The impact of training sessions on physical security awareness : measuring employees' knowledge, attitude and self-reported behaviour

The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour

Marlies Sas, Genserik Reniers, Koen Ponnet, Wim Hardyns

Abstract

Today, the need to deal with workplace security threats has become an important matter for many organisations. While companies have invested in technological and organization measures, the human processes behind these techniques are often ignored. However, employees' awareness of security procedures and policy of the organisation may strengthen or weaken the implemented security measures. This article assessed in an empirical way employees' security awareness and has a twofold aim. First, a study was conducted to examine the associations between three dimensions of employees' security awareness. By the use of a survey (n = 1,443; mean age = 42.5; 60.4% female, 30.4% male), the relationship between employees' knowledge about security procedures and policy, the attitudes towards security and the self-reported security behaviour is measured. Second, a case study was carried out to examine the impact of training sessions on employee's level of security awareness. By organizing an awareness training, its effect on employees' knowledge, attitude and behaviour was measured (*n* = 74; mean age = 51.7; 70.3% female, 29.7% male). While the first study found a significant relationship between employees' knowledge and attitude and their self-reported behaviour, the second study showed that the training session had a positive effect on employees' level of security awareness. Based on the findings from both studies, recommendations for practice and future research are presented.

Keywords: Security awareness, physical security, Knowledge Attitude Behavior (KAB) model, security training

Declarations of interest: none.

1. Introduction

Workplace security threats, and how to handle them, are important issues worldwide (Villa et al., 2016). An increase in the use of digital information and communication techniques, complex modern infrastructures and a closer connection between different systems and organisations have all created greater vulnerability to security breaches. Companies have invested in numerous technological and organisational security measures in an attempt to address this issue, but both researchers and professionals suggest that even the most sophisticated security techniques cannot work effectively unless every member of an organisation acts in a secure way (Wiley et al., 2020). In recent years, there has been a noticeable shift of focus on to the importance of 'human processes' in dealing with security threats (Ghafir et al., 2018; Hassija et al., 2020). These human processes refer to employees' security awareness – the extent to which a member of an organisation understands the importance of security and the level of security required (ISF, 2002). An individual's security awareness can be categorised using three levels: perception, comprehension and protection, depending on the employee's degree of understanding of security issue (Shaw et al., 2009). An employee with the lowest level of awareness may be aware of the potential security risks but does not know how to mitigate them. At the comprehension level of awareness, the employee knows what the potential risks are, and knows how to act in a preventive way. At the protection level, the employee might have already experienced a similar security scenario and decides to act in a preventive way based on this earlier experience.

Researchers have experimented with various learning mechanisms to strengthen the role of employees in security, including online training, poster campaigns, email messages and face-to-face training sessions (ENISA, 2008; Johnson, 2006; Khan et al., 2011a). All these programmes are designed to affect employees' behaviour by increasing their knowledge about the threats and security policy and procedures of the organisation, in order to achieve more secure and compliant behaviour. However, the implementation of a security awareness programme does not guarantee that every employee has understood the information they are given. It is therefore important to measure how effective the specific method is in fulfilling its purpose (Khan et al., 2011b). In previous studies, the effectiveness of security awareness programmes has often been evaluated by measuring three equivalent dimensions (cf. the Knowledge, Attitude and Behaviour (KAB) model of Baranowski et al., 2003): what people know (knowledge), how people feel (attitude) and what people do (behaviour) (Kaur and Mustafa, 2013; Khan et al., 2011a; Kruger and Kearney, 2006; McCormac et al., 2017). Baranowski et al. (2003) propose that human functioning in relation to these dimensions can be fragmented in these dimensions. Acquiring knowledge may result in changes in attitudes, which in turn can lead to changes in behaviour. For instance, when employees have more knowledge about the potential security threats and understand the importance of security procedures, their attitude might change, which may result in more security-compliant behaviour. However, the authors underline that although a person's knowledge, attitude and behaviour are definitely interrelated, they are not necessarily linear or dependent on each other.

Previous studies show ambiguous results about the validity of the KAB model in practice. On the one hand, Chang and Liao (2009) found that an aviation safety education programme positively affected participants' knowledge, attitude and behaviour; Rosenbloom et al. (2008) concluded that an active learning programme in Israeli elementary schools resulted in an increase in children's knowledge and an improvement in behaviour regarding road safety; Van der Linden (2012) reviewed past studies dedicated to climate change and found significant associations between knowledge, attitude and behaviour; and Miller et al. (1990) stated that the KAB approach supported an AIDS prevention programme, as an increase in knowledge led to a change

in behaviour among the participants. On the other hand, Shaftel and Shaftel (2005) indicated that, while universities observe the influence of teaching on students' knowledge and skill development, less is known about the impact on their attitudes and behaviour; and in a study relating to oral health Singh (2009) found no correlations between high school students' knowledge, attitude and behaviour.

Within the field of security, very little research has been carried out on how employees' security awareness can be improved. The few studies that have explored this have mainly focused on the impact of security training and education on employees' awareness regarding information security. Wahyudiwan et al. (2017), for instance, showed that knowledge-based programmes improved the knowledge, attitude and behaviour of employees regarding topics such as password management and email usage. Also, Parsons et al. (2014) found significant associations between a person's knowledge, attitude and behaviour when using a work computer. Kaur and Mustafa (2013) found significant relationships between end users' attitudes and behaviour, and their information security awareness. However, no significant association was found between knowledge and information security awareness.

While the aforementioned studies examined employees' awareness of security threats in an online environment, very few – if any – studies exist about employees' awareness of physical security, or security in the offline world. In order to fill this research gap, the aim of the current research was twofold. In a first study (Study 1) we examined whether employees' knowledge of physical security procedures and policy was associated with their attitudes towards security and their self-reported security behaviour. Using a questionnaire distributed among staff at a university, we measured the relationship between physical security knowledge, attitude and behaviour . In a second study (Study 2) security training sessions were organised, and their impact on staff members' knowledge, attitude and behaviour concerning physical security was measured.

Both studies were conducted among staff members of a university in Antwerp, Belgium. Universities function as interesting research objects for this type of study for several reasons. Higher educational institutions are increasingly confronted with various types of crime (Doss et al., 2017; Jacobsen, 2017; Jennings et al., 2007; Schokkenbroek et al., 2020). While minor crimes such as theft and vandalism occur regularly, universities' characteristics, such as the presence of a large number of young people, server rooms that store valuable information and laboratories with potentially harmful substances make them an attractive target for more serious crimes such as terrorism or espionage (Boynton, 2003; Grubbs, 2019). Moreover, most European universities consist of various (semi-) publicly accessible spaces, which implies that it is not always possible or desirable to implement significant physical security measures, and that security is strongly dependent on the strength of the human factor. A university security model must therefore include initiatives that increase and maintain the level of security awareness among staff members.

Based on the results of both studies, concluding remarks and recommendations are made that are applicable to both higher educational institutions and other types of organisations.

2. Study 1: The association between knowledge, attitude and behaviour

2.1. Hypotheses

Study 1 examined the interconnectedness between the three dimensions of security awareness. To measure the relationships between employees' security knowledge, attitudes and behaviour, three hypotheses were proposed: (i) more knowledge about security procedures and policy leads to a better attitude towards security, (ii) a better attitude towards security leads to more secure self-reported behaviour, (iii) more knowledge about security procedures and policy leads to more secure self-reported behaviour.

2.2. Data and methods

2.2.1. Data collection

A questionnaire was distributed among staff members of a Belgian university between 3 June and 7 August 2019. All employees (*N* = 5,924) working at the university during this period were eligible to participate in the study. Staff members could therefore voluntarily choose to complete the questionnaire, utilising self-selection processes. With the cooperation of the central administration of the university, every employee received an email with a link to the questionnaire, which was developed in Qualtrics. After ten days, a polite reminder was sent via email and an announcement was placed on the university's intranet.

To fulfil the first aim of the study, the survey included questions regarding the three dimensions of the KAB model. A first draft of the questionnaire was developed after a review of existing questionnaires and an analysis of the security information presented on the university's intranet. All questions were self-developed and presented to a panel of ten security experts at the university. Each security expert represented a department related to security (e.g., Department of Infrastructure). They were asked about their understanding of the questions and whether they wanted to include other security topics of importance to them in the survey. Based on their comments and suggestions, the proposed questions were kept, but were adjusted and finalised. In order to measure knowledge, five items were included (e.g., 'At the university, I know where I can report crimes of which I am the victim'). For each item, respondents had to indicate a number on a five-point Likert scale ranging from not at all (= 1) to totally (= 5). To measure employees' attitudes, three items were included in the questionnaire (e.g., 'The university provides its staff members with sufficient information about security'). Each item was scored on a five-point Likert scale ranging from totally disagree (= 1) to totally agree (= 5). Employees' self-reported behaviour was measured using three items (e.g., 'If I noticed something or someone suspicious at the university, I would report it'). Respondents had to indicate their answer on a five-point Likert scale ranging from (almost) never (= 1) to (almost) always (= 5).

2.2.2. Data analysis

Structural equation modeling (SEM) was applied to the collected data using Mplus 8 (Muthén and Muthén, 2017) to examine the relationships between the KAB constructs. First, a measurement model was built to test whether the observed variables reliably reflected the hypothesised latent variables. Second, we estimated a structural model. The SEM results were obtained with the maximum likelihood mean adjusted, because preliminary tests suggested that all three constructs were not normally distributed. Given the large sample size, p-values <0.01 are considered significant.

The model fits of the measurement and path models were evaluated according to several fit indices. Given that the $\chi 2$ is almost always significant and not an adequate test of the model fit (Kline, 2011), we also reported the comparative fit index (CFI), root mean square error of

approximation (RMSEA), and the standardised root mean square residual (SRMR). The CFI ranges from 0 to 1.00, with .95 or higher indicating that the model provides a good fit (Hu and Bentler, 1999). RMSEA and SRMR values below .05 indicate a good model fit, and values from .06 to .08 indicate an adequate fit (Ponnet, 2014).

2.3. Results

2.3.1. Demographic data

In total, 1,443 employees participated in the study, which yields a response rate of 24.4%. Table 1 provides an overview of the demographic characteristics of the participants. Most respondents had been working at the university for 10 years or more (35.3%). The gender split was 60.4% females (*n* = 871) and 39.6% males (*n* = 572). A large majority of the study's participants were administrative and technical staff (51.6%). More than 80% of participants had a full-time equivalent between 76% and 100% at the time they filled in the questionnaire.

Table 1. Demographic characteristics of respondents in Study 1 (*N* = 1,443).

	n	**%**
Gender		
Male	572	39.6
Female	871	60.4
Age		
20-29	249	17.3
30-39	412	28.6
40-49	340	23.6
50-59	275	19.1
≥ 60	163	11.3
Missing	4	0.3
Staff category		
Professors	169	11.7
Assistants	125	8.7
Researchers	358	24.8
Administrative and technical staff	745	51.6
Educational staff	45	3.2
Length of career at university		
Less than 1 year	169	11.7
Between 1 and 5 years	483	33.5
Between 6 and 10 years	282	19.5
More than 10 years	509	35.3
% full time effort		
≤ 25%	50	3.5
Between 26% and 50%	122	8.5
Between 51% and 75%	76	5.3
Between 76% and 100%	1,195	82.8

2.3.2. Overview of the variables

The questionnaire included 11 items, related to the three dimensions of the KAB model: knowledge (5 items), attitude (3 items) and behaviour (3 items). The reliability, or internal consistency, of a set of scale items was checked using Cronbach's alpha. Items that would increase Cronbach's alpha in their absence were deleted (Attitude: 1 item; Behaviour: 1 item). Table 2 provides an overview of all study variables with their descriptives (mean and SD) and internal reliability of each scale. The composite mean score per scale refers to the mean of all scores on the individual items for that scale.

Table 2. Descriptives of the variables in Study 1 (*N* = 1,443).

	M	SD
Knowledge (α = 0.90)	**3.25**	**1.10**
Item 1 – At the university, I know where I can find information about preventive security tips (e.g., tips for the prevention of theft)	3.20	1.31
Item 2 – At the university, I know where to report crimes of which I am the victim (e.g., theft, violence)	3.40	1.34
Item 3 – At the university, I know how to report suspicious behaviour	3.25	1.29
Item 4 – At the university, I know what to do if there is an emergency situation (e.g., bomb alert, active shooter)	3.14	1.30
Item 5 – At the university, I know where to go when I am confronted with unacceptable behaviour (e.g., stalking, inappropriate sexual behaviour)	3.26	1.27
Attitude (α = 0.77)	**3.25**	**0.74**
Item 1 – The university has sufficient security measures	3.13	0.93
Item 2 – The university takes sufficient action in case of an emergency situation	3.51	0.79
Item 3 – The university provides its staff members with sufficient information about security	3.10	0.96
Behaviour (α = 0.60)	**3.73**	**0.79**
Item 1 – If I noticed someone in the hallway who does not seem to belong to the university, I would approach him/her	3.13	1.26
Item 2 – If I noticed someone or something suspicious at the university, I would report it	3.55	1.10
Item 3 – If I witnessed an incident at the university (e.g., violence, theft), I would report it	4.50	0.78

All constructs were significantly related to each other at the $p < .001$ level. The associations between knowledge and attitude, and knowledge and behaviour were .36 and .37 respectively. The association between attitude and behaviour was .16.

2.3.3. Measurement model

The measurement model provided a good fit for the data: $\chi2(41) = 230.65$, $p < .001$; CFI = .968, RMSEA = .057, CI [.050, .065], and SRMR = .047. All factor loadings were significant and above .48. We subsequently included gender, age, % full-time effort, length of career and staff category (professor, assistant, researcher, administrative and technical staff, educational staff) as covariates in the analyses and examined the relationships between these covariates and the study variables.

Age was significantly associated with behaviour ($\beta = .265$, $p < .001$) and knowledge ($\beta = .11$, $p < .001$), which implies that older staff members had more security knowledge and behaved in a

more secure way. Percentage full-time effort was significantly related with knowledge (β = .148, p < .001), suggesting that staff members with a higher % full-time effort at the university knew more about the university's security procedures and policy. Length of career was significantly related to knowledge (β = .204 p < .001), suggesting that staff members who had worked for a longer time at the university had more knowledge about the security procedures and policy. The staff category 'administrative and technical staff' was significantly related to knowledge (β = .366, p < .01). The structural model was adjusted for these covariates.

2.3.4. Structural model

The results of the structural model are presented in Figure 1. The results of the fit statistics indicated an adequate model fit: χ2(80) = 350.95, p < .001; CFI = .959, RMSEA = .049, CI [.044, .054], and SRMR = .047.

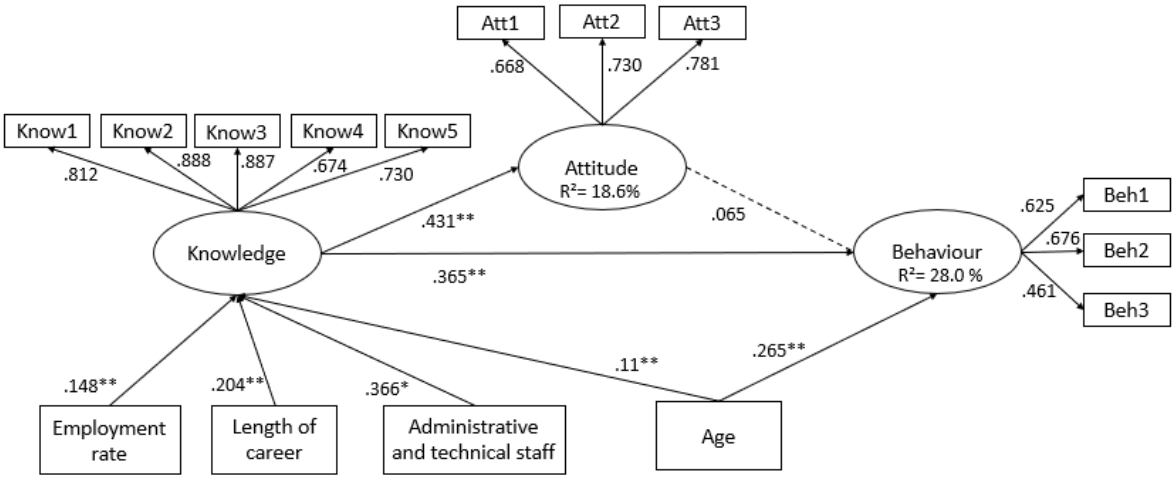

Figure 1. Structural model for the KAB model of security awareness. Note. Know1-5, Att1-3 and Beh1-3 represent the items presented in Table 2. All reported coefficients are standardised values, adjusted for the influence of covariates. The dashed lines indicate non-significant paths. *p < .01; **p < .001.

Our analyses revealed that knowledge explained 18.6% of the variance in attitude, and that knowledge and attitude explained 28.0% of the variance in behaviour. Knowledge was significantly associated with attitude (β = .431, p < .001) and behaviour (β = .365, p < .001), thus confirming that staff members who knew more about security procedures and policy had better attitudes towards security and behaved in a more secure way. Unexpectedly, attitude was not significantly associated with behaviour (β = .065, p = .087). As a result, the indirect effect from knowledge to behaviour was not significant (β = .028, p = .091).

3. Study 2: The impact of training sessions on security awareness

3.1. Hypotheses

In Study 2, three hypotheses were formulated in order to check whether participation in the training session had an impact on employees' level of security awareness: (i) participating in the training sessions significantly improved employees' knowledge of security procedures and policy, (ii) participating in the training sessions significantly improved employees' attitude regarding

security, (iii) participating in the training sessions significantly improved employees' self-reported security behaviour.

3.2. Data and methods

The aim of the second study[1] was to examine to what extent training sessions have an impact on participants' level of security awareness. In order to do this, training was organised for the employees of a Belgian university (the same sample as in Study 1) between 21 March and 19 April 2018. Various security procedures and topics of importance to the university were included in the training. Before the content of the training session was devised, ten security experts from the university (the same experts as in Study 1) were interviewed to explore which topics were relevant. The experts suggested that the focus should be on four topics: terrorism, radicalisation, incident reporting and employees' own security responsibilities at the university. Based on their insights, a training session with a focus on all of these security topics was developed.

The training sessions were held during the working day between 12:00 and 14:00 hours. Three sessions were held on three different dates and at different locations, each with a maximum capacity of 55 participants. All university employees were informed about the training sessions via an announcement on the intranet and a personal email, both of which included a registration link. Registration was entirely voluntary. To analyse the impact of the training sessions on employees' levels of security awareness, two questionnaires were developed and distributed among the participants before and after the sessions. The pre-test questionnaire was sent immediately after employees registered for the training. The post-test questionnaire was distributed among the participants about two weeks after the training session. The aim was to examine whether the training sessions had improved participants' security-related knowledge, attitude and behaviour.

Based on the KAB model, questions regarding knowledge, attitude and behaviour were included in both the pre-test and post-test questionnaire. All questions focused on the specific topics that were discusses during the training sessions. After the questions were formulated, they were presented to the university security expert panel and then adjusted. The final pre-test questionnaire consisted of 24 questions. Five statements were developed to assess employees' knowledge about the university's security procedures and policy (e.g., 'I know how to report suspicious behaviour'). Answers were scored on a five-point Likert scale ranging from totally disagree (= 1) to totally agree (= 5). To measure employees' attitude towards security, three statements were included (e.g., 'Every suspicious behaviour or situation must be reported, even if it turns out to be nothing'). Each item was scored on a five-point Likert scale ranging from totally disagree (= 1) to totally agree (= 5). Additionally, three items referring to employees' self-reported behaviour were included in the questionnaire (e.g., 'If I noticed someone or something suspicious at the university, I would report it'). Staff members indicated their answer on a five-point Likert scale ranging from (almost) never (= 1) to (almost) always (= 5). The post-test questionnaire consisted of exactly the same questions as those in the pre-test questionnaire, together with a couple of additional statements asking participants to evaluate the training session.

[1] A brief summary of the results of Study 2 can also be found in: Sas, M., Reniers, G., Hardyns, W., & Ponnet, K. (2019). The impact of training sessions on security awareness: Measuring the security knowledge, attitude and behaviour of employees. *Chemical Engineering Transactions, 77*, 895-900.

Changes in employees' scores on knowledge, attitude and behaviour between the pre-test and post-test were analysed by using Wilcoxon signed-rank tests, as normality assumptions were unsatisfied. The criterion for significance was set at 0.05.

3.3. Results

3.3.1. Demographic data

In total, 157 employees registered for one of the three sessions, 116 of whom attended a session. As shown in Table 3, the sample comprised 74 employees who both attended the training sessions and completed the pre- and post-questionnaire. A majority of women (70.3%) participated, while every respondent indicated they were over 25 years of age. The defined age groups (see Table 3) were approximately equally represented. When asked about the length of their career at the university, most respondents had either worked at the university for between one and five years (39.2%), or for more than 10 years (47.3%). Only three participants indicated that they had worked at the university for less than a year.

Table 3. Demographic characteristics of respondents of Study 2 (*N* = 74).

	n	**%**
Gender		
Female	52	70.3
Male	22	29.7
Age		
<25	0	0
25-35	15	20.3
36-45	21	28.4
46-55	19	25.7
>56	19	25.7
Length of career at university		
<1 year	3	4.1
1-5 years	29	39.2
6-10 years	7	9.5
>10 years	35	47.3

3.3.2. Results of the pre-test and post-test

The results showed that the training session had a positive effect on employees' knowledge of the university's security procedures and policy (see Table 4). For all statements, significant differences ($p<0.05$) between the two tests were found. The biggest improvement is noticed when comparing the pre- and post-test results for the statements 'I know the difference between the procedures for a fire alarm and a bomb alert' ($z = 6.816$, $p>0.001$) and 'I know how to report signs of radicalisation among students or staff members' ($z = 6.832$, $p<0.001$). Sixty-one of 73 respondents (83.6%) indicated they were more aware of the difference in procedures for a fire alarm and a bomb alert. Additionally, 63 of 74 respondents (85%) were convinced that after the training

session they were more knowledgeable about the internal reporting tools for radicalisation. Based on the results of all knowledge statements, it can be concluded that respondents scored significantly higher on self-reported knowledge about security after their participation in the training session. Therefore, the first hypothesis is confirmed.

Table 4. Changes in employees' knowledge regarding security procedures and policy (*N* = 74).

Statements	Pre-test M (SD)	Post-test M (SD)	z-score	p-value	Sample	Scoring higher	Scoring lower	Scoring even
I know the difference between the procedures for a fire alarm and a bomb alert	2.32 (1.218)	4.04 (0.841)	6.816	p<0.001	73	N=61	N=3	N=9
I know how to report suspicious behaviour	3.14 (1.162)	4.51 (0.503)	6.215	p<0.001	74	N=51	N=2	N=21
I know where to report crimes of which I'm the victim	3.51 (1.317)	4.57 (0.526)	6.461	p<0.001	74	N=54	N=2	N=18
I know how to report signs of radicalisation among students or staff members	2.61 (1.259)	4.30 (0.677)	6.832	p<0.001	74	N=63	N=4	N=7
I know where to go with questions about security	4.07 (0.912)	4.45 (0.708)	3.220	p=0.001	73	N=33	N=9	N=31

Note. A composite mean score of 3.13 (SD = .92) was found. Reliability analysis indicated the scale has a Cronbach's alpha of .84. 'Scoring higher', 'scoring lower' and 'scoring even' refer to a comparison between the post-test and pre-test scores.

For employees' attitudes towards security, the Wilcoxon signed-rank tests showed a significant improvement on two of three statements (see Table 5). After the training session, more employees were convinced about their personal responsibility with respect to security and the need to report suspicious situations. However, when asked to what extent security is an important topic, a majority of 48 respondents indicated the same score. Remarkably, only 11 employees indicated a higher score after the training session, while 14 of them indicated lower scores. Although a limited number of participants scored higher on the post-test, it should be noted that the pre-test mean (4.46) was already very high. Based on the majority of the statements, there was a significant improvement in the attitude of employees towards security. This implies that the second hypothesis is confirmed.

Table 5. Changes in employees' attitude towards security (*N* = 73).

Statements	Pre-test M (SD)	Post-test M (SD)	z-score	p-value	Sample	Scoring higher	Scoring lower	Scoring even
The security of the university is an important topic	4.46 (0.894)	4.48 (0.669)	0.044	p=0.965	73	N=11	N=14	N=48
Every suspicious behaviour or situation must be reported, even	4.01 (0.884)	4.30 (0.639)	2.868	p=0.004	73	N=28	N=10	N=35

though it turns out to be nothing								
I feel responsible for the security of the university	4.01 (0.630)	4.26 (0.578)	2.999	p=0.003	73	N=21	N=6	N=46

Note. A composite mean score of 4.16 (SD = .61) was found. Reliability analysis indicated the scale has a Cronbach's alpha of .60. 'Scoring higher', 'scoring lower' and 'scoring even' refer to a comparison between the post-test and pre-test scores.

Regarding employees' self-reported security behaviour, no significant differences were found between the pre-test and post-test questionnaires (see Table 6). The large majority of employees indicated an even score on both pre-test and post-test. For all three statements, only a very limited number of respondents indicated higher scores in the post-test. Based on these results, it can be concluded that the training sessions had less of an impact on the self-reported behaviour of employees than on their knowledge and attitude. Hence, when looking at all statements, the third hypothesis cannot be confirmed.

Table 6. Changes in employees' self-reported security behaviour (*N* = 71).

Statements	**Pre-test M (SD)**	**Post-test M (SD)**	**z-score**	**p-value**	**Sample**	**Scoring higher**	**Scoring lower**	**Scoring even**
If I noticed someone suspicious, I would report it	4.51 (1.024)	4.28 (0.759)	1.775	p=0.076	71	N=13	N=22	N=36
If I were the victim of a crime, I would report it	4.95 (0.571)	4.87 (0.335)	0.727	p=0.467	71	N=5	N=14	N=52
If I were confronted with an emergency situation, I would report it via the internal reporting tools	4.73 (0.926)	4.83 (0.377)	1.050	p=0.294	71	N=13	N=13	N=45

Note. A composite mean score of 4.73 (SD = .70) was found. Reliability analysis indicated the scale has a Cronbach's alpha of .74. 'Scoring higher', 'scoring lower' and 'scoring even' refer to a comparison between the post-test and pre-test scores.

4. Discussion

Most companies want their employees to exhibit security-compliant behaviour, therefore a clear understanding of the effectiveness and impact of security awareness initiatives is indispensable. To provide more insight into this topic, the aim of the current article was twofold: examining the relationship between employees' security knowledge, attitudes and self-reported behaviour (Study 1) and measuring the impact of security training on their level of security awareness (Study 2). The first study found that employees who have more security knowledge also displayed a better attitude towards security issues. Additionally, employees who reported having more security knowledge and better attitude towards security indicated they would behave in a more secure way. No significant relationship was found between employees' attitudes towards security and their self-reported security behaviour. Taking into account employees' socio-demographic characteristics, positive associations were found between their age, length of career and % full time effort, and their security knowledge. Older employees also indicated that they behaved in a more secure way. The results of the second study showed that the training session had a positive

effect on employees' security knowledge and attitudes towards security. The impact of the training on staff members' self-reported behaviour was also found to be positive, but less strong compared to knowledge and attitude. A comprehensive overview of the findings from both studies indicates that more security knowledge and better attitudes towards security are related to more self-reported security-compliant behaviour. Moreover, training sessions were found to be effective in increasing employees' security knowledge and attitudes. Extra attention should, however, be given to the impact of training on participants' behaviour.

Regarding the validity of the KAB model, our results showed that employees' attitudes towards security were not significantly related to their self-reported behaviour. In this light, it should be acknowledged that other factors could have played a mediating role in the KAB model. Parsons et al. (2014), for instance, state that employees may well know the security procedures and behave in a secure way, even when their attitudes towards security issues are negative. The desire to keep their job may be a mediating factor in employees choosing to act in a security-compliant way. Previous studies in healthcare (Baranowski et al., 2003) and environmental awareness (Newbould and Furnell, 2009) support this statement, and indicate that individuals' knowledge and attitude are not sufficient to explain changes in behaviour. A potential explanation for this complex relationship between attitude and behaviour can be found in the Theory of Planned Behaviour of Azjen (1991), which assumes that a person's behavioural change is dependent on three beliefs: behavioural beliefs, or beliefs about the consequences or other attributes of behaviour; normative beliefs, or beliefs about the normative expectations of other people; and control beliefs, or beliefs about the presence of factors that may support or hinder performance of the behaviour. The intention towards particular behaviour will be higher if the person has a positive attitude about it, more of a subjective norm towards the behaviour and a high perception of behavioural control.

In addition to the impact of mediators, moderators could also influence this attitude–behaviour inconsistency. A potential explanation is provided by the Attitude, Behaviour and Structural Conditions (ABC) model of Guagnano et al. (1995). According to this model, a person's behaviour depends not only on their attitudes, but also on contextual conditions. The relationship between an individual's attitude and behaviour is strongest when contextual factors are neither too strong nor too weak, providing the right level of support. This implies that employees who work in highly supportive structural conditions but have a negative attitude towards security may still act in a secure way. In reality, and adapted to the field of physical security, this means that the organisation must possess the tools and structures that are needed to simulate employees to act in a security-compliant way. Insufficient support or a weak organisational culture could create the opposite result. Another moderating factor may be found in the processes that contribute to people's attitude formation. Regan and Fazio (1977) indicate that individuals who form their attitudes based on direct behavioural interaction with the attitude's object will show significantly greater attitude–behaviour consistency than people whose attitudes were formed by other means. The authors start from the assumption that direct behavioural experiences form an attitude that is more stable than an attitude produced through indirect means. Related to the field of physical security, this would, for instance, imply that people who have themselves been a victim of crime will demonstrate higher attitude–behaviour consistency compared to individuals who have not. Bulgurcu et al. (2010) found that prior negative experiences, both direct and indirect, with information security increased employees' level of information security awareness. In this light, the organisation of more interactive training sessions where people gain experience with the topic may increase the relationship between their attitudes and behaviour. More practical awareness initiatives, such as penetration tests, red teaming, simulation attacks or interactive demos may therefore be recommended.

Furthermore, when implementing security awareness programmes, one should keep in mind the exact level of security awareness that is expected by the organisation. The level of security awareness that is expected of an employee at a university may differ from that required of an employee of a chemical or nuclear company. Therefore, it is important for an organisation to identify the level of security awareness it expects of its employees, and adapt its security awareness programmes to these predefined goals. Moreover, any security awareness programme needs to be continually measured and monitored to respond to all relevant threats at that time. Physical security processes are dynamic because they are dependent on continuously changing threat profiles. This implies that employees have to be updated about these changes, and in order to do that security awareness training should be an integral part of the security culture of the organisation. In each and every organisation, regardless of its type of business, location or size, people are always a key factor for successful physical security management. Furthermore, as Study 1 showed that employees' age, % full-time effort, length of career and staff category are significantly related to their knowledge about security, it is vital to involve everyone in awareness initiatives. Specific attention should be paid to new employees and staff members who only occasionally work at the organisation. In this light, employees who are not formally part of the organisation, such as contractors or consultants, should also be encouraged to participate in security awareness programmes.

Although this article has provided valuable insights into the knowledge–attitude–behaviour relationship regarding physical security, some limitations have to born in mind when interpreting the results of the two studies. First, employees participated in both studies on a voluntarily basis, which implies that the participants represent a self-selected sample of the targeted population or a non-random selection. Unfortunately, the researchers could not control for the self-selection process of voluntary, online surveys. While the high response rate of Study 1 increases the validity of the study, the much smaller number of participants in Study 2 contributes to a lower generalisability of the research findings. Therefore, it is not known how the participants compare to other employees who did not fill in the questionnaire. Even though previous research showed that self-selection does not necessarily bias the results of surveys used in studies conducted at higher educational institutions (Brown et al., 2014; Rosenthal and Freyd, 2018), this limitation should be kept in mind. Additionally, the results of both studies may be influenced by socially desirable behaviour. To overcome this limitation, questionnaires were filled in anonymously and the confidentiality of the answers was emphasised at the beginning of the surveys. However, as with most self-reported data, the results may not be a true reflection of the actual security knowledge, attitude and behaviour of employees. Moreover, we can expect that employees who decided to participate in the first study or who engaged in the training session may already have been more interested in security issues at the university than those who did not choose to take part. This implies that caution is needed when generalising these conclusions to the whole staff member population of the university. Furthermore, in both questionnaires, only a limited number of items were included to measure employees' knowledge, attitude and behaviour. To the authors' knowledge, no measurement tools for physical security awareness were available at the start of the current study. Therefore, all items had to be created based on the security aspects that were relevant for the university where the study was conducted. For future studies, we suggest the question items for each awareness dimension should be redefined. The items should ideally be adapted to the security policy and procedures of the organisation where the study is conducted.

The current research also has the limitation that the results may only be valid for short-term conclusions. Both studies were conducted on a cross-sectional basis, which implies that it was not

possible to explore the long-term effect of employees' security level of awareness and the impact of the training sessions. In the first study, the questionnaire was distributed over a period of two months. Factors such as criminal incidents at the university or communication about security from the university could have influenced employees' security knowledge, attitude or self-reported behaviour at the time they filled in the survey. In the second study, the post-test questionnaire was distributed approximately two weeks after the training session. It is possible that participants scored higher on some questions because they remembered what had been discussed during the training. This implies that, for both studies, only short-term conclusions can be made. Further research is needed to examine whether employees' level of security awareness varies across time, and to what extent training causes a long-term improvement in employees' awareness. Finally, both the studies discussed in this article were conducted among staff members of a university. While this type of organisation functioned as an interesting research environment, one should keep in mind the specific contextual features of higher educational institutions. Caution should be exercised when generalising the conclusions of these studies to populations outside of the specific university where they took place. Similar studies conducted in other types of organisations are needed in order to examine whether the organisational culture and context have a substantial impact on the outcomes.

Despite these limitations, the results provide valuable information for security officers of universities, but also other types of organisation. Empirical results on the association between employees' security knowledge, attitude and behaviour and the efficiency of training programmes in enhancing security awareness were provided. While this study offered a first insight into physical security awareness in a university context, future research is needed in other types of organisations.

5. References

Ajzen, I. (1991). Theory of planned behaviour. *Organizational Behaviour And Human Decision Processes, 50*, 179–211.

Baranowski, T., Cullen, K.W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are current health behavioural change models helpful in guiding prevention of weight gain efforts? *Obesity research*, *11*, 23-43.

Boynton, A. (2003). Securing college campuses in the face of terrorism. *Campus Law Enforcement Journal, 33*(5), 15-17.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-527.

Chang, Y. H., & Liao, M. Y. (2009). The effect of aviation safety education on passenger cabin safety awareness. *Safety science, 47*(10), 1337-1345.

Doss, D. A., Lackey, H., McElreath, D., Goza, R., Gokaraju, B., Tesiero, R., & Sheffield, J. (2017). A Quantitative Examination of Crime: Reported Incidents at Land-Grant Higher Education Institutions versus Reported Societal Incidents. *Journal of Interdisciplinary Studies in Education, 6(*1), 81.

ENISA (2008). *The new users' guide: How to raise information security awareness*, European Network and Information Security Agency.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986-5002.

Grubbs, E. N. (2019). Academic Espionage: Striking the Balance Between Open and Collaborative Universities and Protecting National Security. *North Carolina Journal of Law & Technology, 20*(5), 235.

Guagnano, G. A., Stern, P. C., & Dietz, T. (1995). Influences on attitude–behavior relationships: A natural experiment with curbside recycling. *Environment and Behavior, 27*, 699–718.

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, *99*, 1-25.

Hu, L., & Bentler, P. (1999). Cutof Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus new Alternatives. *Structural Equation Modeling, 6*, 1–55.

ISF (2002). *Effective security awareness (workshop report),* Information Security Forum.

Jacobsen, S. K. (2017). Examining crime on campus: The influence of institutional factors on reports of crime at colleges and universities. *Journal of Criminal Justice Education, 28*(4), 559-579.

Jennings, W. G., Gover, A. R., & Pudrzynska, D. (2007). Are institutions of higher learning safe? A descriptive study of campus safety issues and self-reported campus victimization among male and female college students. *Journal of criminal justice education, 18*(2), 191-208.

Johnson, E. C. (2006). Security awareness: switch to a better programme. *Network security, 2006*(2), 15-18.

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286-290). IEEE.

Khan, B., Alghathbar, K. S., & Khan, M. K. (2011a). Information security awareness campaign: An alternate approach. In Kim, T., Adeli, H., Robles, R.J., & Balitanas, M., (Eds.), *Information Security and Assurance—ISA* (pp. 1-10). Springer.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011b). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, 5*(26), 10862-10868.

Kline, R. B. (2011). Convergence of structural equation modeling and multilevel modelling. In Williams, M., & Vogt, W.P. The SAGE Handbook of Innovation in Social Research Methods (pp. 562-589). Sage Publications.

Kruger, H.A., & Kearney, W.D. (2006). A prototype for assessing information security awareness, *Computers & Security, 25*, 289-296.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

Miller, T.E., Booraem, C., Flowers, J.V., & Iversen, A.E. (1990). Changes in knowledge, attitude, and behavior as a result of a community-based AIDS prevention program, *AIDS Education and Prevention, 2*(1), 12-23.

Muthén, L., & Muthén, B. (2017). *Mplus user's guide (Version 8.0).* Muthén & Muthén.

Newbould, M., & Furnell, S. (2009, December). Playing Safe: A prototype game for raising awareness of social engineering. In : *Australian Information Security Management Conference* (p. 4).

Parsons,, K., McCormac A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), *Computers & Security, 42*, 165-176.

Ponnet, K. (2014). Financial Stress, Parent Functioning and Adolescent Problem Behavior: An actor–Partner Interdependence Approach to Family Stress Processes in Low-, Middle-, and High-Income Families. *Journal of youth and adolescence, 43*(10), 1752-1769.

Regan, D. T., & Fazio, R. (1977). On the consistency between attitudes and behavior: Look to the method of attitude formation. *Journal of experimental social psychology, 13*(1), 28-45.

Rosenbloom, T., Haviv, M., Peleg, A., & Nemrodov, D. (2008). The effectiveness of road-safety crossing guards: Knowledge and behavioral intentions. *Safety Science, 46*(10), 1450-1458.

Sas, M., Reniers, G., Hardyns, W., & Ponnet, K. (2019). The impact of training sessions on security awareness: Measuring the security knowledge, attitude and behaviour of employees. *Chemical Engineering Transactions, 77*, 895-900.

Schokkenbroek, J., Sas, M., Ponnet, K., & Hardyns, W. (2020). Seksuele intimidatie in (dating-) relaties en de publieke ruimte: een vergelijking tussen twee survey-onderzoeken bij Vlaamse universiteitsstudenten. *Panopticon, 41*(1), 99.

Shaftel, J., & Shaftel, T.L. (2005). The influence of effective teaching in accounting on student attitudes, behavior, and performance, *Accounting Education, 20*(3), 231-246.

Shaw, R.S., Charlie, C.C., Harris, A.L., & Huang, H.J. (2009). The impact of information richness on information security awareness training effectiveness, *Computers & Education, 52*, 92-100.

Singh, A. (2009). Oral health knowledge, attitude and practice among NCC Navy Cadets and their correlation with oral hygiene in south India. *Oral health & preventive dentistry, 7*(4), 363.

van der Linden, S. (2012, July 3-6). *Understanding and achieving behavioural change: towards a new model for communicating information about climate change*. International workshop on psychological and behavioural approaches to understanding and governing sustainable Tourism Mobility, Freiburg, Germany.

Villa, V., Reniers G.L.L., & Cozzani V. (2016). Application of cost-benefit analysis for the selection of process-industry related security measures, *Chemical engineering transactions, 53*, 103-108.

Wahyudiwan, D. D. H., Sucahyo, Y. G., & Gandhi, A. (2017). Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In *Proceedings of the 3rd International Conference on Science in Information Technology* (pp. 654-658). IEEE.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640.