Guidelines for Security Education, Training and Awareness: a literature review

Olivier de Casanove, Florence Sèdes

Guidelines for Security Education, Training and Awareness: a literature review

Olivier de Casanove and Florence Sèdes

IRIT, Université Toulouse III, UPS
{Olivier.DeCasanove, Florence.Sedes}@irit.fr

Abstract. Security standards help to create security policies but they are often very descriptive, especially when they are about 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 prevention paradigm and response paradigm. By reviewing the literature, we identify guidelines to design a SETA programme following a PDCA (Plan Do Check Adjust) cycle.

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

1 Introduction

Security awareness is very hard to define. Tsohou et al. [33] even conclude their paper saying the absence of concrete definition creates frustration among security experts; that could be a reason why security awareness remains a problem. We will consider, in this paper, that the objective of security awareness is to reduce the part of security incidents caused by humans. It is hard to estimate, among all the security breaches, how many times humans were responsible. To give an idea of the problem, M.G. Lee [24] estimates, thanks to a dataset of the Commissioner's Office of the United Kingdom, that 46.2% of security breaches resulting in privacy violation are due to well-meaning insider human's mistakes.

To decrease the part of security incidents caused by well meaning users, we need to educate them. As said in [35] "Accountability must be derived from a fully informed, well-trained and aware workforce." Some standards in information system security define objectives to promote a culture of security and raise awareness. Some of the most famous standards addressing this concern are ISO/IEC 27000 family [17] and COBIT [16]. Those standards often follow a Plan Do Check Adjust (PDCA) cycle. PDCA is a method for control and continuous improvement of processes or tools. Because the IT world is ever evolving, a method allowing continuous improvement as PDCA is suited for information systems security. Sadly, many information system security standards are very descriptive [4]. They are setting a goal to reach but rarely offer advice on how to reach them. Therefore, there is a need for guidelines.

In this paper we will focus on security education, training and awareness (SETA) programme. It should be noticed that some authors do not agree to consider education

and training as security awareness [33]. The objective of this paper is to draw guidelines derived from the state of the art. Those guidelines are presented in four sections, each of them is a step of the PDCA cycle. In the final section, we discuss the future of SETA programmes and security awareness and then we conclude.

2 Plan the SETA program

Planning the SETA programme is very important to avoid pitfall. Article L4121-2 of French labour code [25] give guidelines on how to deal with prevention in general: "Plan prevention by integrating, in a coherent whole, technique, work organisation, working conditions, social relations and the influence of environmental factors." In other words, when designing a SETA programme, one should take into consideration the context. This statement is coherent with [5] which state that prevention and response paradigms in security should go hand by hand. The response paradigm, in information system security, encompasses all the techniques, tools and protocols allowing managing an incident and this is a part of the context in which the SETA programme will be used. The role of SETA programmes can be defined as the objective to mitigate risks that can't be avoided. A SETA programme is made to influence behaviours. The objective is to make adopt people a safer behaviour than they had. It means that the people will continue to make mistakes, but if we succeed, they will make less. The most efficient way to change security behaviours is to make people adopt a security culture [31]. To adopt a new culture, it is advised to generate an intrinsic motivation [30]. In other words, SETA programmes should increase empowerment. A SETA programme design to generate intrinsic motivation is most likely to succeed over a long period. Because SETA programme is part of a continuous process, it is important to work with what we already have. In order to not start from scratch, we should assess all the tools at its disposal and currently used to increase security awareness. Once assessing is over, we have to choose the means to conduct the programme.

First, we need to understand who is the source of the message [31]. Depending on the level in the hierarchy, the programme will not have the same level of complexity. For example, if the message comes from the executives, the objective will be to teach non-technical ideas, for example *how to have a good digital hygiene?* Because executives have less understanding of how the production environment works than team leaders, their messages should not be about technical topics. This is the role of the team leaders to translate the non-technical messages into technical messages that are relevant to what their team are facing. For example, the team leader could transform the previous non-technical message into *How to safely use the shared mailbox ?* If executives try to impose technical topics or if team-leaders try to convey non-technical messages, this will lead to a meddling and a SETA programme poorly carried.

Next we must understand how we want to communicate. There are two forms of communication that the SETA programme should take [30][35]:

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

Both are equally important; people will not be satisfied if the only reason given to improve security is "just do it" and they can't do anything if they don't know how. A good programme is a combination of active formation and persuasive communication [30] There are five themes to promulgate security awareness campaign [19].

- *Deterrence messages* match sanction to a bad action. It supposes that people are rational and they will choose the best option for them, which will not be the one with the sanction hopefully. Empirical evidence that SETA programmes are suited for deterrence messages are found in [9]. This finding is confirmed by the literature review [1]. Deterrence messages can also be seen in the literature as fear messages. Fear is one of the most uses them in industry. As an example, the ANSSI, French information systems security organisation, asked for information systems security managers to stop being scary [15].
- *Morality messages* try to evoke our own morality principles to avoid bad decision. Empirical evidence that moral reasoning has an impact on security behaviour is found in [26]. The authors also say that proper punishment activities are important for moral reasoning to be efficient. Punishment activities can, obviously, not be done during a SETA programme.
- *Regret messages* supposed that people can anticipate the emotional consequences or their choices before making a decision. That anticipation will influence people to do the correct choice. Empirical evidence of the positive effect of regret on security behaviour is found in [8] but is not distinguished from deterrence or moral. Regret is theoretically a lever to influence behaviour but no significant evidence is found in [38].
- *Incentive messages* suppose that giving rewards for doing the right thing helps people improve. This can be viewed 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 actual compliance [28]. A survey also concludes that rewards do not directly influence security behaviour [1]. However [2] find theoretical evidence of positive effects on security behaviour and [8] find empirical evidence that incentive has a positive effect. Financial rewards also have a positive effect on security behaviour according to [12].
- *Feedback messages* suppose that people will change their behaviour if they receive feedback about their actions, it can be positive or negative reinforcement. In [34], West explains that classic feedback mechanisms do not work in information systems security; the consequence of a bad action is often delayed, and the best that can happen is nothing. This makes reinforcement learning not efficient.

Each of those themes has specific effects and limits. They are not well documented in the current state of the art of prevention in information systems security.

Finally, a SETA programme should be fit to the audience. Sadly, there is not much work done to study the relationship between types of public and other factors of a SETA programme. The relationship between types of audiences and themes in information systems security awareness make no exception. One paper finds it might be a correlation between personality trait and the effectiveness of a theme [19]. The most relevant advice found concerning the public is to split the population by groups of interest. This

fact is found multiple times in the literature, regardless of the study publication date. [6][32][35].

3 Do the SETA program

There are many media to convey a SETA programme and choosing the right one is an important decision. The choice of media is dependent of multiple factors:

- *The population that we are aiming for:* as said in the previous part, there is little literature about crafting 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. [35] list the medias possible regarding the question they answer.
- *The price:* [35] details which media are cheap and which ones are expensive.

As stated in the previous part, we should use media that allow us to answer the how (active formation) and the why (persuasive communication) questions. There are other factors that could be taken in consideration but they are not as important as the previous ones: (i) Is the media suited for multi-messages? (ii) will the media allow self-dissemination of your message? You can find those secondary characteristics by media in [35].

Catch The Flag (an event where security enthusiasts have to find the more "flags" possible. The "flags" are secrets hidden in purposefully-vulnerable softwares, hardwares or websites) and other types of competitions used for information systems security training are not suited media for a SETA programme. Those exercises ([13] provide a list of examples) aim to improve specific information systems security skills which is not the goal of a SETA progamme. Our goal is to make users adopt a safer behaviour.

It is well known that gamification helps to learn and remember. In consequences, the programme should be as gamify as possible. Our programme will be more attractive and the public touched by our message will be broader. In addition, people will remember the message more easily.

At this point we may have selected multiple media for our programme. If we have the choice between multiple media and we can't use them all in our campaign, we should emphasise the media that match the best our needs considering those four features [35]:

- *Ease of use:* How easy the SETA programme is to access, deploy, update and maintain?
- *Scalability:* Can the material be used for various audiences sizes and in various locations?
- *Support:* Will the support of the programme be internal or external ? How easy it is to find help to use the material?
- *Accountability:* What are the statistics that can be used to measure the effectiveness of the programme ? How complete are the measures?

Finally, we will have to focus on the governance part. In order to impact production the less possible, we should communicate the plan to all stakeholders [1][35]. That means the people we are training but also their immediate superior and other people

they are working with which do not attend to the programme. During the session, the trainees will not be able to maintain production; everyone working with them should be prepared in consequences. In addtion the SETA programme should be organised in short sessions [32]. Offering social interactions during a session increase the efficiency of the SETA programme [1][20][31]. The direct implication of this is that e-learning and other MOOCS are not relevant. At the end of the programme, giving goodies and giveaway is a good way to spread our message and reinforce engagement [32]. When we are doing the programme, the most important thing is the voluntariness of the public [20]. In his literature review about the place of human in information systems security, Dhillon et al. [10] mention that user empowerment is a strong leverage to increase security awareness.

4 Check the SETA program

Checking for our progamme is an important part to continuously improve the SETA programme. To evaluate our programme we will need to gather data. They can be feedback, questioners or some notes taken during the session. We can distinguish three types of evaluation:

- *Measure of behavioural intention:* This is the most represented type of evaluation in the literature. It posits that user intention can be estimated thanks to many other measures, and that user intention is dependent of the real behaviour of the user. For example, if we are doing a campaign to promote password managers, the higher the user intention to use them, the more successful the campaign is.
- *Knowledge oriented:* People with less understanding of security concepts are more likely to be victims of an attack. Therefore, evaluating the knowledge acquired after the SETA programme can be an indicator of how effective the programme is.
- *Ulterior incident rate:* This method consists in measuring the incident rate ulterior to the campaign. For example, if we are doing a campaign against bad password management and the rate of incidents linked to bad password management decrease after the campaign, we can consider that the campaign is successful.

Table 1. References of evaluation methods

Evaluation method	References
Measure of behavioural intention	[14][18][23]* [29]
Knowledge test	[11][21][22]
Ulterior incident rate	[35]

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

Among those three solutions, we can see that measuring the behavioural intention is the dominant method in the current literature. Inference of behavioural intention is about correlate factors to intention, therefore those tools should be used with prudence.

Khan et al. [20] identify that information systems security awareness is late compared to other domains like ecology awareness or public health awareness. They propose to mimic technic from other domains to improve information systems security awareness. For example, in public health, a model of reference is the EPPM (Extended Parallel Process Model) [36][37]. This model works well with messages based on fear (deterrence messages), which are effective for SETA programmes. A model like this could be useful in information security awareness. This model also has the advantage to explain why some campaigns can backfire.

Whatever the solution we choose to evaluate our programme, we should think about automating the evaluation [35][21]. Some SETA programmes can be huge; the operation of gathering data and then interpret them can be time costly.

5 Adjust the SETA program

The final step, adjusting, is the most import part to continuously improve our programme. To do so, the adjustment process can be divided in three steps:

1. Make a retrospective of the campaign and see if we have avoid common traps. Awareness campaigns often fail for the same reasons according to [3].
2. By collecting feedback we should have a better comprehension of the public needs. We should adapt the environment to the new needs highlighted during the programme. As said in section 2, prevention is here to mitigate risks that can't be avoided. With the feedback collected, it is an occasion to avoid new risks.
3. Finally, is the campaign 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. In addition, feedback collected can help to improve the way the SETA programme is done. [27] provides guidelines to make information systems security more user-friendly. Those guidelines are relevant for a SETA programme and can be used to improve it.

Once we have our improved programme, we should consider starting a new campaign, starting by planning for it. These cycle is the single-loop learning of the prevention paradigm described in [5]. Because we are considering SETA programme as continuous process, a new campaign should be start regularly.

6 Conclusion

Security awareness is a major concern. Despite so, there is very little work done to understand which types of messages are most effective for which types of people, and which media is best for which types of messages. Deterrence theme is dominant in security awareness, probably because of the relationship between information systems security and criminology.

Another problem of current security awareness is the lack of datasets. Many models have been compared to find which one explains better the behaviour of the studied

population but none of them were compared with the same dataset. In consequences, it is hard to conclude that a model is better or worse than any other.

SETA programmes are useful tools to improve security awareness. They should be considered as a part of a global security culture, encompassing prevention and response paradigme. However, there is a lack of methodology on how to make 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 to design a SETA programme following a PDCA cycle. Applying PDCA to SETA programmes allows us to give prescriptive guidelines and to continuously improve the programme design.

References

1. Abraham, S.: Information Security Behavior: Factors and Research Directions. In: AMCIS. vol. Proceedings - All Submissions, p. 462. (2011), https://aisel.aisnet.org/amcis2011$_submissions$/462
2. August, T., Tunca, T.I.: Network Software Security and User Incentives. Management Science **52**(11), 1703–1720 (2006), https://www.jstor.org/stable/20110643
3. Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? arXiv:1901.02672 [cs] (Jan 2019), http://arxiv.org/abs/1901.02672, arXiv: 1901.02672
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, www.igi-global.com/chapter/information-resources-management/54471
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, http://www.sciencedirect.com/science/article/pii/S0378720613001171
6. Bauer, S., Bernroider, E.W.N., Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security **68**, 145–159 (Jul 2017). https://doi.org/10.1016/j.cose.2017.04.009, http://www.sciencedirect.com/science/article/pii/S0167404817300871
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, 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, https://www.jstor.org/stable/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, https://doi.org/10.1287/isre.1070.0160
10. 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, https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2575.2001.00099.x
11. 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$_8$
12. Goel, S., Williams, K.J., Huang, J., Warkentin, M.: Can Financial Incentives Help with the Struggle for Security Policy Compliance? Information & management pp. 103447– (2021). https://doi.org/10.1016/j.im.2021.103447
13. Hoffman, L.J., Rosenberg, T., Dodge, R., Ragsdale, D.: Exploring a national cybersecurity exercise for universities. IEEE Security Privacy **3**(5), 27–33 (Sep 2005). https://doi.org/10.1109/MSP.2005.120
14. 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, http://www.sciencedirect.com/science/article/pii/S1071581911001029
15. Informatique, L.M.: L'anssi demande aux rssi de ne plus faire peur (2016), https://www.lemondeinformatique.fr/actualites/lire-assises-de-la-securite-2019-l-anssi-demande-aux-rssi-de-ne-plus-faire-peur-76715.html
16. ISACA: Cobit framework (2019), https://www.isaca.org/resources/cobit
17. ISO: Iso 27000 framework (2018), https://www.iso.org/standard/73906.html
18. 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, https://www.jstor.org/stable/25750691
19. 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, http://www.sciencedirect.com/science/article/pii/S0167404814000327
20. 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$_1$
21. 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, http://www.sciencedirect.com/science/article/pii/S0167404806000563
22. 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, https://doi.org/10.1108/09685221011095236
23. 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, https://doi.org/10.1108/MRR-04-2013-0085
24. Lee, M.G.: Securing the human to protect the system: human factors in cyber security. pp. 4A1–. Stevenage, UK (2012). https://doi.org/10.1049/cp.2012.1519
25. Legifrance2016: Article l4121-2 (Aug 2016), https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072050/LEGISCTA000006160774/
26. 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, https://doi.org/10.1057/ejis.2009.10
27. Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: Past and present. In: 2011 Third International Workshop on Cyberspace Safety and Security (CSS). pp. 21–26 (Sep 2011). https://doi.org/10.1109/CSS.2011.6058566

28. 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
29. 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, http://www.sciencedirect.com/science/article/pii/S0167404815000036
30. 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, https://doi.org/10.1108/09685220010371394
31. 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, http://www.sciencedirect.com/science/article/pii/S0167404804000331
32. 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, https://doi.org/10.1108/09685229810227649
33. 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, https://doi.org/10.1080/19393550802492487
34. West, R.: The psychology of security. Commun ACM pp. 34–40 (2008)
35. 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, https://csrc.nist.gov/publications/detail/sp/800-50/final
36. 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
37. 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, https://doi.org/10.1080/108107396127988
38. 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, https://www.sciencedirect.com/science/article/pii/S1071581905000327