



## Security Education, Training, and Awareness Programs: Literature Review

Siqi Hu, Carol Hsu & Zhongyun Zhou

**To cite this article:** Siqi Hu, Carol Hsu & Zhongyun Zhou (2022) Security Education, Training, and Awareness Programs: Literature Review, Journal of Computer Information Systems, 62:4, 752-764, DOI: [10.1080/08874417.2021.1913671](https://doi.org/10.1080/08874417.2021.1913671)

**To link to this article:** <https://doi.org/10.1080/08874417.2021.1913671>



Published online: 05 May 2021.



Submit your article to this journal [↗](#)



Article views: 2307



View related articles [↗](#)





View Crossmark data [↗](#)



Citing articles: 4 View citing articles [↗](#)



# Security Education, Training, and Awareness Programs: Literature Review

Siqi Hu, Carol Hsu , and Zhongyun Zhou 

Tongji University, Shanghai, China

## ABSTRACT

Security education, training, and awareness (SETA) is one of the most common and prominent strategies for organizational security governance. However, only a small portion of practitioners claimed that their SETA programs were “very effective”. A possible reason for this is the lack of a systematic understanding of the nature of SETA programs, the paths through which SETA impacts employees’ security-related beliefs or behavioral intentions, and the conditions that might influence such a relationship. This study argues that a comprehensive literature review regarding SETA is vital for holistically investigating the findings of previous SETA research and unveiling the characteristics and factors that influence the effectiveness of SETA. A total of 80 articles, published between 1998 and 2020, were included to conduct an in-depth systematic review on SETA.

## KEYWORDS

SETA; security education; training; awareness; organizational security

## 1. Introduction

Security education, training, and awareness (SETA) programs are ongoing efforts to focus employees’ attention on information security-related issues, provide employees with crucial knowledge and skills, enable their deep understanding of why security protection is needed, and increase their awareness of security issues.<sup>1–3</sup> SETA is one of the most common, fundamental, and prominent strategies for organizational security governance<sup>4</sup> and is becoming a strategic priority within many organizations.<sup>2,5,6</sup> For instance, the United States (US) Computer Security Act of 1987 requires that “each agency shall provide the mandatory periodic training in computer security awareness and accepted computer practices for all employees”.<sup>7(p6)</sup>

According to the US National Institute of Standards and Technology (NIST), “failure to give attention to the area of security training puts an enterprise at great risk because the security of agency resource is as much a human issue as it is a technology issue”.<sup>8</sup> This assertion was also supported by the scholarly findings indicating that many security breaches and information security policy violations within organizations occur because employees do not fully understand the importance of information security, which is strongly related to the lack of and/or inadequate levels of SETA in organizations.<sup>9</sup> In other words, a robust SETA program is the key to ensuring that employees have a sufficient understanding of security-related issues and the security countermeasures that could be used to deal with security risks.<sup>8,10</sup>

Most academics and practitioners have agreed on the need for organizations to implement SETA.<sup>2,5,6,11–13</sup> However, only a small portion of practitioners claimed that their SETA programs were “very effective” in reducing security risks and changing employees’ security-related behaviors.<sup>14,15</sup> In practice, many SETA programs are relatively ineffective<sup>4</sup>; employees continually engage in unsafe computing practices.<sup>16</sup> A possible reason for this is organizations often take the “one-size-fits-all” SETA approach, which lacks a systematic understanding of the nature of SETA programs, the paths through which SETA impacts employees’ security-related beliefs or behavioral intentions, and the conditions that might influence such a relationship. In order to enhance our understanding of SETA and strengthen its practical development, we argue that a comprehensive literature review regarding SETA was vital for holistically investigating the findings of previous SETA research and unveiling the characteristics and factors that influence the effectiveness of SETA. Thus, the key objectives of this review are to (1) understand the nature of SETA programs, (2) analyze factors that contribute to the effectiveness of SETA programs, and (3) unveil SETA programs’ influence on employees security-related intentions and behaviors.

The rest of this review is organized as follows: we first describe the review methods, then present an overview of the existing SETA literature. Finally, we discuss the results and propose directions for future research.

## 2. Methodology

### 2.1 Review scope

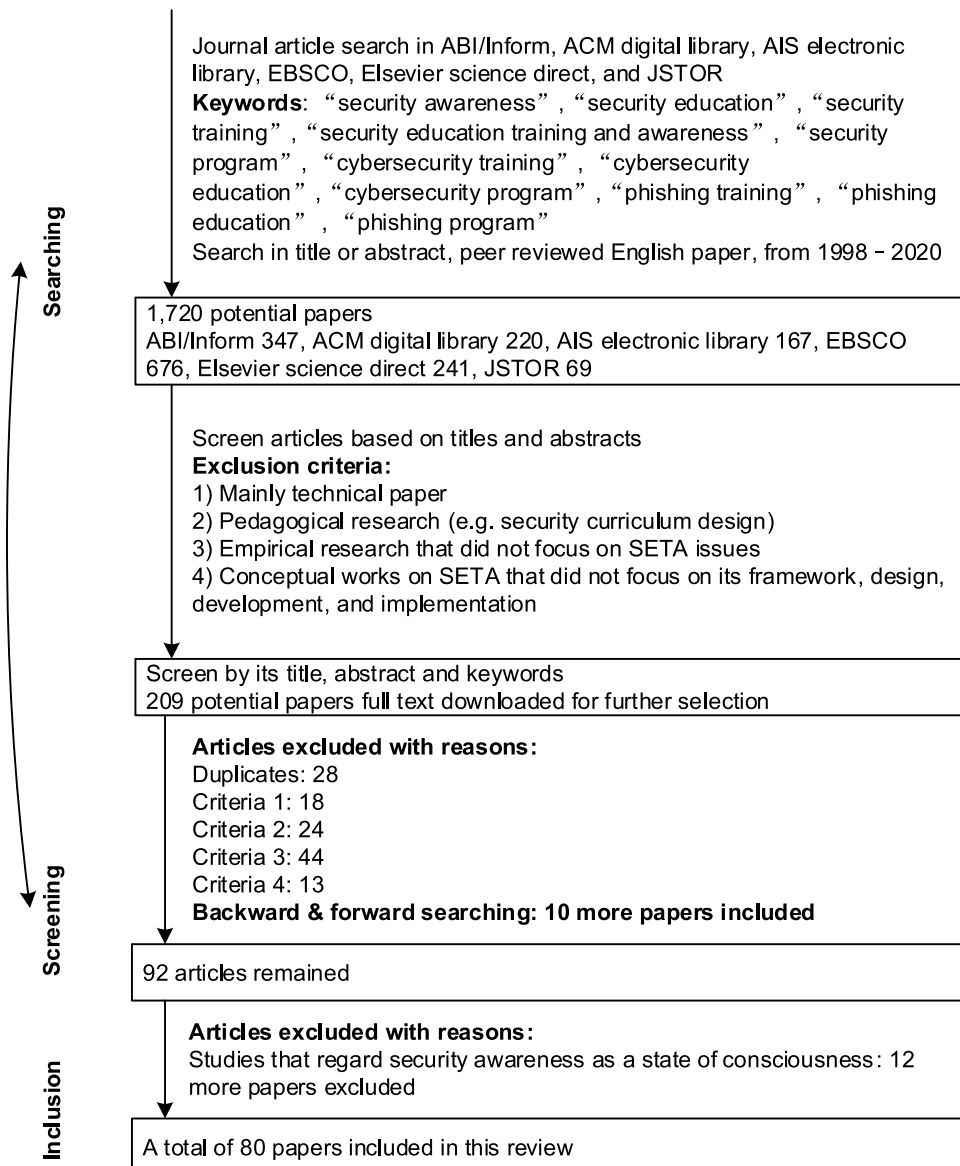
Since SETA consists of three parts (i.e., education, training, and awareness), we included research containing any of these elements. Our goal was to identify the essential elements that may affect SETA programs' success and contribute to its impact on employees' behavior. Thus, apart from empirical studies examining SETA programs' impact on employees, we also included articles that presented the SETA conceptual framework.

We excluded four types of articles from our review: (1) technical articles that focused mainly on different security training systems,<sup>3,17</sup> (2) pedagogical research that, for instance, developed a security curriculum for students,<sup>18</sup> (3) conceptual works on SETA that did not

provide information on its framework, design, development, and implementation (e.g., a needs analysis for SETA), and (4) empirical research that did not investigate the impact of SETA on employees' behavior.

### 2.2 Searching and screening process

Following Webster and Waston's guideline,<sup>19</sup> we conducted a thorough, systematic review of SETA-related literature. As illustrated in Figure 1, our literature review began with a search of the ACM, AIS, EBSCO, Elsevier, and JSTOR for journal and conference papers, using the terms shown in Figure 1. We searched for these terms in the titles or abstracts of peer-reviewed papers. We considered papers published since 1998, given that this is when organizations began to realize that humans were



**Figure 1.** The searching and screening process.

*Note:* We also searched the NIST research library and website for SETA-related handbooks, and four more handbooks were cited accordingly in our manuscript.

the “weakest link” in information security management and started valuing SETA’s importance.<sup>20</sup> We also searched on Google Scholar to account for papers from less well-known conferences.<sup>1</sup>

At this stage, a total of 1,720 potential SETA papers were identified. We first read the abstracts of these papers and screened them according to the inclusion and exclusion criteria. 209 potential papers were full-text downloaded for further selection. After the first stage of screening and backward- and forward-searching, a total of 92 papers remained.

However, during the review, we found that scholars provided two distinct definitions of security awareness. First, security awareness was referred to as a state of consciousness,<sup>21,22</sup> knowledge, and cognizance about security risks and countermeasures.<sup>23–27</sup> Second, security awareness was defined as the basic level of SETA programs and a tool to draw employees’ attention to security issues.<sup>28</sup> These two definitions were different. A few pieces of research even perceived SETA as the antecedent of the first kind of security awareness.<sup>29</sup> Hence, twelve more papers focusing on the first type of security awareness were thus excluded, resulting in 80 peer-reviewed papers for the literature analysis.

### 3. Literature analysis

#### 3.1 The nature of SETA programs

As mentioned earlier, SETA consists of three components, which are security education, security training, and security awareness.<sup>8,20,30</sup> To gain a deep understanding of SETA programs, we reviewed all the related papers that defined SETA or its three components and provided information on the nature of SETA programs. Table 1 provides the definitions of SETA, security education, security training, and security awareness in current literature.

Academics portrayed SETA as formal initiatives that aim to provide employees with cognizance of information security risks around the organization, the skills necessary for them to engage in daily work activities, and their important roles in information security protection.<sup>1,5,29,31–35,37,38</sup>

For security education, Jenkins and Durcikova<sup>16</sup> interpreted it as the portrayal of security information to employees, aiming to prompt constant security behavioral change. Hwang et al.<sup>39</sup> and Pérez-González et al.<sup>40</sup> contended that security education could take the form of programs or other efforts aiming to improve employees’ consciousness of security policies, guidelines, and surroundings in order to persuade them to behave securely using tailored materials. Researchers described security training as an instructional tool and communication tunnel to activate employees’ thinking processes, persuade them to act appropriately, and enable them to gain a better understanding of security policies and procedures.<sup>6,41</sup> For security awareness, Kruger and Kearney<sup>45</sup> pointed out that security awareness presentations communicate the importance of security and the potential consequences of security breaches to employees, prompting them to understand their responsibilities prescribed in security policies and behave accordingly. Scholars have also portrayed security awareness programs as instructional tools to foster employees’ security learning,<sup>48</sup> processes to enable employees’ understanding of the importance of security issues,<sup>42,44</sup> and continuous efforts to produce security behavioral changes.<sup>43,46</sup>

Our analysis indicated that it is difficult to clearly tell the difference between the definition of these terms. Most existing research did not distinguish the difference among the different types of SETA programs but used them interchangeably.<sup>50</sup> Only limited research mentioned that security awareness, security training, and security education are different types of programs with distinct meanings<sup>51</sup> and purposes, contributing to

**Table 1.** Definitions of SETA, security education, security training, and security awareness.

Concept	Definition	Reference
SETA	Ongoing efforts that promote employees’ consciousness of security issues and provide them with general security knowledge and skills to combat security threats and risks.	Alshaikh et al., <sup>31</sup> Burns et al., <sup>32</sup> Cram et al., <sup>1</sup> Dhillon et al., <sup>33</sup> Goode et al., <sup>34</sup> Haeussinger and Kranz, <sup>29</sup> Kim et al., <sup>35</sup> Lowry et al., <sup>36</sup> Posey et al., <sup>5</sup> Talib and Dhillon, <sup>37</sup> Yoo et al. <sup>38</sup>
Security education	Efforts that aim at improving employees’ consciousness of security policies, guidelines, and security surroundings to enhance employees’ security-related behavior.	Hwang et al., <sup>39</sup> Jenkins and Durcikova, <sup>16</sup> Pérez-González et al. <sup>40</sup>
Security training	Instructional tools and communication tunnels to activate employees’ thinking processes, persuade them to act appropriately, and enable them to gain a better understanding of security policies and procedures	Huang et al., <sup>41</sup> Puhakainen and Siponen <sup>6</sup>
Security awareness	Programs that aim to foster employees’ security learning and make employees conscious of the importance of information security protection, and continuous efforts to produce security behavioral changes.	AlMindeel and Martins, <sup>42</sup> Bauer et al., <sup>43</sup> Goo et al., <sup>44</sup> Kruger and Kearney, <sup>45</sup> Tsohou et al., <sup>46</sup> Wolf et al., <sup>47</sup> Wu et al., <sup>48</sup> El-Haddadeh et al. <sup>49</sup>

different phases of the security learning continuum and differing in their delivery methods and target audiences.<sup>8,20</sup> Table 2 differentiates security education, security training, and security awareness.

Normally, an awareness program simply aims to focus employees' attention on information security, often targeting the entire population within an organization. It is the basic level of SETA and is usually delivered through posters, banners, or bulletin boards with simple slogans.<sup>28</sup> While training endeavors to build employees' security knowledge and skills, enabling them to understand how protection can be achieved, and it can be delivered through formal training sessions or seminars.<sup>52</sup> An education program aims to integrate all security-related skills into a common body of security knowledge. It intends to provide employees with a deep understanding of why protection is necessary and give employees insights into information security. As the highest level of security learning, an education program usually targets security professionals and specialists and could be delivered by hand-on labs like cyberattack simulations.<sup>53</sup> SETA is a combination of these three aspects and can be defined as ongoing efforts to focus employees' attention on day-to-day security issues, provide them with general security knowledge and skills, and offer insights into why security protection is needed.<sup>1</sup> These findings are also consistent with the opinion of the NIST handbooks.<sup>8,20,30,54</sup>

As we mentioned above, existing research did not address the distinction of different types of SETA. We believe that understanding the differences in the definition, purpose, delivery method and target audience of various SETA programs would be of paramount importance to the success of such programs in the organization.

### 3.2 The design factor of SETA programs

Another group of scholars focused on design factors that contribute to the effectiveness of SETA programs. They provided a series of recommendations and offering guidance on it.

Adapting a program to meet organizations' or their employees' needs is the key to ensuring the effectiveness of SETA programs.<sup>55,56</sup> Researchers have suggested that SETA programs' topics should be decided according to the needs of the target audience,<sup>57</sup> the security policies of the organization,<sup>34</sup> or the knowledge level of the employees.<sup>12,58,59</sup> Using real-life examples, or encouraging employees provide the security issues they care about enables employees to feel the security program is personally related.<sup>60,61</sup> Scholars also mentioned that it may be better for organizations to segment their employees into small learning groups according to their level of knowledge of information security.<sup>15,53</sup> Heikka<sup>62</sup> empirically confirmed that learner-centered, contextually based, and group-oriented security training improved employees' security behavior. Bauer et al.<sup>43</sup> conducted case studies to explore how employees perceived different security program designs and proposed that organizations should differentiate their target audiences and customize security programs accordingly. If the topic is outdated or not tailored for the target audience, or the delivery approaches are inappropriate, SETA programs may be ineffective for organizations.<sup>61</sup>

The delivery method is another important aspect academics and practitioners consider in relation to the design of a SETA program. Our analysis shows that researchers have compared the effect of different delivery methods. For instance, Caputo et al.<sup>63</sup> conducted a text-based phishing training experiment, which was embedded in an e-mail, and found that it did not influence employees' security behavior. They explained that it might because text-based training could not attract trainees' attention, and the adoption of more interesting approaches, such as multimedia or game-based delivery methods may help. When Abawajy<sup>64</sup> examined employees' preferences over different delivery methods (e.g., text-based, game-based, and video-based), they concluded that game-based methods improved employees' threat identification ability more than others. And a great deal of research confirmed that the game-based or hands-on delivery methods improved the effectiveness of SETA programs.<sup>4,65–67</sup> However, some studies

**Table 2.** Differences between education, training, and awareness programs.

Types of program	Purpose	Delivery method	Target audience	Level of SETA
Education program	Enable employees with deep learning on security knowledge and skills, giving employees insights into why security protection is required.	Usually active and engaging mentoring, like cyberattack simulations.	Usually IT/security specialists and professionals.	Highest
Training program	Builds employees' security knowledge and skills, enabling employees to understand how security protection can be achieved.	Usually hands-on approaches, such as formal classes and seminars.	Usually all employees.	Intermediate
Awareness program	Draws employees' attention to security and explains to employees what security is.	Poster, banners, reminders, etc.	All employees.	Basic



also mentioned that too much information or extensive use of multimedia methods might backfire. Too much information could hinder employees' security learning processes and decrease their willingness to take security precautions.<sup>68,69</sup> Extremely rich media strained employees' cognitive load, making it difficult for them to acquire security knowledge and skills.<sup>70</sup> Academics also mentioned that collaborative learning techniques, such as cyber defense competitions<sup>71</sup> and other hands-on approaches,<sup>72–74</sup> contributed to SETA's effect on employees. In summary, rich media like game-based training programs can attract employees' interest and motivate them to learn security knowledge, but too much information or extremely rich media may be counterproductive. Organizations should identify the appropriate level of information or media richness that their employees can accept, perhaps by conducting a survey.

In addition to topic and delivery method, other factors such as senior management support,<sup>75,76</sup> communication approaches,<sup>43,77</sup> and the frequency of SETA programs<sup>5</sup> also have an impact on the programs' effectiveness. Senior managers' championship is critical for the success of SETA programs.<sup>15,43</sup> Hansche<sup>60,78</sup> detailed the process of designing, developing, and implementing of SETA program and concluded that senior management support was key to ensuring its success. Kim et al.<sup>35</sup> empirically proved that leaders' powerful support strengthens SETA's positive relationship with employees' security policy compliance intentions.

Scholars also emphasized the importance of communication and training employees frequently and in small sessions.<sup>13,43,79</sup> Puhakainen and Siponen<sup>6</sup> suggested that communication efforts and senior management support were the crucial factors for ensuring an effective training program. Barlow et al.<sup>80</sup> proved that anti-neutralization and informational communication approaches decreased employees' violation intentions. Posey et al.<sup>5</sup> highlighted that the lack of periodic SETA programs was the main reason why security plans did not work in organizations. Their empirical results showed that SETA programs'

frequency influenced employees' awareness of threats, their coping appraisal processes, and their protection motivation. Thomson and von Solms<sup>10</sup> mentioned that dividing a long training program into small sessions could produce more powerful changes than larger and longer sessions, and this was empirically proved by Albrechtsen and Hovden's work in 2010.<sup>81</sup>

Strong and persuasive messages emphasizing the benefits and relevance of training programs,<sup>82</sup> along with detailed and specific threat information,<sup>83</sup> have been proved to enhance employees' understanding of security threats and their learning of security countermeasures. Furthermore, cultural and employee differences should be considered when scholars explore SETA programs' impact on security.<sup>84</sup> Wiley et al.<sup>85</sup> verified that cultural factors also influenced employees' perception of information security.<sup>86</sup> Employee personality characteristics, such as conscientiousness and agreeableness, also explained the variance in employees' security awareness.<sup>87,88</sup> Table 3 summarizes the factors contributing to the success of a SETA program, most of which have been empirically verified.

### 3.3 SETA and Employees' security-related behavior

Given that organizations launch SETA programs to improve employees' security-related behavior,<sup>31</sup> we observed that another important SETA research stream is the empirical research examining its impact on employees' security-related behavior.<sup>62,81</sup> Existing security behavioral research on SETA can be divided into two main groups: (1) research examining the direct relationship between SETA and employees' security-related behavior and (2) research exploring the impact of SETA programs on employees through different conceptual foundations.

All the empirical research that examined the direct impact of SETA programs on employees' security behavior proved that it was significant regarding its positive effect on employees' compliance intentions,<sup>6,35</sup> their continuing compliance intentions,<sup>90</sup> their security performance,<sup>40</sup>

**Table 3.** Factors contributing to the success of SETA programs.

Factor	Reference
Senior manager support	Choi et al., <sup>75</sup> Dugan, <sup>77</sup> Hansche, <sup>60,78</sup> Puhakainen and Siponen <sup>6</sup>
Media richness of delivery methods	Bauer et al., <sup>43</sup> Caputo et al., <sup>63</sup> Dugan, <sup>77</sup> Jenkins et al., <sup>70</sup> Shaw et al., <sup>69</sup> Tshchakert and Ngamsuriyaroj <sup>89</sup>
Collaborative learning techniques	Albrechtsen and Hovden, <sup>81</sup> Conklin, <sup>71</sup> Heikka, <sup>62</sup> Karjalainen and Siponen <sup>12</sup>
Communication approach	Barlow et al., <sup>80</sup> Bauer et al., <sup>43</sup> Dugan, <sup>77</sup> Puhakainen and Siponen <sup>6</sup>
Using of persuasive messages	Adepeju-Joseph, <sup>82</sup> AIMindeel and Martins <sup>42</sup>
Duration	Albrechtsen and Hovden <sup>81</sup>
Detailed and specific information	McCrohan et al., <sup>83</sup> McCoy and Fowler, <sup>55</sup> Goode et al., <sup>34</sup> Johnson, <sup>58</sup> Karjalainen and Siponen, <sup>12</sup> Tse et al. <sup>59</sup>
Frequency	Posey et al. <sup>5</sup>
Cultural factors	Chen et al., <sup>86</sup> Wiley et al. <sup>85</sup>
Game-based approaches	Abawajy, <sup>64</sup> Silic and Lowry <sup>4</sup>
Hands-on approaches	Meso et al. <sup>74</sup>

and other security behavior,<sup>38,91,92</sup> or its negative effect on their computer misuse or abuse intentions.<sup>93</sup> The current study has no controversy regarding this issue.

For the second group of studies, researchers have utilized several different theories or conceptual constructs to explore the relationship between SETA and employees' security behavior, including attitudes, efficacy, and perceived sanctions from different theories to explain how to motivate employees' compliance behavior or why employees breach security policies.

A lot of researchers have used protection motivation theory as the conceptual foundation to explain employees' behavior. Protection motivation theory explains the cognitive processes that employees use when facing threats (e.g., threat and coping appraisal processes). Threat appraisal is employee's evaluation of the threats they are facing, including their probable exposure to a particular threat (resource vulnerability) and the potential consequences of a security threat (threat severity). Coping appraisal involves people's evaluation of their ability to take appropriate action (self-efficacy), the efficiency of a suggested strategy in mitigating a security threat (response-efficacy), and the cost of performing such a suggested strategy (response cost). In detail, Posey et al.<sup>5</sup> used SETA as an antecedent of protection motivation-related constructs, empirically proving that SETA programs improved employees' coping and threat appraisal processes, thus motivating employees' protection intentions. Hina et al.<sup>94</sup> confirmed that SETA programs were positively associated with employees' perceptions of the severity of security threats, resource vulnerability, response cost, self-efficacy, and response efficacy, which had a positive impact on their security policy compliance intentions. Other studies verified SETA programs' positive influence on response cost,<sup>95</sup> self-efficacy,<sup>16,32,33,37,38,41,74</sup> and response efficacy.<sup>32,95</sup>

Another group of researchers resorted to deterrence theory to explain SETA programs' impact on employees. Deterrence theory predicts that employees' security breaches could be deterred by sanctions and punishments. SETA programs can convince employees that an organization is serious about information security and that anyone who violates the security policies will be punished. D'Arcy et al.<sup>2</sup> conducted a scenario-based survey to explore the relationship between SETA programs, the perceived certainty and severity of sanctions, and misuse intentions. They revealed that SETA efforts could deter security policy violations by providing information on the possible sanctions and punishment for those who violated security policies, stressing the certainty and severity of punishment for any breach behaviors. Herath et al.<sup>96</sup> claimed that SETA programs made

employees realize that the company was rigorous in ensuring information security, thus decreasing employees' immoral engagement and violation intentions.

Scholars also adopted a rational perspective (perceived benefits and cost) to illustrate employees' choices over different alternatives regarding information security, utilizing SETA as antecedents of these constructs.<sup>97</sup> In addition, Lowry et al.<sup>36</sup> use fairness theory to explain SETA programs' impact on employees' compliance intentions. SETA programs could also decrease employees' moral disengagement,<sup>96</sup> develop their sense of responsibility and accountability toward security issues,<sup>98</sup> increase their psychological empowerment,<sup>33</sup> improve their positive attitudes and perceived behavioral control regarding security issues,<sup>16</sup> and nurture a good security climate,<sup>44</sup> which is positively associated with employees' intentions to comply with security policies, and detailed information is provided in [Figure 2](#).

These findings paved the foundation for our understanding of how SETA affects employees' security-related intentions and proved that SETA was positively associated with employees' compliance intentions and behavior. Nevertheless, some issues should be further clarified. SETA is not an isolated single construct, and many factors can interfere with its impact on employees. SETA is an approach to facilitating employees' learning on security knowledge and skills, and this learning process can be influenced by the approaches used to deliver SETA, the communication approaches, and top managers' beliefs toward it.

Moreover, our assessment of the prior literature indicates that while most conceptual studies have acknowledged the importance of tailored SETA program for the specific type or category of employees,<sup>12,34,55,58,59</sup> this issue was rarely theorized and empirically investigated (details are presented in [Appendix A](#)). The majority of empirical studies have taken up an approach to studying the implementation and effectiveness of SETA applicable to all levels of employees in the organization.

#### 4. Discussion and research agenda

SETA programs are an important and fundamental strategy to mitigate security risks in organizations. In the previous sections, we reviewed the extant literature to explain the nature of SETA, its design and implementation, and its impact on employees' security-related behaviors. In doing so, we uncovered several issues that should be considered by future research focusing on SETA.

First, we propose that more effort and attention should be invested in developing more specific and precise measurements of SETA. As we explained above,

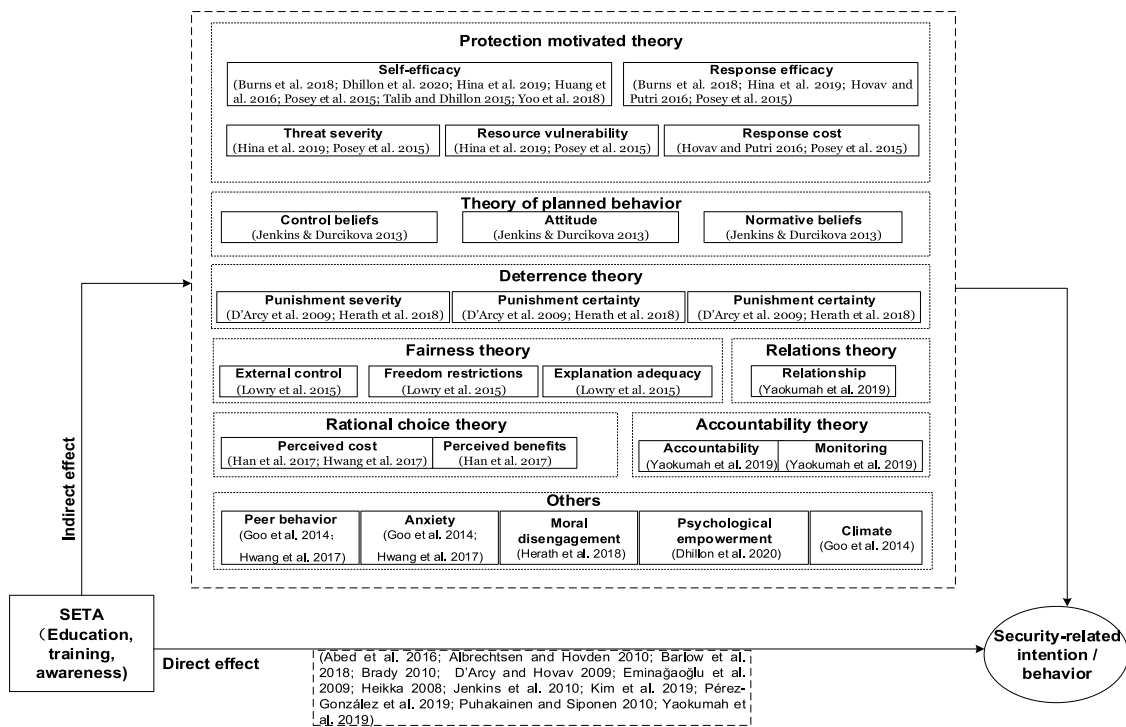


Figure 2. SETA and employees' secure behavior.

SETA consists of three different components that contribute to different levels of security learning. Although researchers broadly acknowledged these differences, our literature review revealed that the previous studies still used these terms interchangeably in their theoretical development and empirical investigations. For instance, some studies defined “security awareness program” as “an instructional tool for employees to clearly understand and accept IS policy suggested by an organization”, but used measurements like “My organization provides training to help employees with their computer security responsibilities.” We contend that there is a disconnection between the conceptualization and operationalization of the construct. A security awareness program merely focuses on employees' attention on security, making them know the information security issues. By comparison, security training is a program that aims to teach employees how security protection can be achieved, and the focus of security education is to enable employees to understand why security protection is required.<sup>8,54</sup> Therefore, future research should clearly explain which components of SETA are under investigation and develop specific measurements accordingly, since each component differs in its purpose, topic, and delivery methods. For instance, if the security awareness program is the focus of the research, a suitable measurement item could be: “My organization provides awareness programs to remind employees that security risks

exist in the environment”. For security training, an exemplary item could be: “My organization provides security programs to help employees learn security knowledge and skills”. By doing so, future research can increase the construct validity of SETA research.

Second, it has long been claimed that there is a need to develop theory-based SETA program design and implementation.<sup>12</sup> In our literature analysis, we found that the existing research scarcely focused on different approaches to designing the content and delivery methods of SETA. Based on the philosophy of learning, the constructivism of learning is fundamentally different from the traditional behaviorist learning approaches. Behaviorists apply the notion of objectivism as a learning theory, with a simple focus on “stimulus-response”. Adopting from the objectivist's view of the existence of one single reality, the behaviorist model of learning asserts that there is a true and absolute knowledge existing in the world and that knowledge is transmittable to learners through a teacher's instruction. In other words, in a behaviorist learning environment, the SETA instructor sets a prescribed learning goal and identifies a series of required behaviors for performance. By contrast, a constructivist learning environment focuses on knowledge discovery, emphasizes knowledge construction, and supports meaningful learning through authentic tasks relating to real-world experiences. In a similar vein, Miller and Seller<sup>99</sup> proposed three



different orientations for curriculum design: transmission, transaction, and transformation. In an information security context, transmission refers to one-way communication and simply presents employees with security information and rules; it does not involve any thinking processes. Transaction stresses cognitive adaptation by training employees in security skills. Transformation aims to shape users' beliefs about information security, providing them with insights and deep understanding regarding information protection countermeasures.

Therefore, we encourage more studies theorizing how different philosophical approaches to learning influence SETA program design in terms of learning activities, the role of instructors, and learning outcomes. Accordingly, future research could investigate whether game-based methods and other rich media are effective ways to encourage employees to participate in SETA programs and activate their learning about, and adoption of, information security mechanisms. Another prospective direction for future study might be to examine the effectiveness of utilizing a hands-on approach, such as a security defense competition in promoting employees' compliance with security policies. These approaches may provide employees with an immersive experience, thus making them see the possible consequences of security breaches. Another interesting research direction could be to further investigate the impact of different learning approaches on employees' security-related behaviors.

Besides, we also found that dominant empirical research on SETA seldom discussed how employees' security knowledge level and the types of SETA programs affect employees' security behavior intention. We propose that future studies on how different forms of SETA programs impact employees' security-related behavior can deepen our understanding of the design of SETA and its effectiveness. Another related issue is to further consider the relationship between the nature of the SETA program and other characteristics of employees such as their position in the organization, gender, and age (as shown in [Appendix A](#)). Empirical studies on these issues could yield additional insights into the association between individual differences and SETA effectiveness.

Lastly, our literature analysis revealed that a rich set of theoretical perspectives exists to explain the relationship between SETA and employees' security-related intentions and behaviors. To better understand such a relationship, a meta-analysis of the existing literature would enable researchers to make a more accurate assessment of this relationship. In addition, future studies could consider the relationship between SETA and different motives or types of employees' computer

abuse behavior. This would help us to understand how to design effective SETA programs targeting specific forms of computer abuse.<sup>9</sup> Methodologically, we believe that qualitative research could provide in-depth insights into the dynamics of organizational structures, employee practices, and institutional cultures that are relevant to the design and implementation of SETA programs.

## 5. Conclusion

We conducted a detailed review of the existing SETA research to explain the nature of SETA, analyze the design factors that contribute to an effective SETA program, and synthesize the impact of SETA on employees' security-related behaviors. This paper makes important theoretical and practical contributions. Theoretically, the research findings deepen our understanding of the role SETA plays on employees' compliance intentions. Practically, this research provides useful insights for designing and implementing SETA programs. We hope our review of the SETA literature will enrich the scope of SETA research, bring greater clarity, and provide guidance for future theoretical and empirical studies in this domain.

## Funding

This work was supported by the National Natural Science Foundation of China [71871162, 72011530135]; Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning [TP2018016].

## ORCID

Carol Hsu  <http://orcid.org/0000-0002-6545-9467>

Zhongyun Zhou  <http://orcid.org/0000-0003-4245-8733>

## References

1. Cram WA, D'Arcy J, Proudfoot JG. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Q* 2019;43(2):525–54. doi:10.25300/MISQ/2019/15117.
2. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf. Syst. Res* 2009;20(1):79–98. doi:10.1287/isre.1070.0160.
3. Furnell SM, Gennatou M, Dowland PS. A prototype tool for information security awareness and training. *Logist. Inf. Manage* 2002;15(5/6):352–57. doi:10.1108/09576050210447037.
4. Silic M, Lowry PB. Using design-science based gamification to improve organizational security training and compliance. *J. Manage. Inf. Syst* 2020;37(1):129–61. doi:10.1080/07421222.2019.1705512.

5. Posey C, Roberts TL, Lowry PB. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *J. Manage. Inf. Syst* 2015;32(4):179–214. doi:10.1080/07421222.2015.1138374.
6. Puhakainen P, Siponen M. Improving Employees' compliance through information systems security training: an action research study. *MIS Q* 2010;34(4):757–78. doi:10.2307/25750704.
7. Public Law 100–235. Available from: <https://www.govinfo.gov/content/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf#page=1>.
8. Wilson M, Hash J Building an information technology security awareness and training program. National Institute of Standards and Technology. 2003. Report No: NIST SP 800–50.
9. Willison R, Warkentin M. Beyond deterrence: an expanded view of employee computer abuse. *MIS Q* 2013;37(1):1–20. doi:10.25300/MISQ/2013/37.1.01.
10. Thomson ME, Von Solms R. Information security awareness: educating your users effectively. *Inf. Manage. Comput. Secur* 1998;6(4):167–73. doi:10.1108/09685229810227649.
11. Eminağaoğlu M, Uçar E, Eren Ş. The positive outcomes of information security awareness training in companies— a case study. *Inf. Secur. Tech. Rep* 2009;14(4):223–29. doi:10.1016/j.istr.2010.05.002.
12. Karjalainen M, Siponen M. Toward a new meta-theory for designing information systems (IS) security training approaches. *J. Assoc. Inf. Syst* 2011;12(8):518–55. doi:10.17705/1jais.00274.
13. Kennedy SE. The pathway to security— mitigating user negligence. *Inf. Comput. Secur* 2016;24(3):255–64. doi:10.1108/ICS-10-2014-0065.
14. Resilia A. Cyber Resilience: are your people your most effective defence? AXELOS Limited; 2016.
15. Caldwell T. Making security awareness training work. *Comput. Fraud Secur* 2016;6:8–14.
16. Jenkins JL, Durcikova A. What, I shouldn't have done that? The influence of training and just-in-time reminders on secure behavior. Proceedings of 34th International Conference on Information Systems; 2013; Milan, Italy.
17. Hu J, Meinel C. Tele-Lab "IT-Security" on CD: portable, reliable and safe IT security training. *Comput. Secur* 2004;23(4):282–89. doi:10.1016/j.cose.2004.02.005.
18. Aboutabl MS The cyberdefense laboratory: a framework for information security education. In: IEEE Information Assurance Workshop. 2006. IEEE, West Point, NY, pp 55–60.
19. Webster J, Watson RT. Analyzing the past to prepare for the future: writing a literature review. *MIS Q* 2002;26:xiii–xxiii.
20. Wilson M, De Zafra DE, Pitcher SI, Tressler JD, Ippolito JB Information technology security training requirements: a role- and performance-based model. National Institute of Standards and Technology. 1998. Report No: NIST SP.800-16.
21. Bauer S, Bernroider EWN. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *Data Base Adv. Inf. Syst* 2017;48(3):44–68. doi:10.1145/3130515.3130519.
22. Siponen MT. A conceptual foundation for organizational information security awareness. *Inf. Manage. Comput. Secur* 2000;8(1):31–41. doi:10.1108/09685220010371394.
23. Al-Omari A, El-Gayar O, Deokar A. Information security policy compliance: the role of information security awareness. Proceedings of the 18th Americas Conference on Information Systems; 2012; Seattle, USA.
24. Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Q* 2010;34(3):523–48. doi:10.2307/25750690.
25. Donalds C, Osei-Bryson K-M. Cybersecurity compliance behavior: exploring the influences of individual decision style and other antecedents. *Int. J. Inf. Manage* 2020;51:1–16. doi:10.1016/j.ijinfomgt.2019.102056.
26. Koohang A, Anderson J, Nord JH, Paliszkievicz J. Building an awareness-centered information security policy compliance model. *IMDS*. 2019;120(1):231–47. doi:10.1108/IMDS-07-2019-0412.
27. Moquin R, Wakefield RL. The Roles of Awareness, Sanctions, and Ethics in Software Compliance. *J. Comput. Inf. Syst* 2016;56(3):261–70. doi:10.1080/08874417.2016.1153922.
28. Kolb N, Abdullah F. Developing an information security awareness program for a Non-Profit organization. *Int. Manage. Rev* 2009;5:103–08.
29. Haeussinger F, Kranz J. Information security awareness: its antecedents and mediating effects on security compliant behavior. Proceedings of 34th International Conference on Information Systems; 2013; Milan, Italy.
30. Grance T, Nolan T, Burke K, Dudley R, White G, Good T Guide to test, training, and exercise programs for IT plans and capabilities. National Institute of Standards and Technology. 2006. Report No: NIST SP 800–84.
31. Alshaikh M, Naseer H, Ahmad A, Maynard SB. Toward sustainable behaviour change: an approach for cyber security education training and awareness. Proceedings of 27th European Conference on Information Systems; 2019; Stockholm, Sweden.
32. Burns AJ, Roberts TL, Posey C, Bennett RJ, Courtney JF. Intentions to Comply Versus Intentions to Protect: a VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts: intentions to Comply Versus Intentions to Protect. *Decis. Sci* 2018;49(6):1187–228. doi:10.1111/deci.12304.
33. Dhillon G, Talib YYA, Picoto WN. The mediating role of psychological empowerment in information security compliance intentions. *JAIS*. 2020;21:152–74. doi:10.17705/1jais.00595.
34. Goode J, Levy Y, Hovav A, Smith J. Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *OJAKM*. 2018;6(1):67–80. doi:10.36965/OJAKM.2018.6(1)67-80.
35. Kim HL, Choi HS, Han J. Leader power and employees' information security policy compliance. *Secur. J* 2019;32(4):1–19. doi:10.1057/s41284-019-00168-8.

36. Lowry PB, Posey C, Bennett RBJ, Roberts TL. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. *Inf. Syst. J* 2015;25(3):193–273. doi:10.1111/isj.12063.
37. Talib YYA, Dhillon G. Employee ISP compliance intentions: an empirical test of empowerment. *Proceedings of 36th International Conference on Information Systems*; 2015; Fort Worth, USA.
38. Yoo CW, Sanders GL, Cervený RP. Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decis. Support Syst* 2018;108:107–18. doi:10.1016/j.dss.2018.02.009.
39. Hwang I, Kim D, Kim T, Kim S. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Inf. Rev* 2017;41(1):2–18. doi:10.1108/OIR-11-2015-0358.
40. Pérez-González D, Preciado ST, Solana-Gonzalez P. Organizational practices as antecedents of the information security management performance: an empirical investigation. *ITP*. 2019;32(5):1262–75. doi:10.1108/ITP-06-2018-0261.
41. Huang H-W, Parolia N, Cheng K-T. Willingness and ability to perform information security compliance behavior: psychological ownership and self-efficacy perspective. *Proceedings of 34th Pacific Asia Conference on Information Systems*; 2016; Chiayi, Taiwan.
42. AlMindeed R, Martins JT. Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *ITP*. 2020.1–19.
43. Bauer S, Bernroider EWN, Chudzikowski K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Comput. Secur* 2017;68:145–59. doi:10.1016/j.cose.2017.04.009.
44. Goo J, Yim M, Kim DJA. Path to successful management of employee security compliance: an empirical study of information security climate. *IEEE Trans. Prof. Commun* 2014;57(4):286–308. doi:10.1109/TPC.2014.2374011.
45. Kruger HA, Kearney WD. A prototype for assessing information security awareness. *Comput. Secur* 2006;25(4):289–96. doi:10.1016/j.cose.2006.02.008.
46. Tsohou A, Karyda M, Kokolakis S, Kiountouzis E. Managing the introduction of information security awareness programmes in organisations. *Eur. J. Inf. Syst* 2015;24(1):38–58. doi:10.1057/ejis.2013.27.
47. Wolf M, Haworth D, Pietron L. Measuring an information security awareness program. *Rev. Bus. Inf. Syst* 2011;15(3):9–21. doi:10.19030/rbis.v15i3.5398.
48. Wu YA, Guynes CS, Windsor J. Security awareness programs. *RBIS*. 2012;16(4):165–68. doi:10.19030/rbis.v16i4.7435.
49. El-Haddadeh R, Tsohou A, Karyda M. Implementation challenges for information security awareness initiatives in E-government. *Proceedings of 20th European Conference on Information Systems*; 2012; Barcelona, Spain.
50. Furnell S, Vasileiou I. Security education and awareness: just let them burn? *Netw. Secur* 2017;12:5–9. doi:10.1016/S1353-4858(17)30122-8.
51. Katsikas S. Health care management and information systems security: awareness, training or education? *Int. J. Med. Inform* 2000;60(2):129–35. doi:10.1016/S1386-5056(00)00112-X.
52. Amankwa E, Loock M, Kritzing E. A conceptual analysis of information security education, information security training and information security awareness definitions. *Proceedings of 9th International Conference for Internet Technology and Secured Transactions*; 2014; London, UK.
53. Peltier TR. Implementing an information security awareness program. *Inf. Syst. Secur* 2005;14(2):37–49. doi:10.1201/1086/45241.14.2.20050501/88292.6.
54. Ross R, Pillitteri V, Dempsey K, Riddle M, Gary G. Protecting controlled unclassified information in nonfederal systems and organizations. *National Institute of Standards and Technology*. 2020. Report No: NIST SP 800-171.
55. McCoy C, Fowler RT. 'You are the key to security': establishing a successful security awareness program. In: *Proceedings of the 32nd annual ACM SIGUCCS conference on user services*. Baltimore (USA); 2004. p. 346–49.
56. Spurling P. Promoting security awareness and commitment. *Inf. Manage. Comput. Secur* 1995;3(2):20–26. doi:10.1108/09685229510792988.
57. Tsohou A, Karyda M, Kokolakis S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Comput. Secur* 2015;52:128–41. doi:10.1016/j.cose.2015.04.006.
58. Johnson EC. Security awareness: switch to a better programme. *Netw. Secur* 2006;2:15–18. doi:10.1016/S1353-4858(06)70337-3.
59. Tse WKD, Hui MH, Lam ST, Mok YC, Oei WC, Tang KL, Yau XL. Education in IT security: a case study in banking industry. *GSTF J. Comput* 2013;3(3):1–10. doi:10.7603/s40601-013-0019-8.
60. Hansche S. Designing a security awareness program: part 1. *Inf. Syst. Secur* 2001;9(6):1–9. doi:10.1201/1086/43298.9.6.20010102/30985.4.
61. May C. Approaches to user education. *Netw. Secur* 2008;9:15–17. doi:10.1016/S1353-4858(08)70109-0.
62. Heikka J. A constructive approach to information systems security training: an action research experience. *Proceedings of 14th Americas Conference on Information Systems*; 2008; Toronto, Canada.
63. Caputo DD, Pfleeger SL, Freeman JD, Johnson ME. Going spear phishing: exploring embedded training and awareness. *IEEE Secur. Privacy*. 2014;12(1):28–38. doi:10.1109/MSP.2013.106.
64. Abawajy J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol* 2014;33(3):237–48. doi:10.1080/0144929X.2012.708787.
65. Greitzer FL, Kuchar OA, Huston K. Cognitive science implications for enhancing training effectiveness in a serious gaming context. *J. Educ. Resour. Comput* 2007;7(3):1–15. doi:10.1145/1281320.1281322.
66. Hart S, Margheri A, Paci F, Sassone V. Riskio: a serious game for cyber security awareness and education.

- Comput. Secur. 2020;95:1–16. doi:[10.1016/j.cose.2020.101827](https://doi.org/10.1016/j.cose.2020.101827).
67. Yasin A, Liu L, Li T, Fatima R, Jianmin W. Improving software security awareness using a serious game. *IET Software*. 2019;13(2):159–69. doi:[10.1049/iet-sen.2018.5095](https://doi.org/10.1049/iet-sen.2018.5095).
68. Jenkins JL, Durcikova A, Burns MB. Simplicity is Bliss: controlling extraneous cognitive load in online security training to promote secure behavior. *J. Organ. End User Comput* 2013;25(3):52–66. doi:[10.4018/joeuc.2013070104](https://doi.org/10.4018/joeuc.2013070104).
69. Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. *Comput. Educ* 2009;52(1):92–100. doi:[10.1016/j.compedu.2008.06.011](https://doi.org/10.1016/j.compedu.2008.06.011).
70. Jenkins JL, Durcikova A, Burns MB. Forget the Fluff: examining how media richness influences the impact of information security training on secure behavior. *Proceedings of 45th Hawaii International Conference on System Sciences*; 2012; Maui, HI, USA.
71. Conklin A. Cyber defense competitions and information security education: an active learning solution for a capstone course. *Proceedings of the 39th Hawaii International Conference on System Sciences*; 2006; Washington, DC, USA.
72. Dodge RC, Carver C, Ferguson AJ. Phishing for user security awareness. *Comput. Secur* 2007;26(1):73–80. doi:[10.1016/j.cose.2006.10.009](https://doi.org/10.1016/j.cose.2006.10.009).
73. Konak A, Clark TK, Nasereddin M. Using Kolb's experiential learning cycle to improve student learning in virtual computer laboratories. *Comput. Educ* 2014;72:11–22. doi:[10.1016/j.compedu.2013.10.013](https://doi.org/10.1016/j.compedu.2013.10.013).
74. Meso P, Ding Y, Xu S. Applying protection motivation theory to information security training for college students. *J. Inf. Privacy Secur* 2013;9(1):47–67. doi:[10.1080/15536548.2013.10845672](https://doi.org/10.1080/15536548.2013.10845672).
75. Choi N, Kim D, Goo J, Whitmore A. Knowing is doing: an empirical validation of the relationship between managerial information security awareness and action. *Inf. Manage. Comput. Secur* 2008;16(5):484–501. doi:[10.1108/09685220810920558](https://doi.org/10.1108/09685220810920558).
76. Tsohou A, Kokolakis S, Karyda M, Kiountouzis E. Investigating information security awareness: research and practice gaps. *Inf. Secur. J.: A Global Perspect* 2008;17:207–27.
77. Dugan N. Security awareness training in a corporate setting [Doctoral Dissertation], IOWA STATE UNIVERSITY. 2018.
78. Hansche S. Information system security training: making it happen, part 2. *Inf. Syst. Secur* 2001;10(3):1–20. doi:[10.1201/1086/43316.10.3.20010701/31727.6](https://doi.org/10.1201/1086/43316.10.3.20010701/31727.6).
79. Stewart G, Lacey D. Death by a thousand facts: criticising the technocratic approach to information security awareness. *Inf. Manage. Comput. Secur* 2012;20(1):29–38. doi:[10.1108/09685221211219182](https://doi.org/10.1108/09685221211219182).
80. Barlow JB, Warkentin M, Ormond D, Dennis AR. Don't Even Think About It! the effects of antineutralization, informational, and normative communication on information security compliance. *J. Assoc. Inf. Syst* 2018;19(8):689–715. doi:[10.17705/1jais.00506](https://doi.org/10.17705/1jais.00506).
81. Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Comput. Secur.* 2010;29(4):432–45. doi:[10.1016/j.cose.2009.12.005](https://doi.org/10.1016/j.cose.2009.12.005).
82. Adepeju-Joseph S. The ELM as behavior modeling technique for effective cybersecurity training, awareness and education development [Doctoral Dissertation]. University of Nebraska. 2018.
83. McCrohan KF, Engel K, Harvey JW. Influence of awareness and training on cyber security. *J. Internet Commerce*. 2010;9(1):23–41. doi:[10.1080/15332861.2010.487415](https://doi.org/10.1080/15332861.2010.487415).
84. Kruger HA, Drevin L, Flowerday S, Steyn T. An assessment of the role of cultural factors in information security awareness. In: *Proceedings of 2011 information security for South Africa*. Johannesburg (South Africa): IEEE; 2011. p. 1–7.
85. Wiley A, McCormac A, Calic D. More than the individual: examining the relationship between culture and Information Security Awareness. *Comput. Secur* 2020;88:1–8. doi:[10.1016/j.cose.2019.101640](https://doi.org/10.1016/j.cose.2019.101640).
86. Chen CC, Dawn Medlin B, Shaw RS. A cross-cultural investigation of situational information security awareness programs. *Inf. Manage. Comput. Secur* 2008;16(4):360–76. doi:[10.1108/09685220810908787](https://doi.org/10.1108/09685220810908787).
87. Kajzer M, D'Arcy J, Crowell CR, Striegel A, Van Bruggen D. An exploratory investigation of message-person congruence in information security awareness campaigns. *Comput. Secur* 2014;43:64–76. doi:[10.1016/j.cose.2014.03.003](https://doi.org/10.1016/j.cose.2014.03.003).
88. McCormac A, Zwaans T, Parsons K, Calic D, Butavicius M, Pattinson M. Individual differences and information security awareness. *Comput. Human Behav* 2017;69:151–56. doi:[10.1016/j.chb.2016.11.065](https://doi.org/10.1016/j.chb.2016.11.065).
89. Tschakert KF, Ngamsuriyaroj S. Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*. 2019;5(6):1–10. doi:[10.1016/j.heliyon.2019.e02010](https://doi.org/10.1016/j.heliyon.2019.e02010).
90. Abed J, Dhillon G, Ozkan S. Investigating continuous security compliance behavior: insights from information systems continuance model. *Proceedings of 22nd Americas Conference on Information Systems*; 2016; San Diego, USA.
91. Brady JW. An investigation of factors that affect HIPAA security compliance in academic medical centers [Doctoral dissertation]. Nova Southeastern University. 2010.
92. Jenkins JL, Durcikova A, Ross G, Nunamaker JF. Encouraging users to behave securely: examining the influence of technical, managerial, and educational controls on Users' secure behavior. *Proceedings of 31st International Conference on Information Systems*; 2010; St. Louis, USA.
93. D'Arcy J, Hovav A. Does one size fit all? examining the differential effects of IS security countermeasures. *J. Bus. Ethics*. 2009;89:(S1):59–71. doi:[10.1007/s10551-008-9909-7](https://doi.org/10.1007/s10551-008-9909-7).
94. Hina S, Panneer Selvam DDD, Lowry PB. Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Comput. Secur* 2019;87:1–15. doi:[10.1016/j.cose.2019.101594](https://doi.org/10.1016/j.cose.2019.101594).
95. Hovav A, Putri FF. This is my device! Why should I follow your rules? Employees' compliance with



- BYOD security policy. *Pervasive Mob. Comput* **2016**;32:35–49. doi:[10.1016/j.pmcj.2016.06.007](https://doi.org/10.1016/j.pmcj.2016.06.007).
96. Herath T, Yim M-S, D'Arcy J, Nam K, Rao HR. Examining employee security violations: moral disengagement and its environmental influences. *Inf. Technol. People* **2018**;31(6):1135–62. doi:[10.1108/ITP-10-2017-0322](https://doi.org/10.1108/ITP-10-2017-0322).
  97. Han J, Kim YJ, Kim H. An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective. *Comput. Secur* **2017**;2018(66):52–65. doi:[10.1016/j.cose.2016.12.016](https://doi.org/10.1016/j.cose.2016.12.016).
  98. Yaokumah W, Walker DO, Kumah P. SETA and security behavior: mediating role of employee relations, monitoring, and accountability. *J. Global Inf. Manage* **2019**;27(2):102–21. doi:[10.4018/JGIM.2019040106](https://doi.org/10.4018/JGIM.2019040106).
  99. Miller JP, Seller W. *Curriculum Perspectives and Practice*. Longman Inc. (95 Church Street, White Plains, NY 10601): Pearson Education Canada; **1985**.



## Appendix A: Analysis of SETA by Employee Level, Geographic Location, and Industry

Category	Category/Type of Employees	Employee's Level	Definition	Geographic Location	Industry/Type of business	Reference
Nature of SETA (Conceptual)	General employees	N/A	N/A	N/A	N/A	Alshaiikh et al., <sup>31</sup> Amankwa et al., <sup>52</sup> Funnell and Vastleiou, <sup>50</sup> Katsikas, <sup>51</sup> Kolb and Abdullah, <sup>28</sup> Spurling, <sup>56</sup> Thomson and von Solms, <sup>10</sup> Tsohou et al., <sup>46</sup> Wu et al., <sup>48</sup> Caputo et al., <sup>63</sup> Kruger and Kearney, <sup>45</sup> Wolf et al. <sup>47</sup>
	General employees	N/A	N/A	Saudi Arabia	N/A	AlMindeel and Martins <sup>42</sup>
	University faculty, students	N/A	N/A	N/A	University	McCoy and Fowler <sup>55</sup>
	Public sector employees	N/A	N/A	N/A	Government	El-Haddadeh et al. <sup>49</sup>
Design factor of SETA (Conceptual or Empirical)	General employees	N/A	N/A	N/A	N/A	Caldwell, <sup>15</sup> Choi et al., <sup>75</sup> Dodge et al., <sup>72</sup> Greitzer et al., <sup>65</sup> Hansche, <sup>60,78</sup> Johnson, <sup>58</sup> Karjalainen and Siponen, <sup>12</sup> Kennedy, <sup>13</sup> May, <sup>61</sup> Peltier, <sup>53</sup> Shaw et al., <sup>69</sup> Stewart and Lacey, <sup>79</sup> Tsohou et al., <sup>76</sup> Yasin et al., <sup>67</sup> Abawajy, <sup>64</sup> Goode et al., <sup>34</sup> Silic and Lowry <sup>4</sup>
	General employees	N/A	N/A	Spain	Industrial SMEs	Pérez-González et al. <sup>40</sup>
	General employees	N/A	N/A	N/A	Bank	Bauer et al., <sup>43</sup> Tse et al. <sup>59</sup>
	Students	N/A	N/A	Thailand	N/A	Aboutabl, <sup>18</sup> Hu and Meinel, <sup>17</sup> Tschakert and Ngamsuriyaroj <sup>89</sup>
	General employees	N/A	N/A	United states	N/A	Kajzer et al. <sup>87</sup>
	General employees	N/A	N/A	Australia	N/A	Wiley et al. <sup>85</sup>
	Managers	N/A	N/A	N/A	N/A	Tsohou et al. <sup>57</sup>
	Students	N/A	N/A	N/A	N/A	Conklin, <sup>71</sup> Hart et al., <sup>66</sup> Jenkins et al., <sup>68,70</sup> Konak et al., <sup>73</sup> McCrohan et al., <sup>83</sup> Meso et al. <sup>74</sup>
	Students	N/A	N/A	South Africa	N/A	Kruger et al. <sup>84</sup>
	General employees	N/A	N/A	N/A	N/A	Albrechten and Hovden, <sup>81</sup> Barlow et al., <sup>80</sup> Gram et al., <sup>1</sup> D'Arcy et al., <sup>2</sup> Eminaoglu et al., <sup>11</sup> Funnell et al., <sup>3</sup> Haeussinger and Kranz, <sup>29</sup> Han et al., <sup>97</sup> Heikka, <sup>62</sup> Huang et al., <sup>41</sup> Kim et al., <sup>35</sup> Posey et al., <sup>5</sup> Yaokumah et al. <sup>98</sup>
	General employees	N/A	N/A	Taiwan, America	N/A	Chen et al. <sup>86</sup>
	General employees	N/A	N/A	Australia	N/A	McCormac et al. <sup>88</sup>
SETA & security-related behavior (Empirical)	General employees	N/A	N/A	Finland	Manufacture	Puhakainen and Siponen <sup>6</sup>
	General employees	N/A	N/A	N/A	Bank, financial, insurance	Lowry et al. <sup>36</sup>
	General employees	N/A	N/A	N/A	Bank	Abed et al. <sup>90</sup>
	General employees	N/A	N/A	Indonesia	N/A	Hovav and Putri <sup>95</sup>
	General employees	N/A	N/A	Malaysia	N/A	Hina et al. <sup>94</sup>
	General employees	N/A	N/A	South Korea	Law reinforcement agency	Yoo et al. <sup>38</sup>
	General employees	N/A	N/A	South Korea	Multinational IT organization	Herath et al. <sup>96</sup>
	General employees	N/A	N/A	South Korea	Manufacturing, service	Hwang et al. <sup>39</sup>
	General employees	N/A	N/A	N/A	IT organization	Goo et al. <sup>44</sup>
	Students and staff members	N/A	N/A	N/A	N/A	Jenkins et al. <sup>92</sup>
	Students and general employees	N/A	N/A	United states	N/A	D'Arcy and Hovav <sup>93</sup>
	General employees	N/A	N/A	United states	N/A	Burns et al. <sup>32</sup>
	Management and non-management employees	N/A	N/A	United states	N/A	Dhillon et al., <sup>33</sup> Talib and Dhillon <sup>37</sup>
	Students	N/A	N/A	N/A	N/A	Jenkins and Durcikova <sup>16</sup>
	General employees	N/A	N/A	N/A	N/A	
	General employees	N/A	N/A	N/A	N/A	
	General employees	N/A	N/A	N/A	N/A	
	General employees	N/A	N/A	N/A	N/A	
	General employees	N/A	N/A	N/A	N/A	
	General employees	N/A	N/A	N/A	N/A	

\*They argued that students represent new employees.