7. Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W.: If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems **18**(2), 151–164 (Apr 2009). https://doi.org/10.1057/ejis.2009.8
8. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly **34**(3), 523–548 (2010). https://doi.org/10.2307/25750690
9. D'Arcy, J., Hovav, A., Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research **20**(1), 79–98 (Mar 2009). https://doi.org/10.1287/isre.1070.0160
10. Das, S., Dabbish, L.A., Hong, J.I.: A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. pp. 97–115 (2019)
11. Das, S., Kim, T.H.J., Dabbish, L.A., Hong, J.I.: The effect of social influence on security sensitivity. In: 10th Symposium On Usable Privacy and Security (SOUPS 2014). pp. 143–157. USENIX Association, Menlo Park, CA (Jul 2014)
12. Deterding, S., Dixon, D., Khaled, R., Nacke, L.: From game design elements to gamefulness: defining gamification. In: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. pp. 9–15. MindTrek '11, ACM, New York, NY, USA (Sep 2011). https://doi.org/10.1145/2181037.2181040
13. Dhillon, G., Backhouse, J.: Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal **11**(2), 127–153 (2001). https://doi.org/https://doi.org/10.1046/j.1365-2575.2001.00099.x
14. Drevin, L., Kruger, H., Bell, A.M., Steyn, T.: A Linguistic Approach to Information Security Awareness Education in a Healthcare Environment. In: Bishop, M., Futcher, L., Miloslavskaya, N., Theocharidou, M. (eds.) Information Security Education for a Global Digital Society. pp. 87–97. IFIP Advances in Information and Communication Technology, Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-58553-6$_8$

15. Goel, S., Williams, K.J., Huang, J., Warkentin, M.: Can financial incentives help with the struggle for security policy compliance? Information Management **58**(4), 103447 (2021). https://doi.org/https://doi.org/10.1016/j.im.2021.103447, https://www.sciencedirect.com/science/article/pii/S0378720621000215
16. Huang, D.L., Patrick Rau, P.L., Salvendy, G., Gao, F., Zhou, J.: Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies **69**(12), 870–883 (Dec 2011). https://doi.org/10.1016/j.ijhcs.2011.07.007
17. ISACA: Cobit framework (2019), https://www.isaca.org/resources/cobit
18. ISO: Iso 27000 framework (2018), https://www.iso.org/standard/73906.html
19. Johnston, A.C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly **34**(3), 549–566 (2010). https://doi.org/10.2307/25750691
20. Kajzer, M., D'Arcy, J., Crowell, C.R., Striegel, A., Van Bruggen, D.: An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security **43**, 64–76 (Jun 2014). https://doi.org/10.1016/j.cose.2014.03.003
21. Khan, B., Alghathbar, K.S., Khan, M.K.: Information Security Awareness Campaign: An Alternate Approach. In: Kim, T.h., Adeli, H., Robles, R.J., Balitanas, M. (eds.) Information Security and Assurance. pp. 1–10. Communications in Computer and Information Science, Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23141-4$_1$
22. Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Computers & Security **25**(4), 289–296 (Jun 2006). https://doi.org/10.1016/j.cose.2006.02.008
23. Kruger, H., Drevin, L., Steyn, T.: A vocabulary test to assess information security awareness. Information Management & Computer Security **18**(5), 316–327 (Jan 2010). https://doi.org/10.1108/09685221011095236
24. Kävrestad, J., Skärgård, M., Nohlberg, M.: Users perception of using CBMT for informationsecurity training. In: Human Aspects of Information Security & Assurance (HAISA 2019) International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), Nicosia, Cyprus, July 15-17, 201. pp. 122–131. University of Plymouth Press (2019)
25. Lebek, B., Uffen, J., Neumann, M., Hohler, B., H. Breitner, M.: Information security awareness and behavior: a theory-based literature review. Management Research Review **37**(12), 1049–1092 (Jan 2014). https://doi.org/10.1108/MRR-04-2013-0085
26. Mayer, P., Kunz, A., Volkamer, M.: Motivating Users to Consider Recommendations on Password Management Strategies. In: HAISA 2018. pp. 28–37 (2018)
27. Mayer, P., Schwartz, C., Volkamer, M.: On the systematic development and evaluation of password security awareness-raising materials. In: Proceedings of the 34th Annual Computer Security Applications Conference. pp. 733–748 (2018)
28. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems **18**(2), 126–139 (Apr 2009). https://doi.org/10.1057/ejis.2009.10
29. Ophoff, J., Dietz, F.: Using Gamification to Improve Information Security Behavior: A Password Strength Experiment. In: Drevin, L., Theocharidou, M. (eds.) Information Security Education. Education in Proactive Information Security. pp. 157–169. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-23451-5$_1$2
30. Pahnila, S., Siponen, M., Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance. pp. 156b–156b. IEEE (2007). https://doi.org/10.1109/HICSS.2007.206

31. Renaud, K., Flowerday, S.: Contemplating human-centred security & privacy research: Suggesting future directions. Journal of Information Security and Applications **34**, 76–81 (Jun 2017). https://doi.org/10.1016/j.jisa.2017.05.006
32. Shropshire, J., Warkentin, M., Sharma, S.: Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security **49**, 177–191 (Mar 2015). https://doi.org/10.1016/j.cose.2015.01.002
33. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security **8**(1), 31–41 (Jan 2000). https://doi.org/10.1108/09685220010371394
34. von Solms, R., von Solms, B.: From policies to culture. Computers & Security **23**(4), 275–279 (Jun 2004). https://doi.org/10.1016/j.cose.2004.01.013
35. Thomson, M., von Solms, R.: Information security awareness: educating your users effectively. Information Management & Computer Security **6**(4), 167–173 (Jan 1998). https://doi.org/10.1108/09685229810227649
36. Tsohou, A., Kokolakis, S., Karyda, M., Kiountouzis, E.: Investigating Information Security Awareness: Research and Practice Gaps. Information Security Journal: A Global Perspective **17**(5-6), 207–227 (Dec 2008). https://doi.org/10.1080/19393550802492487
37. West, R.: The psychology of security. Commun. ACM **51**(4), 34–40 (apr 2008). https://doi.org/10.1145/1330311.1330320, https://doi.org/10.1145/1330311.1330320
38. Wilson, M., Hash, J.: Building an Information Technology Security Awareness and Training Program. Tech. rep. (Oct 2003). https://doi.org/10.6028/NIST.SP.800-50
39. Witte, K.: Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs **59**(4), 329–349 (1992). https://doi.org/10.1080/03637759209376276
40. Witte, K.: Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. Journal of Health Communication **1**(4), 317–342 (Oct 1996). https://doi.org/10.1080/108107396127988
41. Wright, C., Ayton, P.: Focusing on what might happen and how it could feel: can the anticipation of regret change students' computing-related choices? International Journal of Human-Computer Studies **62**(6), 759–783 (Jun 2005). https://doi.org/10.1016/j.ijhcs.2005.03.001