Applying PDCA to Security, Education, Training and Awareness Programs

Olivier de Casanove, Nicolas Leleu, Florence Sèdes

Applying PDCA to Security, Education, Training and Awareness Programs

Olivier de Casanove[1], Nicolas Leleu[1] and Florence Sèdes[1],

[1] Institut de Recherche en Informatique de Toulouse – IRIT, Université Toulouse III – Paul-sabatier 118 route de Narbonne, 31062 CEDEX 9 Toulouse France
{olivier.decasanove, florence.sedes}@irit.fr Nicolas.leleu@ut-capitole.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 programs (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 program following a PDCA (Plan Do Check Act) cycle.

Keywords: PDCA, Information Systems Security, Awareness, SETA, Guidelines.

1 Introduction

Defining security awareness and more specifically its goals is a challenging task. This leads to a diversity of approaches and Tsohou et al. [1] conclude their paper saying that it 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 [2] "Accountability must be derived from a fully informed, well-trained and aware workforce." To promote a security culture, we can use security, education, training and awareness programs (SETA programs). “SETA programs aim to provide employees with the knowledge and motivation necessary to comply with security policies when confronted with a security risk” [3]. Some information system security standards define objectives for promoting a security culture and for raising awareness. Two of the most famous standards addressing this concern are the ISO/IEC 27000 family [4] and the NIST Cybersecurity Framework [5]. Unfortunately, information system security standards are very descriptive [6]. They set goals to reach, but rarely provide process or methodology on how to reach them; there is a need for guidelines. We propose to apply the Plan Do Check Act (PDCA) method to SETA programs to fulfil this need.

Plan Do Check Act

The Deming wheel (figure 1), also called continuous improvement wheel is a concept that illustrates the PDCA principle. It was made popular by William Edwards Deming. It aims to improve and optimise the gains and reduce the losses of products, processes or services. In the PDCA technique, the slope represents process improvement, the turning wheel continuously cycles Plan Do Check Act and thus climbs the hill, increasingly optimising the product, process or service with the aim of achieving the desired objective. Deming's representation also contains a wedge, it represents the quality system resulting from the previous improvement processes, the experience acquired which prevent the processes from going back. It must imperatively follow the upward movement of the wheel to avoid stagnating or even regressing. In other words, beyond the visual metaphor, it is necessary each time to improve the way of proceeding by avoiding repeating the errors of the past. We believe this tool can help design better SETA programs. With PDCA, we can limit the risk of failure, avoid repeating the same mistakes and provide guidelines.

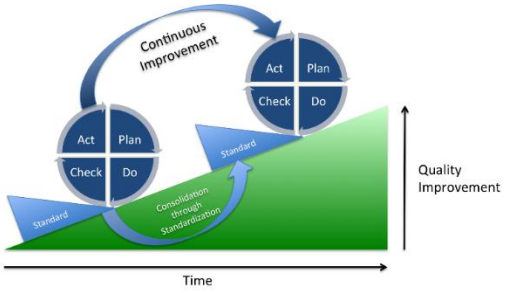

Fig. 1. Deming's Wheel illustration

In this paper, we will extract guidelines from the literature to promote a security culture and raise awareness thanks to SETA programs. We do not seek to provide an exhaustive literature review but rather a useful compilation of SETA practices. These guidelines are presented in four sections, each section corresponds to a step in the PDCA cycle. Then, we discuss the future of SETA programs and security awareness. Finally, we conclude.

2 Plan the SETA Program

A SETA program 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 [7]. To adopt a new culture, it is advised to generate an intrinsic motivation [8]. In other words, SETA programs should increase empowerment, which is a strong lever to increase security awareness [9]. A SETA program designed to generate intrinsic motivation is more likely to be successful over a long period of time. To design such a program, 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. Making the right choice decrease the risk of failing the SETA program.

2.1 The Source

First, we need to understand who is the source of the message [7]. Depending on its hierarchical level, the program will not have the same degree of complexity. For instance, 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 program should adopt [8] [2]:

- **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 competences.

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 program is a combination of active training and persuasive communication [8].

There are five themes to conduct a security awareness campaign [10]: 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 programs are suitable for deterrence messages can be found in [11]. This finding is confirmed by the literature review [12]. Lowry et al. [13] advise staying careful when using this theme, as deterrence messages create reactance and can “result in unintended negative consequences” [13].
- **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 [14]. 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 program.
- **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 [15] but is not distinguished from deterrence or morality. No significant evidence is found in [16].

- **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 [17] or with compliance [18]. A survey also concludes that rewards do not directly influence security behaviour [12]. However, [19] finds theoretical evidence of positive effects on security behaviour and [15] finds empirical evidence that the incentive has a positive effect. Financial rewards also have a positive effect on security behaviour according to [20].
- **Feedback messages** assume that people will change their behaviour if they receive feedback on their actions, this can be positive or negative reinforcement. In [21], 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 [22], 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 program and choosing the right one is an important decision.

The choice of media depends on multiple factors, seven have been identified in [2]:

- **The population we are targeting:** we will not use the same media if the targeted audience is computer literate or if it is not, for example.
- **The why or the how:** some media are more suited for persuasive communication, and others for active participation. [2] lists the possible media according to the question they answer. [23] 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:** [2] details which media are cheap and which are expensive.
- **Ease of use:** How easy is it to access, deploy, update and maintain the SETA program?
- **Scalability:** Can the material be used for different sized audiences and in different locations?
- **Support:** Will support for the program 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 program? How comprehensive are these measures?

As mentioned in the previous subsection 2.2, 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 program 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 program. However, one paper finds that there might be a correlation between personality traits and the effectiveness of a theme [10]. 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 [24] [25] [2].

Summary

To plan a SETA program 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. If these attributes are identified, we decrease the risk of failing the campaign.

3 Do the SETA Program

During the Do step, we apply the choices made in the previous step and we conduct the SETA program. When we carry out the program, the most important thing is the public's willingness to participate [27]. Security gamification is a tool "to strengthen employees' motivations to encourage learning, efficacy, and increased employee compliance with organisational security initiatives" [3]; we can therefore use it to design a successful SETA program. Guidelines on how to properly implement gamification are provided [3]. Yet, as shown by [32] and [33], gamification in the context of security awareness does not always hit. Providing social interactions during a session increases the effectiveness of the SETA program and triggers positive changes in security behaviour [12] [26] [27] [28] [7]. This argument seems to demonstrate that e-learning is not appropriate since there are no interactions. On the other hand, Kävrestad et al. [29] [30] show that e-learning could be effective if "information [is] presented in short sequences to the learner. It should also include a practical element and be of direct relevance to the user's intention." [31] Organised SETA programs in short sessions is a good practice, even if we are not doing e-learning [25]. At the end of the program, giving gifts is a good way to spread our message and reinforce the commitment [25].

If the SETA program happens in a company or in an industrial context, the session needs to have as little impact as possible on production; therefore we should communicate the plan to all stakeholders [12] [2]. This means the people we are training, but also their immediate superiors and other people they work with who are not involved in the program. During the session, the trainees will not be able to maintain production; everyone working with them must be prepared for the consequences.

Summary

A program is more likely to succeed if it offers human interaction. If the program happens in a company, attendees' coworkers should be warned that attendees will not be available to maintain production.

4 Check the SETA Program

In the check step, we should verify whether we have processes to monitor the effectiveness and efficiency of the SETA program. To evaluate our program, we 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, knowledge oriented and ulterior incident rate. A non-exhaustive list of papers related to each category can be found in table 1.

- **Measure of behavioural intention:** 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:** This evaluation method posits that 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 program can be an indicator of the effectiveness of the program.
- **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.

EVALUATION METHODS	**REFERENCES**
Measure of behavioural intention	[34] [35] [36]* [37]
Knowledge test	[22] [38] [39] [40] [41]
Ulterior incident rate	[2]

Table 1. Evaluation methods (* is a review)

Regardless of the solution we choose for evaluating our program, we need to think about automating the evaluation [2] [39]. Some SETA programs 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.

Summary.

We establish a process to evaluate our program. As the SETA program 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 program.

5 Adjust the SETA program

During the Act phase (also known as Adjust phase), we establish a process to ensure we perform a review on a periodic basis to confirm the continuing applicability, adequacy, effectiveness and efficiency of the SETA programs. In the first place, we take in consideration the data collected in the previous section to improve our program. Then, we 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 need to update them or add new ones. Once we have our new program, we should consider launching a new campaign. This cycle is the single-loop learning of the prevention paradigm described in [42]. Since we are considering SETA program 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 program 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 and Perspectives

SETA programs are an important aspect of security. It differs from other aspects of security by putting the user back at the centre of the information system. This is associated with the field of "Human-Centred Security and Privacy" (HCSP), see [43] for a brief overview of this field.

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 program. We used the PDCA cycle because it is a widely used tool in the industry, but other continuous improvement tools should be studied, or created if needed, to better suit the needs of information system security. We seek, in future works, to develop a PDCA-based method for the implementation of organisational SETA work.

SETA programs have been researched extensively, but some aspects have been neglected. For example, how themes interact with other variables, like the target of a campaign, is not well studied in the literature. We want to extract other weaknesses in future works, thanks to techniques such as content analysis.

Khan et al. [27] 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) [44]. This model works well with messages fear-based (they are similar to deterrence-based messages), which are effective for SETA programs according to what we found in the literature (see subsection 2.2).

At the check step, we listed models allowing measuring the SETA campaign effectiveness (see table 1). The lack of common datasets makes it difficult to compare them together and to conclude if one is better than another. In addition, there is a need for reproducibility since the datasets are not public.

7 Conclusion

Security awareness is a major concern in information system security. To promote awareness, we use SETA program. 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 SETA programs following a PDCA cycle. The PDCA cycle allows us to be prescriptive and not just descriptive as many current standards do. In addition, PDCA facilitates the continuous improvement of awareness campaigns which, as every security tool, should stay updated.

We believe this work can help information system security actors to design better prevention programs 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 programs to convey messages, leading to more efficient prevention campaign and more significant results.

References

1. A. Tsohou, S. Kokolakis, M. Karyda et E. Kiountouzis, «Investigating Information Security Awareness: Research and Practice Gaps,» Information Security Journal: A Global Perspective, vol. 17, p. 207–227, 12 2008.
2. M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program," 2003.
3. M. Silic et P. B. Lowry, «Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance,» Journal of Management Information Systems, vol. 37, p. 129–161, 1 2020.
4. ISO, ISO 27000 framework, 2018.
5. K. M. Stine, K. Quill and G. A. Witte, "Framework for Improving Critical Infrastructure Cybersecurity," 2 2014.
6. Y. Barlette and V. V. Fomin, "The Adoption of Information Security Management Standards: A Literature Review," IGI Global, 2010, p. 69–90.
7. R. von Solms and B. von Solms, "From policies to culture," Computers & Security, vol. 23, p. 275–279, 6 2004.

8. M. T. Siponen, «A conceptual foundation for organizational information security awareness,» Information Management & Computer Security, vol. 8, p. 31–41, 1 2000.
9. G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," Information Systems Journal, vol. 11, p. 127–153, 2001.
10. M. Kajzer, J. D'Arcy, C. R. Crowell, A. Striegel and D. Van Bruggen, "An exploratory investigation of message-person congruence in information security awareness campaigns," Computers & Security, vol. 43, p. 64–76, 6 2014.
11. J. D'Arcy, A. Hovav et D. Galletta, «User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,» Information Systems Research, vol. 20, p. 79–98, 3 2009.
12. S. Abraham, «Information Security Behavior: Factors and Research Directions.,» chez AMCIS - 2011 Proceedings - All Submissions, 2011.
13. P. B. Lowry and G. D. Moody, "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies," Information Systems Journal, vol. 25, p. 433–463, 2015.
14. L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen et A. Vance, «What levels of moral reasoning and values explain adherence to information security rules? An empirical study,» European Journal of Information Systems, vol. 18, p. 126–139, 4 2009.
15. B. Bulgurcu, H. Cavusoglu et I. Benbasat, «Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,» MIS Quarterly, vol. 34, p. 523–548, 2010.
16. C. Wright and P. Ayton, "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, vol. 62, p. 759–783, 6 2005.
17. S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss, "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," European Journal of Information Systems, vol. 18, p. 151–164, 4 2009.
18. S. Pahnila, M. Siponen and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," 2007.
19. T. August et T. I. Tunca, «Network Software Security and User Incentives,» Management Science, vol. 52, p. 1703–1720, 2006.
20. S. Goel, K. J. Williams, J. Huang et M. Warkentin, «Can financial incentives help with the struggle for security policy compliance?,» Information & Management, vol. 58, p. 103447, 2021.
21. R. West, «The Psychology of Security,» Commun. ACM, vol. 51, p. 34–40, 4 2008.
22. P. Mayer, A. Kunz et M. Volkamer, «Motivating Users to Consider Recommendations on Password Management Strategies.,» chez HAISA 2018, 2018.
23. Y. Albayram, J. Liu et S. Cangonj, «Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager,» chez European Symposium on Usable Security 2021, New York, NY, USA, Association for Computing Machinery, 2021, p. 89–104.
24. S. Bauer, E. W. N. Bernroider and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," Computers & Security, vol. 68, p. 145–159, 7 2017.
25. M. E. Thomson et R. von Solms, «Information security awareness: educating your users effectively,» Information Management & Computer Security, vol. 6, p. 167–173, 1 1998.
26. S. Das, L. A. Dabbish and J. I. Hong, "A Typology of Perceived Triggers for End-User Security and Privacy Behaviors," 2019.

27. B. Khan, K. S. Alghathbar and M. K. Khan, "Information Security Awareness Campaign: An Alternate Approach," in Information Security and Assurance, Berlin, 2011.
28. S. Das, T. H.-J. Kim, L. A. Dabbish et J. I. Hong, «The Effect of Social Influence on Security Sensitivity,» chez 10th Symposium On Usable Privacy and Security (SOUPS 2014), Menlo, 2014.
29. J. Kävrestad, M. Skärgård and M. Nohlberg, "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, 2019.
30. J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos and S. Furnell, "Evaluation of Contextual and Game-Based Training for Phishing Detection," Future Internet, vol. 14, p. 104, 4 2022.
31. J. Kävrestad and M. Nohlberg, "ContextBased MicroTraining: A Framework for Information Security Training," in Human Aspects of Information Security and Assurance, Cham, 2020.
32. J. Ophoff and F. Dietz, "Using Gamification to Improve Information Security Behavior: A Password Strength Experiment," in Information Security Education. Education in Proactive Information Security, Cham, 2019.
33. R. J. Baxter, K. Holderness and D. A. Wood, "Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field," Rochester, 2015.
34. D.-L. Huang, P.-L. Patrick Rau, G. Salvendy, F. Gao and J. Zhou, "Factors affecting perception of information security and their impacts on IT adoption and security practices," International Journal of Human-Computer Studies, vol. 69, p. 870–883, 12 2011.
35. A. C. Johnston et M. Warkentin, «Fear Appeals and Information Security Behaviors: An Empirical Study,» MIS Quarterly, vol. 34, p. 549–566, 2010.
36. B. Lebek, J. Uffen, M. Neumann, B. Hohler et M. H. Breitner, «Information security awareness and behavior: a theory-based literature review,» Management Research Review, vol. 37, p. 1049–1092, 1 2014.
37. J. Shropshire, M. Warkentin and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," Computers & Security, vol. 49, p. 177–191, 3 2015.
38. L. Drevin, H. Kruger, A.-M. Bell and T. Steyn, "A Linguistic Approach to Information Security Awareness Education in a Healthcare Environment," in Information Security Education for a Global Digital Society, Cham, 2017.
39. H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," Computers & Security, vol. 25, p. 289–296, 6 2006.
40. H. Kruger, L. Drevin et T. Steyn, «A vocabulary test to assess information security awareness,» Information Management & Computer Security, vol. 18, p. 316–327, 1 2010.
41. P. Mayer, C. Schwartz et M. Volkamer, «On the systematic development and evaluation of password security awareness-raising materials,» chez Proceedings of the 34th Annual Computer Security Applications Conference, 2018.
42. R. Baskerville, P. Spagnoletti and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," Information & Management, vol. 51, p. 138–151, 1 2014.
43. K. Renaud and S. Flowerday, "Contemplating human-centred security & privacy research: Suggesting future directions," Journal of Information Security and Applications, vol. 34, p. 76–81, 6 2017.
44. K. Witte, «Putting the fear back into fear appeals: The extended parallel process model,» Communication Monographs, vol. 59, p. 329–349, 1992.