Journal of Global Information Management
Volume 27 • Issue 2 • April-June 2019

SETA and Security Behavior:

Mediating Role of Employee Relations, Monitoring, and Accountability

Winfred Yaokumah, Pentecost University College, Accra, Ghana

Daniel Okyere Walker, Pentecost University College, Accra, Ghana

Peace Kumah, Ghana Education Service, Accra, Ghana

ABSTRACT

This article contends that information security education, training and awareness programs can improve employee security behavior. Empirical studies have analyzed the direct effects of employee security training on security behavior without taking into account the mediating role of employee relations, monitoring, and accountability. Based on employee relations and accountability theories, this study proposes and tests a causal model that estimates the direct effect of employee security training on security behavior as well as its indirect effects as mediated by employee relations, monitoring, and accountability. The empirical analysis relies on a survey data from a cross section of employees from five major industry sectors and a structural equation modeling approach via SmartPLS 3.0. The results show that employee security training has indirect and significant effects on security behavior through its influence on employee relations, monitoring, and accountability. However, the result does not indicate direct and significant effect of security training on employee security behavior.

KEYWORDS

Accountability, Employee Relations, Information Security, Monitoring, Security Behavior, Security Education

INTRODUCTION

Organizations rely on information systems to enhance productivity and performance, thereby gaining competitive advantage and achieving strategic goals. Users of information systems are, however, prone to intentional and unintentional security risks. Users tend to be the major contributing factor in many information security breaches (Abawajy, 2014). As such, an increasing amount of attention is being paid to the human side of information security (Marett, 2015). According to Ponemon Institute (2012), employees are the main causes of many data breaches in organizations. Information security breaches often occur in organizations due to employees' ignorance or careless behaviors (Abawajy, 2014). For instance, employee negligence or maliciousness account for 78% of data breaches in organizations (Ponemon Institute, 2012). As a result, organizational leaders are seeking behavioral

DOI: 10.4018/JGIM.2019040106

solutions to effect a positive change in employee behavior toward the security of information resources (Pattinson et al., 2016).

An important aspect of managing employee security behavior in organizations is through security education, training, and awareness. Information security education is the organizational effort at making employees aware of the security environment, policies, and security manuals of the organization (D'Arcy et al., 2009). A growing body of evidence suggests that information security training can be used to improve employee information security behavior (Chen, Ramamurthy & Wen, 2015; Helkala & Bakås, 2014; Tsohou et al., 2015). The main reason organizations provide security education, training, and awareness programs is to change employees' behavior and to reduce employees' undesirable security behavior toward organizational information resources (Abawajy, 2014). Through the use of effective training techniques, employees can be educated on how to make safe information security decisions (Kennedy, 2016).

Employee information security education, training and awareness programs and security behavior continue to be strong themes in the human aspects of information security literature (Boss et al., 2015; Chu & Chau, 2014; Pattinson & Anderson, 2007). However, little attention is being paid to human factors that can influence employee security behavior. Many organizations have established SETA and security monitoring programs to safeguard information resources (Chen, Ramamurthy & Wen, 2015). But the current methods of training employees about information security are apparently failing as the number of employee-related breaches is increasing each year (Kennedy, 2016). Lacey (2010) believes that lack of proper training and supervision are the contributing factors behind many information security breaches. However, Slusky and Partow-Navid (2012) argue that failure of employees to comply with security measures is not due to lack of security training and awareness. Even individuals with security knowledge are unable to draw the necessary conclusions about digital risks when browsing the web (Bennett & Bertenthal, 2016). Thus, there is a significant gap between employee information security training and security behavior (Stanciu & Tinca, 2016). Parsons et al. (2014) suggest that organizations should assess the impact of information security training programs on addressing organizational information security challenges.

According to Meso, Ding and Xu (2013), there is the need for a broader and better training of employees to be able to effectively deal with information security risks. Organizations need to incorporate into security education, training and awareness programs three key interventions (mediators), including establishing closer employee relations, monitoring employees' security behavior, and making employees accountable for security. Employee relations, monitoring, and accountability are core human resource (HR) management activities that can improve employee behavior. Human resource management plays an important role by coordinating the activities (policies and procedures) of the organization, which are consistent with the overall business goals and objectives. Employee relations are identified as social exchange relationship between an employer and the employees in the organization (Sivalogathasan & Hashim, 2013). Monitoring is the activities undertaken by one party to gain information about another party's level of compliance (Ferrin et al., 2007) to specified requirements. Accountability is a "process in which a person has a potential obligation to explain his or her actions to another party who has the right to pass judgment on those actions and to administer potential positive or negative consequences in response to them" (Vance, Lowry & Eggett, 2015, p. 347).

Based on the accountability and employee relations theories, this study develops and examines the influence of employee information security training on employee information security bahavior mediated through the organizational security activities of creating employee relations, security monitoring, and accountability. Yaokumah and Kumah (2018) explore the effect of security policy on compliance. D'Arcy, Hovav, and Galletta (2009) investigate perceived certainty and severely of sanctions as the major mediating factors between security policies; security education, training, and awareness (SETA) programs; computer monitoring, and information systems misuse intention. Both certainty and severely of sanctions explain only 30% of the variations in information systems misuse intention. This suggests that other factors can account for information systems misuse intention, and for that matter employee security behavior. Thus, the extent of the impact training, employee relations, monitoring, and accountability have on improving employee information security behavior has not been adequately researched from theoretical and empirical perspectives. For improving employee information security behavior, this paper proposes that employee relations, monitoring, and accountability should directly improve employee information security behavior or act as the vital link or mediators between employee information security training and the employee information security behavior.

BACKGROUND AND HYPOTHESES

Theoretical Background and Conceptual Model

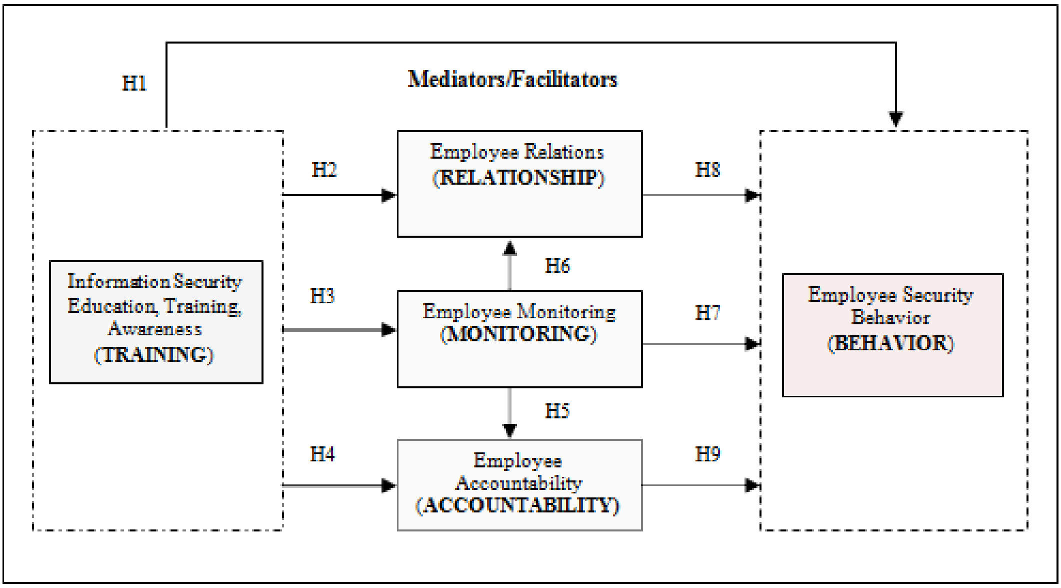
Two theories were used in this study to explain how security training could improve security behavior: the accountability theory (Vance, 2013; Vance, Lowry & Eggett, 2015) and the employee relations theory (Coleman, 2017; Ross & Bamber, 2009; The Great Soviet Encyclopedia, 1979). Accountability theory comprised of four main constructs: identifiability, expectation of evaluation, awareness of monitoring, and social presence (Vance, Lowry & Eggett, 2015). Identifiability is a person's knowledge that his activities could be linked to him and thus revealed his/her true identity (Vance, Lowry & Eggett, 2015). Expectation of evaluation is the belief that one's "performance would be assessed by another according to some normative ground rules and with some implied consequences" (Lerner & Tetlock, 1999, p. 255). Awareness of monitoring is a user's state of active cognition that his or her system-related work is being monitored (Vance, Lowry, & Eggett 2015). Social presence is the awareness that there are other users in the system (Vance, Lowry, & Eggett 2015).

The employee relations theory proposed that humans are socio-psychological beings and have moral qualities - including goals, motivation, and values (The Great Soviet Encyclopedia, 1979). To increase productivity, a method of dealing with employees should take into consideration human moral needs. The theory focused on factors fostering a positive or negative attitude toward employees, the influence of the work group on the individual, the effectiveness of forms and methods of supervision, and the improvement of conditions for work, relaxation, and leisure (The Great Soviet Encyclopedia, 1979). The unitarist theory of employee relations emphasized co-dependency of employers and employees in which the organization is viewed the as an integrated, friendly and collaborative whole (Coleman, 2017). The employers and employees regard the organization as a happy family with a common purpose and mutual co-operation (Ross & Bamber, 2009) towards the achievement of organizational goals. Unitarist focussed on increased employee loyalty in the attainment of organizational goals.

Based on these theories, the current study proposed that an employee with the knowledge that his or her identity could not be hidden and his activities are being monitored would be more likely to engage in desirable security behavior. The fundamental assumption in our theoretical use of accountability theory is that accountability and monitoring would change employees' behavior toward information security policies. For employee relations theory, our assumption is that when employees' moral needs are addressed there would be the tendency of positive behavior toward information security. Our conceptual model proposed that employee' information security training, mediated by employee accountability, employee relations, and employee monitoring would improve employee desirable information security behavior (see Figure 1). The conceptual model suggested that employees who had security training would have increased perception of accountability, which in turn would influence their behavior toward information security.

Given the above explanation of the mediating effect of accountability, employee relations, and employee monitoring, the study posited that employees who had security training would have desirable security behaviors that would improve information security. Moreover, the model suggested

Figure 1. Conceptual model of employee security training on security behavior



that security training would directly improve employees' security behavior without the mediators (accountability, employee relations, and employee monitoring).

Employee Security Behavior

Literature on employee security behavior provided diverse and sometimes inconsistent findings. A recent study suggested that the level of user security behavior is low (Das & Khan, 2016). According to Safa et al. (2015), user security behavior such as user negligence, ignorance, lack of awareness, mischievous, apathy and resistance were usually the reasons for security breaches. Applying structural equation modelling techniques, Safa et al. (2015) found that information security awareness and attitude towards information security had positive effect on users' behavior, while perceived behavioral control did not significantly affect user behaviour. However, in an earlier and a related study, Zhang et al. (2009) examined the factors affecting end-user security behavior and found that perceived behavioral control had significant impact on intention to comply with security policy. Chen and Li (2014) distinguished between formal control (deterrence and punishment) and informal control (misperception of social norms). Formal control mechanisms effectively reduced employee's omission behaviors whereas informal control mechanisms contributed to the dissemination of omission behaviors among employees (Chen & Li, 2014). Considering these contradictory findings, the current study proposed that security training, monitoring, accountability, and employee relations could have significant influence on employee security behavior.

Security Training, Education, Awareness

Information security education, training, and awareness are three inter-related activities organizations employ to foster employees' understanding and compliance with information security policies and guidelines. According to NIST Special Publication 800-16 (1998), user education, training, and awareness are important aspects when addressing human factors and competencies in information security. Security education is a means of providing adequate information security awareness amongst employees (Kaspersky & Furnell, 2014). Information security awareness is the level of comprehension that users have about the importance of information security best practices (Abawajy, 2014). Security awareness is a primary pillar of security for any organization to avoid major security breaches (Dahbur, Bashabsheh, & Bashabsheh, 2017) and the most cost-effective means of enhancing security (Albrechtsen & Hovden, 2010).

Previous studies reported inconsistent findings with regard to whether security training and awareness programs have direct influence on employee security behavior. For example, Zhang and McDowell (2009) noted that security education alone is of little value to changing user behavior. However, according to McCrohan, Engel and Harvey (2010), information security awareness and training initiatives would improve security behavior. McCrohan, Engel, and Harvey (2010) found that cyber threat education and awareness intervention could change user security behavior. Helkala and Bakås (2014) also demonstrated that education is necessary in changing people's security behaviour. This suggested that the more information security knowledge employees' have, the better their behavior toward information security. Based on this notion the following hypothesis was proposed:

Hypothesis 1: There is a direct, positive, and significant relationship between employee information security training, education and awareness (TRAINING) and employee's information security behavior (BEHAVIOR).

Moreover, the dependency on humans in protecting information resources necessitated an information security awareness program to make people conscious of their roles and responsibilities toward information security (Kruger, Drevin, & Steyn 2010). An important aspect of security training is to made employee responsible and accountable for security. Kruger, Drevin, and Steyn (2010) found a significant relationship between knowledge of concepts and behavior. But McCrohan, Engel and Harvey (2010) doubted whether simple admonition of security threats can change behavior. A global security survey confirmed that security education, training and awareness programs are not working as well as they could be (Tsohou et al., 2012), hence the need for accountability, monitoring, and employee relations.

Accountability theory proposed that user's active cognitive ability is enhanced when they are made aware that their activities are being monitored (Vance, Lowry, & Eggett 2015). Employees monitoring produces fruitful outcomes when the employee is aware that they are being monitored (Vance, Lowry, & Eggett 2015). Thus, when employees participated in security training and awareness programs, they should be monitored to ascertain whether the training goals have been achieved. With respect to the relationship between training and accountability, Burley (2017) noted that training has significant impact on employee accountability. For example, a well-designed security training program would include how the employee should create an action plan. This would include how to apply what has been learned when the employee returned to work. Based on these concepts, the following hypotheses were put forth:

Hypothesis 2: There is a positive and a significant relationship between employee information security training, education and awareness (TRAINING) and improvement in employee relations (RELATIONSHIP).

Hypothesis 3: There is a positive and a significant relationship between employee information security training, education and awareness (TRAINING) and improvement in information security monitoring (MONITORING).

Hypothesis 4: There is a positive and a significant relationship between employee information security training, education and awareness (TRAINING) and employee information security accountability (ACCOUNTABILITY).

Employee Monitoring

Systematic monitoring and evaluation of employees' security behavior are of great importance (Albarrak, 2011). Employee monitoring is an important component of organizational efforts to maintain employee productivity and to manage employee misconduct (Ford et al., 2015). Lack of security evaluation method might expose organizations to several risky situations (Rigon et al., 2014). To enhance employee performance, many organizations are increasingly using electronic performance monitoring systems (Bhave, 2014). Technology allows for extensive monitoring of employees with video, phones, internet, social media, application logs, and other methods with which employee behaviors can be tracked (Ford et al., 2015). Another emerging form of employee monitoring is through global positioning system (GPS) (Bhave, 2014). However, employee monitoring has been contended as it could be considered a breach of privacy (Towns & Cobb, 2012) and close monitoring might result in negative employee reactions (Jeske & Santuzzi, 2015). Similarly, Whalen and Gates (2010) suggested that voluntary monitoring should be made a condition of employment in order to yield positive results.

One key construct of accountability theory is social presence. Social presence suggested that users are aware of the presence of other users in the system (Vance, Lowry & Eggett, 2015) who might observe their activities. The awareness that others are observing (monitoring) their activities might compel employees to comply with policies. Monitoring could influence accountability in two ways. Dishonest employees might fear disciplinary actions and those complying with security requirements might expect acknowledgment. Also, employee relations theory focused on meeting the social and psychological needs of the employees. Through monitoring, an organization would ascertain the needs of the employees. Knowing the needs and addressing those needs would create closer employee relations (Coleman, 2017).

Moreover, when people are being monitored they would put up acceptable behavior (Vance, Lowry, & Eggett 2015). Monitoring employees gives the organization the opportunity to watch for mistakes and errors. A monitoring system enables the organization to identify strength and weaknesses of employees on regular bases. Employees' strength and weaknesses would be exposed. When employees' strengths are acknowledged their behavior toward work might change (Ross & Bamber, 2009). Also, pointing out employees' weaknesses and mistakes might improve security behaviors (Ford et al., 2015). A previous study found that a frequent supervisory use of electronic performance monitoring was associated with better task performance and organizational citizenship behaviors (Bhave, 2014). Thus, the following hypotheses were proposed:

Hypothesis 5: There is a positive and a significant relationship between security monitoring (MONITORING) and employee information security accountability (ACCOUNTABILITY).

Hypothesis 6: There is a positive and a significant relationship between security monitoring (MONITORING) and improvement in employee relations (RELATIONSHIP).

Hypothesis 7: There is a positive and a significant relationship between security monitoring (MONITORING) and employee's information security behavior (BEHAVIOR).

Employee Relations

Gennard and Judge (2002) defined employee relations as the study of rules, regulations, and agreements which are employed to manage employees individually and collectively with the aim of gaining employee commitment to the realization of an organization's goals and objectives. To ensure security in information systems, it is necessary to address human behavior and organisation-related issues (Trcek et al., 2007). Employee relations are human resource strategies designed to manage relationships between employers and employees (Andrea Rea, n.d). Employee relations programs are aimed at providing fair and consistent treatment to all employees, prevent and resolve problems arising from situations at work, and addressing issues affecting employees such as pay and benefits, supporting work-life balance, and safe working conditions (Andrea Rea, n.d). Employee relations programs ensure the most effective use of employees to accomplish the organization's objectives (Andrea Rea, n.d.). The strength of an employee's identification with and involvement in an organization has a significant effect on behavioral intention (Lebek et al., 2014). This is because disgruntled employees can expose valuable business trade secrets or engage in corporate espionage or sabotage (Ford et al., 2015). The social exchange relationship between the employer and the employee determined the employee work outcomes (Sivalogathasan & Hashim, 2013). Therefore, employee relations could influence employee security behavior. The following hypothesis was proposed:

Hypothesis 8: There is a positive and a significant relationship between employee relations (RELATIONSHIP) and employee's information security behavior (BEHAVIOR).

Employee Accountability

While organizations invest significant funds to ensure that buildings and computing systems are secured, the responsibility that the employees have for maintaining information systems security is often overlooked (Hazari, Hargrave & Clenney, 2008). Responsibility and accountability could change the behaviors of users who accesses systems and applications to perform tasks. Accountability is seen as a quality in which a person displays a willingness to accept responsibility (Vance, 2013). It is regarded as a process in which a person has a potential obligation to explain his or her actions to another party who has the right to pass judgment on the actions as well as to subject the person to potential consequences (Vance, 2013). One promising means of modifying the behaviors of employees is through accountability (Tadmor & Tetlock, 2009). Accountability theory suggested that a person's expectation that he or she would be held accountable for an action or inaction reduces the likelihood of behaving in socially unacceptable way (Sedikides et al., 2002). Zaman and Saif (2016) found that perceived accountability has a significant positive relationship with job performance as it could change the behaviors while performing tasks. According to Styles and Tryfonas (2009), employees are responsible for and are duty-bound to secure computing resources they operate and interact with. Based on this notion, the following hypothesis was proposed:

Hypothesis 9: There is a positive and a significant relationship between employee information security accountability (ACCOUNTABILITY) and employee's information security behavior (BEHAVIOR).

METHODOLOGY

The accessible population was the organizations located within Greater Accra municipal area of Ghana. A total of 49 organizations were selected from within industry sectors involving 650 respondents (15 participants from each organization within the 5 main industry sectors and 80 participants from other organizations) were invited to take part in the study. Details of the sample includes: (a) ten (2 public and 8 private) universities (150 participants); (b) ten licensed banks (150 participants); (c) six public utility companies (water, electricity, telecommunication) (90 participants); (d) seven government public service institutions (105 participants); (e) five healthcare institutions (75 participants); and (f) eleven others (IT, Manufacturing, Oil and Gas, etc.) (80 participants). These organizations were selected because they are mandated by law and regulations such as the Electronic Transactions Act 772 (2008) and Bank of Ghana Act 612 (2002) (Bank of Ghana, 2011) to maintain the confidentiality and integrity of customers' information.

A simple random sampling method was employed to select participants from the organizations. A structured questionnaire was used to gather information from the respondents. The questions on the questionnaires were modified such that it could be relevant to the context of the study. The modification was done as a result a field test conducted, with comments received from a panel of experts (two information security practitioners, two HR practitioners, and one senior academic faculty) to establish the validity the instrument. The questionnaires were then self-administered to the respondents through post and by email.

The first part of the questionnaire was designed to reflect the profile of the respondents. The second part contained the questions which reflected four independent (exogenous) latent variables and one dependent (endogenous) variable. The questions were 40 indicator variables from the five constructs (see Figure 2 and Table 2). The questionnaire comprised of 11 measurement items relating to *information security education, training and awareness* (Hwang et al., 2017), *5 items on employee relations* (Bumgarner & Borg, 2007), 4 items on *security monitoring* (Al-Omari, El-Gayar & Amit Deokar, 2012), 11 items on *accountability* (Bumgarner & Borg, 2007), and 9 items on *security behavior* (Siponen et al., 2014). Ratings were done on a Likert scale of 1 (strongly disagree) to 5 (strongly agree). Respondents were asked to rate the extent to which each of the variables that could influence their behavior toward information security.

Out of the 650 questionnaires sent to the respondents, 318 were completed and used in the data analysis. This represented a response rate of 48.9 percent. Table 1 showed the sample characteristics of the respondents. The Partial Least Square (PLS) structural Equation Modelling (SEM) path modeling was adopted in analyzing the data. The study first analyzed the measurement model to test the reliability and validity of the measurement model. SmartPLS 3.0 (Ringle, Wende, & Becker, 2015) was used to perform path analysis and test the research hypotheses. Moreover, the study used bootstrapping with 5000 re-samples (Goodhue, Lewis, & Thompson, 2007) for obtaining t-statistics between constructs of the research model.

DATA ANALYSIS

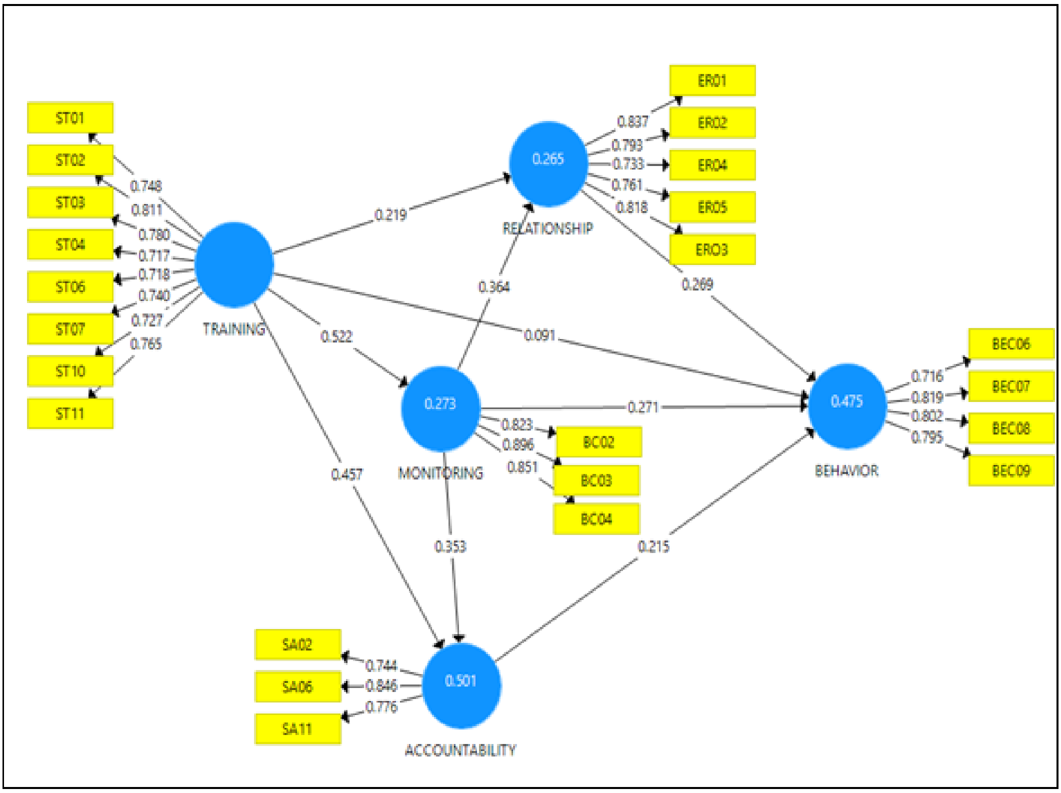
This study employed a two-step structural equation modelling (SEM) approach: a) assessment of the measurement model and b) the analysis of the structural model. The assessment of the measurement model measured the adequacy of the model with respect to the relationship between the latent variables and the items measuring them (Hair et al., 2014). Thus, the measurement model was used to confirm

Table 1. Sample characteristics

Respondents	No. of Questionnaire Received	Percent (%)
Industry Sector		
Education Institution	74	23.3
Public Utility Company	38	11.9
Financial Institution	68	21.4
Government	36	11.3
Health Care	38	11.9
Others (IT Companies, Oil and Gas, Manufacturing)	64	20.1
Experience (Years)		
1-5	46	14.5
6-10	114	35.8
11-15	138	43.4
16-20	18	5.7
21 and above	2	0.6

N = 318

Figure 2. Structural model of security training on security behavior



the reliability and validity of the measures. The structural model was employed to determine the influence of employee security training on security behavior by testing a set of hypotheses.

Assessment of the Measurement Model

The assessment of the model was to ascertain the relationship between the constructs and their indicators. The assessment model was evaluated for the a) individual item reliability (factor loading), b) internal consistency reliability (composite reliability and Cronbach's alpha), and c) construct validity (convergent validity and discriminant validity).

The individual item reliability (factor loading) indicated the correlations of the items with their respective latent variables (Hulland, 1999). The standardized loadings were assessed in order to evaluate individual item reliability. The items with low loadings must be dropped and should not be used in further analysis as they provided very little explanatory power to the model and therefore biasing the estimates of the parameters linking the latent variables (Nunnally, 1978). For the cut-off point, a rule of thumb was to accept items with loadings of 0.7 or more (Fornell & Larcker, 1981). A loading of 0.7 indicated that about 50% of the variance in the observed variables was due to the latent variable (Hulland, 1999). According to Chin (1998), where scales were adapted from other settings, a loading of 0.5 might be used as the cut-off point (Chin, 1998). However, items with loadings of less than 0.4 (a threshold commonly used for factor analysis results) or 0.5 should be dropped (Hulland, 1999). In this study, all items having a loading less than 0.7 were dropped. Twenty items were used in the analysis of the structural model while the rest were dropped for not attaining the loadings cut-off point of 0.7.

Table 2. Factor loading

Constructs	Indicators	Loading > 0.7
SECURITY EDUCATION, TRAINING AND AWARENESS		
ST01	My organization provides employees with appropriate security education before giving them authorized access to the corporate network.	0.748
ST02	My organization provides employees with education on the proper usage of technologies associated with information.	0.811
ST03	My organization provides employees with proper security education on risks associated with internet usage.	0.780
ST04	Employees in my organization are made not to store passwords in insecure places.	0.717
ST06	My organization utilizes various communication methods in order to improve the information security awareness of employees.	0.718
ST07	My organization provides employees with education on their responsibility for information security exposure.	0.740
ST10	My organization provides education to promote employees' awareness of information security issues.	0.727
ST11	All employees are periodically tested on their knowledge of security procedures, including their knowledge of newly emerging threats.	0.765
EMPLOYEE MONITORING		
BC02	I am aware that my organization monitors any modification or altering of computerized data by employees	0.823
BC03	I am aware that my organization monitors employees' computing activities and conducts periodic audits to detect the use of unauthorized software on its computers.	0.896
BC04	I am aware that my organization reviews logs of employees' computing activities on a regular basis.	0.851
EMPLOYEE RELATIONS		
ER01	My organization makes fairness and good faith in the treatment of employees a priority.	0.837
ER02	My organization provides adequate mechanisms for employees to express their grievances without penalty and for them to see those grievances being conscientiously addressed.	0.793
ER03	My organization handles re-deployment/down-sizing in a manner that minimizes hostile feelings on the part of former employees.	0.818
ER04	My organization offers a procedure which would allow employees to report attempts by outsiders to extort their organization in circumventing security.	0.733
ER05	If an employee is going through a period of great difficulties in his or her personal life, there is a policy for temporarily reducing that employee's responsibilities for critical systems and access to critical systems.	0.761
ACCOUNTABILITY		
SA02	All employees are required to sign confidentiality and intellectual property agreements.	0.744
SA06	Information security policies defined the proper use of e-mail, internet access, and instant messaging by employees.	0.846
SA11	Employees are given adequate incentives to report security breaches and bad security practices.	0.776
INFORMATION SECURITY BEHAVIOR		
BEC06	I comply with information security policies (e.g. secure password, clear desk/screen policy, classification and handling of information).	0.819
BEC07	I assist others in complying with information security policies.	0.802
BEC08	I recommend that others comply with information security policies.	0.795
BEC09	I do not access social networking websites during work time.	0.716

Furthermore, the study ascertained the Cronbach's alpha and composite reliability scores to determine the reliability of the measured constructs (Fornell, & Larcker, 1981). Cronbach's alpha represented the coefficient of reliability (or consistency). It denoted how well a set of items (or variables) measured a single one-dimensional latent construct (Hair et al., 2011). Composite reliability (CR) score was considered superior to Cronbach's Alpha as it used the item loadings obtained within the theoretical model (Fornell, & Larcker, 1981). However, both composite reliability and Cronbach's Alpha could be acceptable with scores of 0.7 and above (Nunnally, 1978). Applying the benchmark of 0.7 for Cronbach's Alpha and composite reliability ((Nunnally, 1978), the five constructs (security training, employee relations, employee monitoring, accountability, security behavior) in this study exceeded the minimum requirements for reliability measures (Hair et al., 2014). Thus, all the constructs demonstrated acceptable level of reliability (see Table 3).

When multiple items were used to measure individual latent variables, attention should be paid not only to the reliability of the individual measurement items, but also to the extent to which the measures demonstrated convergent validity (Hulland, 1999). Convergent validity represented the measure of internal consistency. It was estimated to ensure that the items measure each latent variable it measured and not measuring another latent variable. The average variance extracted (AVE) (Fornell & Larcker, 1981) was used to assess the convergent validity of the latent variables. AVE measured the amount of variance that a latent variable captured from its measurement items relative to the amount of variance due to measurement errors (Hair et al., 2014). Fornell and Larcker ((1981) stated that AVE should be higher than 0.5. This meant that at least 50% of measurement variance was captured by the latent variables. In this study, the estimates of AVEs (Table 3) were above 50% for all the latent variables. After assessing the individual item reliability and convergent validity of the measurement model, the discriminant validity of the measurement was also evaluated. Discriminant validity indicated the extent to which a given latent variable was different from other latent variables in the model (Hulland, 1999).

To assess discriminant validity, two tests were conducted: a) analysis of cross-loadings and b) analysis of average variance extracted (AVE). The analysis of cross-loading was conducted by following the rule that items should have a higher correlation with the latent variable that they were supposed to measure than with any other latent variable in the model (Chin, 1998). Convergent validity was initially assessed through indicator reliability. The rule of thumb was that standardized indicator outer loadings must be 0.708 or higher (Hair et al., 2014). Two indicators were removed from accountability construct. All other indicators were above 0.708. The average variance extracted (AVE) was also a measure of convergent validity and it exceeded 0.60 for all the constructs in the model; the cut-off was 0.50 (Hair et al., 2014). The Fornell and Larcker (1981) criterion for assessing discriminant validity was applied. The squared interconstruct correlations were all below the construct AVEs, thus indicating discriminant validity. Finally, all indicator loadings were higher than their cross-loadings, providing further evidence that all the criteria for discriminant validity were met (Table 3).

Assessment of the Structural Model

On the basis of the analyzed results from the assessment of the measurement model, the questionnaire used was considered valid and reliable in assessing the model. Following, the quality of the structural model was assessed to determine its ability to predict endogenous constructs. This was achieved by using the cross-validated redundancy Q^2, coefficient of determination R^2 (Sarstedt et al., 2014; Urbach & Ahlemann, 2010), and the strength of the path coefficients (Hair et al., 2011). The Stone-Geiser Q^2 (Geisser, 1975; Lee et al., 2011) assessed the predictive accuracy of the proposed model (Hair et al., 2011; Hair et al., 2012). It measured how accurately the PLS-SEM model predicted the observed data points (Hair et al., 2014). The Q^2 was a nonparametric measure obtained using the blindfolding procedure with values larger than zero indicating predictive relevance (Hair et al., 2011). SmartPLS automatically provided the Q^2 value for each endogenous latent variable. The analysis yielded a Q^2 value of 0.289 for accountability, 0.149 for employee relations, 0.188 for monitoring, and 0.272 for

Table 3. Results of the measurement model evaluation

Construct		1	2	3	4	5	AVE (> 0.5)	CA (> 0.7)	CR (> 0.7)
1	ACCOUNTABILITY	**0.790**					0.624	0.701	0.833
2	BEHAVIOR	0.584	**0.784**				0.615	0.790	0.864
3	MONITORING	0.591	0.575	**0.857**			0.734	0.818	0.892
4	RELATIONSHIP	0.560	0.556	0.479	**0.789**		0.623	0.849	0.892
5	TRAINING	0.641	0.480	0.522	0.410	**0.752**	0.565	0.890	0.912

Note: Discriminant validity - Square roots of average variances extracted (AVEs) shown on diagonal in bold. CR – Composite reliability, CA – Cronbach's Alpha.

security behavior (Table 4). Therefore, each factor had a high predictive capability in predicting employee information security behavior.

The R^2 denoted the measure of the variance of each of the endogenous constructs explained by exogenous constructs, thus measuring the predictive power of the exogenous constructs (Chin, 2010; Urbach & Ahlemann, 2010). The R^2 measure ranged from 0 to 1, with values closer to 1 indicating greatest degree of predictive power. For variance explained by the endogenous variables to have practical and statistical significance, it was recommended that R^2 values be greater than 0.10 (Hair et al., 2014). As a guideline for assessing R^2, 0.67, 0.33 and 0.19 represented substantial, moderate, and weak respectively (Lee et al., 2011). A more stringent assessment with R^2 value of 0.75 representing substantial; value of 0.5 and 0.25 represented moderate and weak R^2 respectively (Hair et al., 2014).

From Table 4 and Figure 2, R^2 for accountability was 0.501, indicating that about 50.1% of the variance in accountability was explained by security training and monitoring. The R^2 for monitoring was 0.273, revealing that about 27.3% of the variance in monitoring was accounted for by security training. The R^2 for employee relations was 0.265, showing that about 26.5% of the variance in employee relations were accounted for by security training and monitoring. Finally, the R^2 for employee security behavior was 0.468, revealing that about 46.8% of the variance in employee security behavior was accounted for by employee relations, security training (not significant), monitoring, and accountability. Consequently, the results were a sign of adequate model fit between the proposed research model and the empirical data.

Hypotheses Testing

Table 5 and Figure 2 disclosed the standardized path coefficients of the structural model under investigation. The path coefficients indicated the strength of the direct relationship between constructs. Security training has no direct and significant influence on security behavior ($\beta_1 = 0.091, p = 0.\ 0.065$), indicating that H1 was not supported. Security training, however, had positive and significant influence on employee relations (β_2 = 0.219, <0.001), monitoring (β_3 = 0.522, <0.001), and accountability

Table 4. R^2 and Q^2 coefficients

Constructs	R^2	R^2 Adjusted	Q^2
ACCOUNTABILITY	0.501	0.498	0.289
MONITORING	0.273	0.270	0.188
RELATIONSHIP	0.265	0.260	0.149
BEHAVIOR	0.475	0.468	0.272

Table 5. Hypotheses testing results

Hypotheses		Path Coefficients (β)	Sample Mean (M)	Standard Deviation (*SD*)	Effect Size (f^2)	t-Statistics	*p*-Values	Result
H1	TRAINING -> BEHAVIOR	0.091	0.092	0.049	0.009	1.852	0.065	Not Supported
H2	TRAINING -> RELATIONSHIP	0.219	0.223	0.056	0.048	3.904	0.000	Supported
H3	TRAINING -> MONITORING	0.522	0.527	0.035	0.375	14.788	0.000	Supported
H4	TRAINING -> ACCOUNTABILITY	0.457	0.452	0.051	0.304	8.973	0.000	Supported
H5	MONITORING -> ACCOUNTABILITY	0.353	0.357	0.053	0.181	6.620	0.000	Supported
H6	MONITORING -> RELATIONSHIP	0.364	0.370	0.061	0.131	5.984	0.000	Supported
H7	MONITORING -> BEHAVIOR	0.271	0.272	0.064	0.082	4.252	0.000	Supported
H8	RELATIONSHIP -> BEHAVIOR	0.269	0.271	0.057	0.090	4.722	0.000	Supported
H9	ACCOUNTABILITY -> BEHAVIOR	0.215	0.213	0.073	0.039	2.938	0.003	Supported

($\beta_4 = 0.457$, $p < 0.001$); inferring that hypotheses H2, H3 and H4 were all supported. Moreover, employee monitoring had a positive and significant influence on accountability ($\beta_5 = 0.353, p < 0.001$), employee relations ($\beta_6 = 0.364, p < 0.001$), and on security behavior ($\beta_7 = 0.271, p < 0.001$); inferring that hypotheses H5, H6 and H7 were also supported. Finally, employee relations had positive and significance influence on security behavior ($\beta_8 = 0.269$, $p < 0.001$), showing support for hypothesis H8. Also, accountability had a positive and significant influence on employee security behavior ($\beta_9 = 0.215, p < 0.001$), supporting H9. As could be observed from Figure 2, the paths through the mediators (employee relations, monitoring, and accountability) showed the highest significant path coefficients to security behavior. This suggested that employee relations, monitoring, and accountability played a vital role between security training and improvement in employees' security behavior.

The effect size (f^2) was another measure that verified whether the effects indicated by the path coefficients were low (0.02), moderate (0.15), or high (0.35) (Cohen, 1988). Effect size showed whether the effect of a specific independent latent variable on a dependent latent variable was substantial (Chin, 2010). Table 5 indicated that the effect size of security training on monitoring was the highest 0.375, whereas that of security training on security behavior was the lowest (0.009). Other effect sizes ranged between low and moderate.

DISCUSSION

Previous research emphasized the use of SETA programs to improve employee security behavior (Helkala, & Bakås, 2014; McCrohan, Engel & Harvey, 2010). Regarding the direct effect of SETA on security behaviour, our current study did not find direct and significant effect of SETA on security behavior. This contradicted earlier findings that SETA programs were the most effective means of influencing employee security behavior (Kennedy, 2016; Mani, Choo, & Mubarak, 2014). The results of the current study showed no direct and significant effect of employee security education, training and awareness on improving employee security behavior. This is in consonance with an earlier study that did not find a significant change in users' security behavior between those who had completed a training program and those who did not have any security training on information security (Chin, Etudo & Harris, 2016). Thus, security education alone is of little value to changing user behavior (Zhang & McDowell, 2009). This suggested that security education, training and awareness programs are least effective in themselves if organizations fail to include other mediating factors.

With respect to the effect of the mediators (employee monitoring, employee relations, and accountability) on security behavior, our results found that employee relations, employee monitoring, and accountability were the most important factors that could shape employee behavior toward information security. This was clearly demonstrated in the total effects they had on security behavior (Table 5). In order of the predicative values of their influence on security behavior were: employee monitoring, employee relations, and accountability. Thus, in particular, employee monitoring played the most crucial role in enhancing employee behaviour, followed by employee relations. Evidently, the pathway from security training, monitoring, employee relations, through to security behavior appeared to be the most significant based on their path coefficients. Thus, security education, training and awareness programs should include stronger employee monitoring system. Contrary to the argument that employee would object to monitoring (Jeske & Santuzzi, 2015), monitoring can create employee relations which would then improve security behavior. As can be observed from the findings, security monitoring has direct influence on employee relations which then influence employees' desirable security behavior. Much attention has not been paid to employee relations in earlier studies. However, its influence on employee behavior is crucial in protecting information resources. For example, disgruntled employees can expose valuable business trade secrets or engage in corporate espionage or sabotage (Ford et al., 2015). Accordingly, Sivalogathasan & Hashim (2013) believed that the social exchange relationship between the employer and the employee would determine the employee work outcomes.

Though significant, accountability contributed the least to improving employee security behavior among the three mediators. Overall, the significant influence of employees' accountability on employees' behavior toward information security offered another important opportunity for information security management practices. Although earlier studies have reported that accountability and deterrent factors might not be very effective in altering employee behavior (Siponen & Vance, 2010; Hu et al., 2011), our results suggested that when employees undergo security training and are made accountable, their security behaviors improve. Therefore, accountability plays a crucial role in making employees behave in acceptable manner (Tadmor & Tetlock, 2009). Accordingly, similar to a previous finding (D'Arcy, Hovav, & Galletta, 2009), accountability is required to enhancing employee security behavior. Thus, organizations should also pay attention to accountability when implementing security training programs.

CONCLUSION

The current study examined the extent of the influence information security education, training and awareness (SETA) programs has on employee information security behavior. The study argued that failure of employees to apply with security measures is not mainly due to lack of security training and awareness (Slusky & Partow-Navid, 2012). For organizations to improve employees' security behavior, organizational leaders should not only focus resources on security training programs, but also pay an equal attention to creating employee relations, monitoring employee security behavior, and make employee accountable for security behavior. SETA made the most significant impact on security behavior through monitoring, followed by employee relations, and then accountability. This suggested that security training designers should implement security monitoring systems after security training has been conducted. This would help evaluate any changes in employees' security behavior. Information gathered on employees should provide the bases for accountability in the form of reward and punishment. However, our findings revealed significant role of employee relations on security behavior. Thus, instead on melting out instant punishment as a way of accountability, HR managers should develop policies to address employees' social and moral needs.

This research fills an important gap in the literature on employees' information security behavior from two perspectives: theoretical and methodological. This study developed and empirically tested a five-construct model that examined the influence of employee information security training experience on employees' information security behavior, mediated via employee relations, monitoring, and accountability. From theoretical perspective, the study brought together two theories - the employee relations theory and the accountability theory - that have not been combined in the context of employee information security behavior. The study tested the model using partial least squares structural equation modelling (PLS-SEM).

From methodological perspective, prior studies related to employee information security behavior focussed on univariate quantitative approach and qualitative research methods. Multivariate techniques are recommended to encourage diverse approaches, along with methodological rigor. The result provides one of the few empirical validations of employee security behavior. It recognizes its multidimensional nature as conceptualized through security training, employee relations, monitoring, and accountability. In particular, it extends security behavior research by considering the influence of employee relations, monitoring and accountability drawn from the organizational behavior theories. The findings of this study also have important implications for information security program management practices. Management could use the finding of this study as a guide in developing and implementing information security policy by paying critical attention not only to security training, but also putting in place monitoring, accountability, and employee relations to improve employee security behavior.

This study is limited to a developing country. There would be the need to test the model in different contexts for possible refinement of the model, thus providing a better understanding of the influence of security training on employee security behavior in different settings. Future work would consider important-performance analysis to identify the key indicators for improving employee security behavior, which would be beneficial for management decision-making. Also, the current study did not consider the influence of the control variables - industry sector differences and the experience of the participants. Information security practices might differ from one industry to the other due to various laws and regulation compliance. Therefore, future work would examine different structural models for each industry sector and compare the results. Multi-group analysis would provide useful information by obtaining differences and similarities in inter-sector security practices.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. doi:10.1080/0144929X.2012.708787

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. In *45th Hawaii International Conference on System Sciences*. doi:10.1109/HICSS.2012.516

Albarrak, A. I. (2011). Evaluation of Users Information Security Practices at King Saud University Hospitals. *Global Business & Management Research*, *3*(1).

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: An Intervention Study. *Computers & Security*, *29*(4), 432–445. doi:10.1016/j.cose.2009.12.005

Andrea Rea (n.d) What Is Employee Relations? - Definition & Concept Retrieved from http://study.com/academy/lesson/what-is-employee-relations-definition-lesson-quiz.html

Bank of Ghana. (2011). Preamble for the Legal and Regulatory framework. Retrieved from https://www.bog.gov.gh/supervision-a-regulation/regulatory-framework

Bhave, D. P. (2014). The Invisible Eye? Electronic Performance Monitoring and Employee Job Performance. *Personnel Psychology*, *67*(3), 605–635. doi:10.1111/peps.12046

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Management Information Systems Quarterly*, *39*(4), 837–864. doi:10.25300/MISQ/2015/39.4.5

Bumgarner, J., & Borg, S. (2007). US-CCU Cyber-Security Check List (2007). US-CCU (Cyber Consequences Unit) Cyber-Security Check. Retrieved from www.usccu.us

Burley, K. (2017). Employee Accountability Training Activities. Retrieved from https://bizfluent.com/info-8407188-employee-accountability-training-activities.html

Chen, H., & Li, W. (2014). Understanding organization employee`s information security omission behavior: An integrated model of social norm and deterrence. In *PACIS 2014 Proceedings*. Retrieved from http://aisel.aisnet.org/pacis2014/280

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. doi:10.1080/08874417.2015.11645767

Chin, A. G., Etudo, U., & Harris, M. A. (2016). On Mobile Device Security Practices and Training Efficacy: An Empirical Study. *Informatics In Education*, *15*(2), 235–252. doi:10.15388/infedu.2016.12

Chin, W. W. (1998). *The partial least squares approach for structural equation modeling*. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). London: Lawrence Erlbaum.

Chin, W. W. (2010). How to write up and report PLS analyses. In V. Esposito Vinzi, W.W. Chin, J. Henseler et al. (Eds.), Handbook of Partial Least Squares: Concepts, Methods and Applications (pp. 655-690). London. UK: Springer.

Chu, A. M., & Chau, P. Y. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems*, *66*(C), 93–101. doi:10.1016/j.dss.2014.06.008

Coleman, Q. (2017). What Are the Different Theories of Industrial Relations? Retrieved from https://bizfluent.com/facts-6323679-different-theories-industrial-relations-.html

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. doi:10.1287/isre.1070.0160

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of Security Awareness: A Qualitative and Quantitative Study. *International Management Review*, *13*(1), 37–58.

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security*, *24*(1), 116–134. doi:10.1108/ICS-04-2015-0018

Ferrin et al., (2007). Can I Trust You to Trust Me? A Theory of Trust, Monitoring, and Cooperation in Interpersonal and Intergroup Relationships. *Group & Organization Management*, *32*(4), 465-474.

Ford, J., Willey, L., White, B. J., & Domagalski, T. (2015). New concerns in electronic employee monitoring: Have you checked your policies lately? *Journal of Legal*, *Ethical & Regulatory Issues*, *18*(1), 51–70.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *JMR, Journal of Marketing Research*, *18*(1), 39–50. doi:10.2307/3151312

Geisser, S. (1975). The predictive sample reuse method with applications. *Journal of the American Statistical Association*, *70*(350), 320–328. doi:10.1080/01621459.1975.10479865

Gennard, J., & Judge, G. (2002). *Employee Relations*. London: CIPD.

Goodhue, D., Lewis, W., & Thompson, R. (2007). Statistical power in analyzing interaction effects: Questioning the advantage of PLS with product indicators. *Information Systems Research*, *18*(2), 211–227. doi:10.1287/isre.1070.0123

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage.

Hair, J. F., Ringle, C., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–151. doi:10.2753/MTP1069-6679190202

Hair, J. F., Sarstedt, M., Ringle, C., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414–433. doi:10.1007/s11747-011-0261-6

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security*, *4*(4), 3–20. doi:10.1080/2333696X.2008.10855849

Helkala, K., & Bakås, T. H. (2014). Extended results of Norwegian password security survey. *Information Management & Computer Security*, *22*(4), 346–357. doi:10.1108/IMCS-10-2013-0079

Hu, V. C., & Scarfone, K. (2012). Guidelines for Access Control System Evaluation Metrics. *National Institute of Standards and Technology Interagency Report, NISTIR*, *7874*. doi:10.6028/NIST.IR.7874

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of recent studies. *Strategic Management Journal*, *20*(2), 195–204. doi:10.1002/(SICI)1097-0266(199902)20:2<195::AID-SMJ13>3.0.CO;2-7

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18. doi:10.1108/OIR-11-2015-0358

Jeske, D., & Santuzzi, A. M. (2015). Monitoring what and how: Psychological implications of electronic performance monitoring. *New Technology, Work and Employment*, *30*(1), 62–78. doi:10.1111/ntwe.12039

Kaspersky, E., & Furnell, S. (2014). A security education Q&A. *Information Management & Computer Security*, *22*(2), 130–133. doi:10.1108/IMCS-01-2014-0006

Kelley, T., & Bertenthal, B. I. (2016). Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites. *Information & Computer Security*, *24*(2), 164–176. doi:10.1108/ICS-01-2016-0002

Kennedy, S. E. (2016). The pathway to security – mitigating user negligence. *Information & Computer Security*, *24*(3), 255–264. doi:10.1108/ICS-10-2014-0065

Kent Marett, K. (2015). Checking the manipulation checks in information security research. *Information & Computer Security*, *23*(1), 20–30. doi:10.1108/ICS-12-2013-0087

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316–327. doi:10.1108/09685221011095236

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13. doi:10.1108/09685221011035223

Lebek, B., Markus, J. N., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. doi:10.1108/MRR-04-2013-0085

Lee, L., Petter, S., Fayard, D., & Robinson, S. (2011). On the use of partial least squares path modeling in accounting research. *International Journal of Accounting Information Systems*, *12*(4), 305–328. doi:10.1016/j.accinf.2011.05.002

Mani, D., Choo, K. R., & Mubarak, S. (2014). Information security in the South Australian real estate industry. *Information Management & Computer Security*, *22*(1), 24–41. doi:10.1108/IMCS-10-2012-0060

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. doi:10.1080/15332861.2010.487415

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47–67. doi:10.1080/15536548.2013.10845672

National Institute of Standards and Technology (NIST). (1998). *Information technology training requirements: A role- and performance-based model (NIST Special Publication 800-16)*. Washington, DC: U.S. Department of Commerce.

NCA. (2008). Electronic Transactions Act 772. Retrieved from https://nca.org.gh/assets/Uploads/NCA-Electronic-Transactions-Act-773.pdf

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Cate Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334–345. doi:10.1108/IMCS-10-2013-0078

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information & Computer Security*, *24*(2), 228–240. doi:10.1108/ICS-01-2016-0009

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management & Computer Security*, *15*(5), 362–371. doi:10.1108/09685220710831107

Ponemon Institute. (2012). *The human factor in data protection*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey–2012.pdf

Rigon, E. A., Westphall, C. M., dos Santos, D. R., & Westphall, C. B. (2014). A cyclical evaluation model of information security maturity. *Information Management & Computer Security*, *22*(3), 265–278. doi:10.1108/IMCS-04-2013-0025

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH. Retrieved from http://www.smartpls.com

Ross, P., & Bamber, G. J. (2009). Strategic choices in pluralist and unitarist employment relations regimes: A study of Australian telecommunications. *Industrial & Labor Relations Review*, *63*(1), 24–41. doi:10.1177/001979390906300102

Safa, N. A., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, *53*, 65–78. doi:10.1016/j.cose.2015.05.012

Sarstedt, M., & Mooi, E. A. (2014). *A Concise Guide to Market Research: The Process, Data, and Methods Using IBM SPSS Statistics*. Berlin: Springer. doi:10.1007/978-3-642-53965-7

Sedikides, C., Herbst, K. C., Hardin, D. P., & Dardis, G. J. (2002). Accountability as a deterrent to self-enhancement: The search for mechanisms. *Journal of Personality and Social Psychology*, *83*(3), 592–605. doi:10.1037/0022-3514.83.3.592 PMID:12219856

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. doi:10.1016/j.im.2013.08.006

Siponen, M., & Vance, A. O. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *Management Information Systems Quarterly*, *34*(3), 487–502. doi:10.2307/25750688

Sivalogathasan, V., & Hashim, A. (2013). changes in employee relations: Impact of perceived organizational support on social exchange of the outsourcing industry in Sri Lanka. *Skyline Business Journal*, *9*(1), 43–49.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3–6. doi:10.1080/15536548.2012.10845664

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting & Management Information Systems*, *15*(1), 112–130.

Styles, M., & Tryfonas, T. (2009). Using Penetration Testing Feedback to Cultivate an of Proactive Security amongst End-users. *Information Management & Computer Security*, *17*(1), 44–52. doi:10.1108/09685220910944759

Tadmor, C., & Tetlock, P. E. (2009). Accountability. In D. Matsumoto (Ed.), *The Cambridge Dictionary of Psychology* (p. 8). Cambridge: Cambridge University Press.

The Gale Group, Inc. (1970). *The Great Soviet Encyclopedia(1970-1979)* (3rd ed.). Retrieved from http://encyclopedia2.thefreedictionary.com/Human+Relations+Theory

Towns, D., & Cobb, L. (2012). Notes on: GPS technology; employee monitoring enters a new era. *Labor Law Journal*, *63*(3), 203–208.

Trcek, D., Trobec, R., Pavešic, N., & Tasic, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology*, *26*(2), 113–118. doi:10.1080/01449290500330299

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, *25*(3), 327–352. doi:10.1108/09593841211254358

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38–58. doi:10.1057/ejis.2013.27

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application*, *11*(2), 5–40.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263–290. doi:10.2753/MIS0742-1222290410

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *Management Information Systems Quarterly*, *39*(2), 345–366. doi:10.25300/MISQ/2015/39.2.04

Whalen, T., & Gates, C. (2010). Watching the watchers: "voluntary monitoring" of infosec employees. *Information Management & Computer Security*, *18*(1), 14–25. doi:10.1108/09685221011035232

Yaokumah, W., & Kumah, P. (2018). Exploring the Impact of Security Policy on Compliance. In *Global Implications of Emerging Technology Trends* (pp. 256–274). Hershey, PA: IGI Global.

Zaman, U., & Saif, M. I. (2016). Perceived accountability and conflict management styles as predictors of job performance of public officials in Pakistan. *Gomal University Journal of Research*, *32*(2), 24–35.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340. doi:10.1108/09685220910993980

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, *8*(3–4), 180–197. doi:10.1080/15332860903467508

Winfred Yaokumah is the Dean of the Faculty of Engineering, Science and Computing at the Pentecost University College, Accra, Ghana. He obtained his PhD in Information Technology with specialization in Information Assurance and Security at the Capella University, USA. He has published extensively in several international journals, including the Information Resources Management Journal, Information Management & Computer Security, International Journal of Technology Diffusion, Journal of Information Technology Research, International Journal of Information Systems and Social Change, International Journal of IT/Business Alignment and Governance, and the International Journal of Information Systems in the Service Sector. His research interest includes information security, e-services, IT governance, cloud computing, technology diffusion, information security governance, and IT leadership.

Daniel Okyere Walker holds an MSc in Regional Planning (University of Liberia), an MA in Mission Studies (University of Birmingham, UK), and a PhD in Theology (University of Birmingham, UK). He is currently Rector at Pentecost University College, Accra, Ghana

Peace Kumah is currently a doctoral student at the SMC University, Switzerland pursuing Business Administration with specialization in Human Resource Management. She holds an MBA (Human Resource Management) degree from Wisconsin International University College, Accra, Ghana. She has several years of teaching experience and has occupied leadership positions in various educational institutions. Her research interest includes strategic human resource development, organizational leadership and motivation, change management, employment relations, human resource and information systems workforce.