Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce

Abstract

Employees are increasingly relying on mobile devices. In international organizations, more employees are using their personal smartphones for work purposes. Meanwhile, the number of data breaches is rising and affecting the security of customers' data. However, employees' cybersecurity compliance with cybersecurity policies is poorly understood. Researchers have called for a more holistic approach to information security. We propose an employee smartphone-security compliance (ESSC) model, which deepens understanding of employees' information-security behavior by considering influences on the national, organizational, technological (smartphone-specific), and personal levels. The research focuses on secure smartphone use in the workplace among Gen-Mobile (aged 18-35) employees in a cross-cultural context: the United Kingdom (UK), United States (US) and United Arab Emirates (UAE) where 1,735 questionnaires were collected. Our findings suggest that those who wish to understand employees' smartphone-security behavior should consider national cybersecurity policies, cultural differences in different countries, and threats specific to smartphone use. In addition, our findings help companies to increase customers' trust and maintain a positive reputation.

Keywords: Customer data; smartphone security; employee cybersecurity compliance; cross-cultural information security

1. Introduction

The growth of this mobile workforce is driven by technological change, globalization, and changes in employees' expectations. These employees prefer mobility in terms of the devices they use and their approach to work. The benefits of using technology, more specifically, smartphones at work include faster innovation, flexible work opportunities, higher-quality work, and better collaboration and communication across borders (Kshetri, 2015; British Telecom, 2018; Frost & Sullivan, 2016; Prud'Homme & von Zedtwitz, 2019). However, managing the security of data in these devices remains a challenge. Employees can use their personal smartphones to access different work-related applications for example: corporate mobile

applications, company and employee contact details, and mobile dashboards. They can also download business documents on their smartphones. This makes smartphone security an even more pressing issue. Previous reports have identified that smartphone security can be compromised by different threats: loss of the device, the operating system (Android or Apple iOS), insecure networks, weak authentication processes, poor data-protection, insufficient privacy, viruses, malware, and SMS-based attacks (McAfee, 2018). Losing critical company data, especially relating to customers, is a major concern for most organizations (European Commission, 2017).

Smartphones are the most widely used devices for work (Global Web Index, 2017) and personal purposes. As their prevalence has increased, smartphones have become more prone to cyberattacks and they are associated with a higher level of security risk. Meanwhile, increasing numbers of companies are adopting the bring your own device (BYOD) model, which involves "employees bringing their personally owned mobile devices such as laptops, tablets, and smartphones to the workplace, and using those devices to access privileged company information and applications" (Tu, Adkins & Zhao, 2018, p. 1). In many countries, the workforce has gone mobile (Spokephone, 2018), performing their professional duties using their smartphones or tablets. Generation-mobile (Gen-Mobile) employees, most of whom are at the early stages of their career, are shaping their working lives around their mobile devices. The global mobile workforce is set to increase from 1.45 billion in 2016, accounting for 38.8 percent of the global workforce, to 1.87 billion in 2022, accounting for 42.5 percent of the global workforce (Strategy Analytics, 2016).

International organizations whose employees use mobile devices are exposed to vulnerabilities that could be highly disruptive for their businesses. According to a recent global survey of security professionals (Dimensional Research, 2017, p.2), 64 percent of participants doubt that their organization could prevent a mobile cyberattack, 94 percent expect the frequency of mobile cyberattacks to increase, 32 percent of organizations fail to secure mobile devices adequately, and 79 percent believe that it is becoming more difficult to secure their mobile devices. More importantly, 56 percent of organizations think that regular employees who are trusted and authorized users pose the biggest security risk to their business (Cyber Security Insiders, 2018). Meanwhile, under the General Data Protection Regulation (GDPR), companies

must report security breaches or face prosecution if they are based in the European Union (EU), have employees in the EU, or do business there.

Tackling cybersecurity requires international efforts. The World Economic Forum revealed concerns over failure to tackle global threats to cybersecurity and stated that nations and governments across the globe have struggled to form information sharing channels with companies (World Economic Forum, 2018). Organizational cybersecurity will not improve unless nations begin working together and with their own technical security experts to improve their understanding of security problems and the tools used to fix them (Sheridan, 2018). Hence, there is a need for an international perspective when addressing cybersecurity issues in organizations (Bing, 2018). Recent statistics show that only less than half the companies in the USA are fully prepared to deal with cyberattacks (Palmer, 2019). Companies in the USA report have one of the highest total average cost of cybersecurity at US$21 million (Accenture, 2017). Furthermore, despite following the General Data Protection Regulation (GDPR), the case is similar in the UK where recent statistics show that only 57% have a cyber incident response plan they test on a regular basis (Department for Digital, Culture, Media and Sport, 2019). Companies in the UK also report one of the highest total average cost of cybersecurity at US$9 million (Accenture, 2017).

Most academic studies on employees' information-security compliance have focused on the individual and organizational levels (e.g. Dang-Pham & Pittayachawan, 2015; Hu, Dinev, Hart & Cooke, 2012; Hwang & Cha, 2018; Janmaimool, 2017; Putri & Hovav, 2014; Salleh et al., 2012; Siponen, 2006; Tu & Yuan, 2015). More recently, a study conducted by Johnston, Di Gangi, Howard and Worrell (2019) investigated this phenomenon at the group level. A few studies have used the Hofstede cultural dimensions to consider effects of culture at the national level on employee information-security compliance (e.g. Arage, Belanger & Tesema, 2016; Connolly, Lang & Tygar, 2014). Herrera, Ron and Rabadão (2017) have highlighted the general impact of national cybersecurity policies. However, no studies have explored the effects of national cybersecurity policies and technology-specific threats on employees' information-security behavior. Further, the need for a more holistic approach to information security has been highlighted in recent literature (Soomro, Shah & Ahmed, 2016).

Managing teams in different countries is a major challenge for global companies (Singh, 2010). This is due to national differences in political, economic, social, and regulatory factors (Brewster, Chung & Sparrow, 2016). By influencing employees' behavior, national laws on mobile cybersecurity may play a significant role in reducing breaches of company data through a mobile device. However, this area remains unexplored in the prior studies. Hence, this research investigates the effects of national cybersecurity policies and security threats that are specific to smartphones on employees' smartphone-security compliance. In doing so, it proposes a more holistic model that considers national, organizational, technological (smartphone-specific) and personal factors to understand employees' information-security behavior.

The proposed model combines three theories that apply to employees' information-security behavior: protection motivation theory (Rogers, 1983), general deterrence theory (Beccaria, 1963; Gibbs, 1975), and the theory of reasoned action (Fishbein & Ajzen, 1975). The model integrates national cybersecurity policies and technological (security threats specific to smartphone technology). Our research contributes a more holistic understanding of how national cybersecurity policies and security threats specific to smartphone technology influence employee information-security compliance in international organizations that have adopted the BYOD model. In addition, it raises awareness of the need to include these factors within strategies for information security.

We focus on BYOD (specifically smartphone) security among Gen-Mobile employees aged 18-35 in the United Kingdom (UK), the United States (US), and the United Arab Emirates (UAE). These three countries have different characteristics. According to the Global Cyber-Security Index provided by the International Telecommunication Union (2018), the UK is ranked first in terms of commitment to cybersecurity, the US is ranked second, and the UAE is ranked thirty-third. Despite this gap, the UAE is one of the most technologically advanced countries in the Middle East. In addition, it has close business ties with both the US and the UK, which are tech leaders in comparison with other markets. Economic, cultural, and regulatory factors also differ among the three countries. It is a wealthy country that has direct trade relations with other regions in the world, including Europe. For example, the UAE is the UK's largest export market in the Middle East, a market that has been under researched in terms of management systems and leadership styles (Karacay, Bayraktar, Kabasakal & Dastmalchian, 2019). The number of global companies with teams

operating in different countries is increasing rapidly. Hence, it is important to investigate whether there are differences in employees' cybersecurity compliance in different countries and cultures. Therefore, focusing on these countries provides academics and practitioners with in-depth insights into employee behavior in different countries. Thus, we also respond to the call for improving the quality of cross-cultural research beyond Hofstede and GLOBE (Tung & Vebeke, 2010).

The remainder of the study is structured as follows. Section two gives an overview of security issues related to BYOD. Theoretical background is discussed in section three. Research model is presented and hypotheses are developed in section four. Section five describes research methodology. Section six describes the process of data collection and the results are interpreted in the same section. Section seven is dedicated for discussion. Theoretical and practical contributions are elaborated in section eight. Limitations and directions for future research are given in section nine. Last, study findings are summarized in the conclusion section.

2. BYOD Security

Under the GDPR, companies that operate in the EU must follow a set of laws on data protection. If a data breach is identified, the company must report it within 72 hours to the data protection authority in their country (Jaques, 2017). That authority then decides how much to fine the organization for the breach. This could be up to four percent of the organization's global annual turnover or EUR20 million, whichever is highest (Jaques, 2017). BYOD security practices covered by the GDPR include controlling data storage, limiting data transfers, emphasizing security (including restricting the installation of third-party mobile applications), and increasing employee privacy (Hanna, 2018). The GDPR applies to companies that operate in Europe or that deal directly with customers in Europe. However, it also has implications for global organizations when employees from European countries are connected using a technological medium, such as a mobile application installed on the employee's smartphone.

The existing literature fails to account for the external environment (specifically, national cybersecurity policies), which can have a significant effect on how employees use their personal devices—both inside and outside their companies. In addition, despite recognition that it is important to assess employees' awareness of the specific security threats posed by the BYOD model, the existing literature has not considered this

phenomenon or integrated these threats into BYOD security models. Table 1 sets out the findings of recent studies (up to January 2019) on employees' BYOD security behavior.

Table 1. Studies on BYOD security behavior

Author	Context	Methodology	Findings
Putri and Hovav (2014)	Focuses on the factors affecting the adoption of BYOD at work, but integrates two factors related to security. Combines reactance, organizational justice, and protection motivation theory.	Data was collected via questionnaires distributed to employees. Received 230 usable responses from employees in Indonesia.	While protection motivation theory partially enhances compliance, perceived loss of freedom reduces intention to comply with an organization's BYOD information-security policy. Similarly, perceptions of justice increase compliance.
Allam Flowerday and Flowerday (2014)	Focuses on smartphone security among employees. Adapts an awareness model from the domain of accident prevention.	Carried out an expert review of the model. Seven responses were received.	Smartphone-security awareness depends on smartphone productivity levels, the pressure applied on employees to increase the amount of effort required to perform work using smartphone devices, and pressure from policies.
de las Cuevas et al. (2015)	Proposes an adaptive and free software system to manage security in BYOD environments: the multi-platform usable endpoint security (MUSES).	Adopted an experimental approach.	The MUSES system focuses on creating technology that accounts for user behavior and security.
Al Askar & Shen (2016)	Focuses on five main contextual factors: device ownership, place, time, activity/task, and sensitivity.	The research was theoretical and no empirical work was conducted	The literature has failed to accurately identify the contextual factors that can affect employees' BYOD security behavior.
Wang et al. (2017)	Extends the unified theory of acceptance and use of technology (UTAUT) to include threats to business security and private security.	Collected data via questionnaires distributed to employees. Collected data from the US, China, and Germany. Included 302 usable responses in the analysis.	Performance expectancy, effort expectancy, and perceived threat have a significant influence on behavioral intention to use BYOD for work-related activities.
Jarrahi, Nelson and Thomson (2017)	Integrates factors related to artifact ecologies: personal context, spatial context, collaborative context, organization context,	Conducted semi-structured interviews with 36 mobile knowledge workers from North Carolina's Research Triangle.	The findings highlight the significance of the artifact ecology that embodies various social and contextual forces that shape the engagement of mobile workers with a broad diversity of personal

	multitude of technologies, and work activities.		computing tools, as well as organizational and local infrastructures.
Baillette, Barlette and Leclercq-Vandelannoitte (2018)	A theoretical analysis of reversed IT adoption logic vs traditional IT adoption logic.	The work was theoretical, and no empirical work was conducted.	Employees enjoy the personal advantages of using their own device, but this comes with more threats to the security of personal data.
Cho and Ip (2018)	Uses technology threat avoidance theory to study BYOD security in organizations.	Collected data via a questionnaire distributed to employees. Included 450 usable responses in the analysis.	Perceived cost and protection of privacy has no significant effect on employees' intention to adopt BYOD, while organizational commitment and job security have the strongest influences on that intention.
Tu et al. (2018)	Extends protection motivation theory by integrating moderating factors related to mixed use and surveillance visibility.	Collected data using a questionnaire distributed to employees. Included 122 usable responses in the analysis.	Employees' intention to comply is motivated by perceived effectiveness when the device is used for personal and work purposes.
Blythe and Coventry (2018)	Extends protection motivation theory in the context of BYOD security.	Collected data via an online survey distributed to employees. Included 526 usable responses in the analysis.	Coping appraisal is more predictive of security behaviors than threat appraisal. Response costs may be a barrier to behavior, but response efficacy is a key facilitator.
Weber and Rudman (2018)	Identifies risks associated with adopting BYOD.	Analyzed the literature on BYOD risks.	Identifies 50 types of risk that may arise if an organization adopts a BYOD program. The key risks are malware, data leakage, loss and theft.
Doargajudhur and Dell (2018)	Combines the job demands-resources (JD-R) model and the task-technology fit (TTF) model.	Collected data using a questionnaire completed by employees in different sectors. Included 400 usable responses in the analysis.	BYOD indirectly affects job satisfaction, job performance, organizational commitment, job demands (perceived workload), job resources (perceived job autonomy), and TTF.

As shown in Table 1, previous studies have investigated BYOD, in particular; smartphone security among employees. However, none of these studies focus on the effects of national factors and the effects of the GDPR in a cross-cultural context. In addition, there is a lack of studies proposing a holistic model that accounts for national, organizational, technological (smartphone-specific) and personal factors which is needed for a deeper understanding of this behavior among the Gen-Mobile workforce. The studies in Table

1 mainly focused on personal and organizational factors rather than a careful integration of these types of factors with national and technological factors at a cross-cultural level. Because international organizations have limited control over how employees use BYOD smartphones outside work in voluntary settings, they are at higher risk of a security breach. It is necessary to investigate the effects of different national cybersecurity policies on BYOD security in more depth. This is especially important for global companies because different national policies may result in different smartphone-security behavior among employees. Gen-Mobile employees use their mobile devices for personal and work purposes, but no studies have focused on this segment of the population. Hence, more research is needed for more information about the context within which BYOD security lies.

3. Theoretical Background

The literature is rich with theories that have been applied to the area of information-security management. However, only a few studies have investigated employees' actual behavior in this context (Cram, Proudfoot & D'Arcy, 2017; Karlsson, Kolkowska & Prenkert, 2016; McCole, Ramsey & Williams 2010; Gozman & Willcocks, 2019; Amankwah-Amoah & Wang, 2019). Theories in the literature include protection motivation theory (Rogers, 1983), general deterrence theory (Beccaria, 1963; Gibbs, 1975), rational choice theory (Paternoster & Simpson, 1996), neutralization theory (Siponen & Vance, 2010; Sykes & Matza, 1957), theory of reasoned action (Fishbein & Ajzen, 1975), theory of planned behavior (Ajzen, 1985) and social cognitive theory (Bandura, 1986). Table 2 provides, the factors integrated in each of these theories, and definitions of those factors. Table 3 shows the strengths and limitations of each theory.

Neutralization theory, developed by Sykes and Matza (1957), originates in criminology, though it has been developed for use in other contexts (Siponen & Vance, 2010). In a nutshell, neutralization theory is about how individuals rationalize illicit behavior and turn off certain values in order to perform certain actions. The original theory describes five justifications that individuals use for their actions. Siponen and Vance (2010) incorporate four of these: denial of responsibility, denial of injury, appeal to higher loyalties, and condemnation of the condemners (Table 2).

Rational choice theory, developed by Paternoster and Simpson (1996), posits that the decision to engage in illicit behavior is a function of the perceived costs and benefits of the act (Simpson, 2002). In other words, an individual determines what action to take by balancing the costs and benefits of their options. It integrates five main factors: formal sanction, informal sanction, shame, perceived benefits, and moral beliefs (Simpson, 2002; see Table 2). In contrast, protection motivation theory (Rogers, 1975) explains how employees' security behavior is motivated by the fear of loss that could occur due to a threat (Herath & Rao, 2009a; Siponen, Pahnila, & Mahmood, 2010). The theory integrates five main factors: perceived risk vulnerability, severity of the adverse consequences, response efficacy, self-efficacy, and response cost (Rogers, 1975, 1983; see Table 2). It has been applied in the context of employees' awareness of organizational information-security policies (Herath & Rao, 2009a; Siponen et al., 2010) and individuals' use of security software (Johnston & Warkentin, 2010).

Adapted from criminal justice research, general deterrence theory is based on the concept of rational decision-making (Beccaria, 1963; Gibbs, 1975). It proposes that as the certainty and severity of punishment increase, the level of unacceptable behavior decreases (Herath & Rao, 2009b). Rooted in classic criminology (Beccaria, 1963; Gibbs, 1975), the theory assumes that people make reasoned decisions about perpetrating or abstaining from crime, and that these decisions are based on maximizing their benefits and minimizing cost. From this perspective, when employees' make decisions on whether or not to comply with information-security policies they are influenced by their perceptions of the certainty and severity of the sanctions they may face, balancing the costs and benefits (Bulgurcu, Cavusoglu & Benbasat, 2010; D'Arcy, Hovav & Galletta, 2009; Herath & Rao, 2009a; Herath & Rao, 2009b; Hovav & D'Arcy, 2012).

The theory of reasoned action was primarily developed to understand and predict human social behavior (decision-making). It was introduced by Fishbein and Ajzen (1975). Because it provides insights on behavior, it is an important starting point for many of the theories and models of technology acceptance that extend it. The theory integrates three main factors: attitude, subjective norms, and behavioral intention (see Table 2). It was extended by Ajzen (1985) to form the theory of planned behavior, which integrates perceived behavioral control to account for the external environment that surrounds individuals. Recently, the theory

has been applied in the context of information-security management (Bauer, 2016; Kim, Yang & Park, 2014). Social cognitive theory has also been used to study information systems security. This theory is based on social learning theory, studied by Miller and Dollard (1941), in which three major elements for learning are identified: self-efficacy, environmental factors, and behavior modelling (see Table 2).

Table 2. Factors found in previous employee security compliance theories

Source	Theory	Factor	Definition and brief explanation of factor
Rogers (1975)	Protection motivation theory	Perceived risk vulnerability	One's perception of experiencing possible negative consequences of behaving in a risky way (Rogers, 1983; Salleh et al., 2012).
		Severity of the adverse consequences	One's perception of the level of damage that may result from engaging in a risky situation (Rogers, 1983; Salleh et al., 2012).
		Perceived response efficacy	The degree to which one believes that their response will be effective in alleviating the threat (Rogers, 1983).
		Perceived self-efficacy	Belief in one's ability to perform a particular task (Rogers, 1983; Salleh et al., 2012).
		Response cost	The cost (time and effort) of performing the recommended behavior (Rogers, 1983).
Beccaria (1963); Gibbs (1975)	General deterrence theory	Perceived severity of sanctions	How one perceives the severity of penalties for noncompliance. If the perceived severity is high, one's intention to behave in an undesirable way is likely to decrease (Peace et al., 2003).
		Perceived certainty of sanctions	How certain one is that one will receive a penalty for disobeying a law or policy (D'Arcy & Herath, 2011).
Paternoster and Simpson (1996)	Rational choice theory	Formal sanction	Rules and laws that have penalties associated with the behavior (Arage et al., 2016).
		Informal sanction	Disapproval of friends or peers in response to a given action (Arage et al., 2016; Paternoster & Simpson, 1996).
		Shame	Feelings of guilt or embarrassment about one's socially undesirable actions (Arage et al., 2016; Eliason & Dodder 1999, as cited in Siponen & Vance, 2010).
		Perceived benefits	Intrinsic benefits, such as the internal satisfaction one gets from breaking a rule (Wood et al., 1997), and extrinsic benefits, such as money received for breaking a rule (Arage et al., 2016; Lafree et al., 2005).
		Moral beliefs	One's judgment about engaging in ISSP violation as morally wrong or right (Arage et al., 2016).
Sykes and Matza (1957); Siponen	Neutralization theory	Denial of responsibility	Not taking responsibility for one's actions; seeing oneself as powerless to have acted in another way (Sykes & Matza, 1957).
		Denial of injury	Rationalizing one's own actions as being harmless and not causing any damage (Sykes & Matza, 1957). People often use this rationalization when nothing serious happens to them and to others as a consequence of their actions.

and Vance (2010)		Appeal to higher loyalties	Justifying one's actions as being necessary to get out of a problematic situation (Sykes & Matza, 1957) or as being for the greater good in the long term (Siegel, 2005).
		Condemnation of the condemners	Justifying one's actions by arguing that the rule against the action is unreasonable (Sykes & Matza, 1957). In the context of information-security policies, an employee could argue that they are justified in breaking a rule because it is counterproductive and a hindrance to work.
		Defense of necessity	Justifying one's actions by arguing that there was no other course of action to take. One does not feel guilt when one perceives the action as necessary (Minor, 1981).
Fishbein and Ajzen (1975)	Theory of reasoned action	Attitude	One's belief that the behavior leads to certain outcomes, and one's evaluations of those outcomes (Ajzen & Fishbein, 1980).
		Subjective norms	One's belief that specific individuals or groups think that one should or should not behave in a certain way, and one's motivation to comply with those norms (Ajzen & Fishbein, 1980).
		Intention	One's readiness (cognitively) to perform a certain behavior. Accordingly, the possibility of a person behaving in a certain way depends on their intention (Ajzen & Fishbein, 1980).
Ajzen (1985)	Theory of planned behavior	Perceived behavioral control	When one believes that one has less control over a certain behavior (Ajzen, 1985; 1991). The perceived ease or difficulty of behaving in a certain way, and the sense of having the skills and resources to do so (Ajzen, 2005). This factor combines self-efficacy and controllability (Terry & O'Leary, 1995).
Bandura (1986)	Social cognitive theory	Self-efficacy	One's perception of one's capability to perform the behaviors (Bandura, 1986).
		Environmental factors	The social norms and community (Bandura, 1986).
		Behavior modelling	Knowledge or skills influencing behavior (Bandura, 1986).

Table 3. Strengths and limitations of existing theories

Theory	Strengths	Limitations
Protection motivation theory	• Effective for studying changes in human behavior through the use of fear (Shaw, 2012; van Bavel Rodríguez-Priego, Vila & Briggs, 2019).	• Does not consider environmental and cognitive factors such as social norms (El-Den & Dangi, 2016; Shaw, 2012; Vance, Siponen & Pahnila, 2012).
General deterrence theory	• Effective tool for preventing crime (El-Den & Dangi, 2016; Bulgurcu et al., 2010) • Emphasizes the power of punishment to deter crime (El-Den & Dangi, 2016; Bulgurcu et al., 2010).	• Central assumption of the theory is that people are deterred from committing crime by the severity of the punishment (El-Den & Dangi, 2016; Tomlinson, 2016). • Lacks a complete understanding of crime causation (El-Den & Dangi, 2016; Tomlinson, 2016).
Rational choice theory	• Uses a deductive-based approach and allows for generality (El-Den & Dangi, 2016; Zafirovski, 1999). • Makes it possible to treat variations in choices among actors or by an actor over time as a function of their structural position (El-Den & Dangi, 2016; Zafirovski, 1999).	• Does not capture the complexity of human social actions and interactions (El-Den & Dangi, 2016; Paternoster & Bachman, 2001; Zafirovski, 1999). • Rejects the concept of social action as expressive, nonrational, or irrational, or as caused by external factors (El-Den & Dangi, 2016; Paternoster & Bachman, 2001; Zafirovski, 1999). • Assumes that all choices made by humans are rational (El-Den & Dangi, 2016; Paternoster & Bachman, 2001; Zafirovski, 1999). • Conceptualizes rational (and all) human action as simply utility- or profit-optimizing behavior (El-Den & Dangi, 2016; Paternoster & Bachman, 2001; Zafirovski, 1999).
Neutralization theory	• Makes it possible to understand criminals' thought processes when justifying their behavior when committing crimes (Lanier & Henry, 2004; Siponen et al., 2012).	• Offenders may not be committed to conventional values and norms in the first place (Hamlin, 1988; Lanier & Henry, 2004). • There are problems with causality, particularly in establishing when the neutralizations occur (Hamlin, 1988; Lanier & Henry, 2004).

Theory of reasoned action	• Explains human behavior when interacting with technology (Ameen, 2017; Montaño & Kasprzyk, 2015). • Forms the basis of subsequent theories on human-computer interaction (Ameen, 2017; Montaño & Kasprzyk, 2015).	• Does not account for external factors that can affect humans' behavior (Ameen, 2017; Silva & Dias, 2007). • Assumes that people behave in a rational way and that all actions are planned (Ameen, 2017; Silva & Dias, 2007).
Theory of planned behavior	• Accounts for external factors during the decision- making process (Ajzen, 2002; Cho & Walton, 2009).	• Overlooks emotional factors associated with individual actions, such as fear, danger, threat, and any positive feelings (Cho & Walton, 2009; El-Den & Dangi, 2016).
Social cognitive theory	• Covers important aspects of human behavior and personal beliefs about one's ability to behave in a certain way (Ameen, 2017; Compeau & Higgins, 1995).	• Does not account for changes that may take place over a person's life (El-Den & Dangi, 2016). • Not fully systematized (El-Den & Dangi, 2016).

In the context of information-security management, none of the theories listed in Tables 3 and 4 include factors that are specific to the external environment (beyond the organizational context) and none of them consider the security threats that are specific to the technology being used. A recent systematic literature review by Soomro et al. (2016) explains that current research is mainly concerned with the role of management in organizational information security. The authors suggest taking a more holistic approach to studying information technology management in organizations by investigating not only participation from top managers and human resources managers but also the development and execution of information-security policies, training and awareness in information security, and the involvement of strategic decision-makers.

Threats related to the type of technology under investigation are also important. International organizations are moving beyond using desk-based technologies, such as computers. Many now favor wireless technologies, such as iPads and smartphones, which integrate sophisticated software and provide more benefits (Putri & Hovav, 2014). These technologies have created new and unpredictable challenges for information security within organizations (Wandera, 2018a). Smartphones can pose a major security threat simply because they are used so extensively which make them a more attractive target for cybercrime. Furthermore, features that are specific to smartphones create security threats that are unique to these devices.

Examples of these features include mobility, device ownership (as the device is owned by the employee rather than the organization), the ability to connect to different networks, multiple sophisticated mobile applications integrated into one device, and dual use of the device for personal and professional purposes (Wandera, 2018a; Weber & Rudman, 2018).

Recent studies have emphasized that national policies have a significant impact on how people intend to use, and actually use, smartphones (Ameen & Willis, 2018a; Ameen & Willis, 2018b; Ameen, Willis & Shah, 2018). National policies on the secure use of smartphones and mobile applications can influence organizations' policies on smartphone use. In turn, this influences how employees use smartphones for personal and professional purposes. We developed the employee smartphone-security compliance (ESSC) model proposed in this study by combining and extending three existing theories: protection motivation theory, general deterrence theory, and theory of reasoned action. We combined these theories for the four reasons. First, each theory has been used to study employees' information-security behavior (Cram et al., 2017). Second, when capturing the complexity of human social actions and interactions, these theories are more effective than other relevant theories, such as rational choice theory, neutralization theory, and social cognitive theory (El-Den & Dangi, 2016). Third, combining the three selected theories helps to overcome the limitations that apply when using them individually (see Table 3). Fourth, some of these theories have been used individually to study mobile security behavior in previous research. For example, Dang-Pham and Pittayachawan (2015) adopted the protection motivation theory to study individuals' BYOD (mobile phones) security. The authors found that the theory serves the purpose of understanding students' mobile security behavior. Similarly, the theory pf planned behavior has been adopted to study individuals' mobile security behavior (Cho & Ip, 2018). Furthermore, Yang et al. (2019) explained that the general deterrence theory can be used to study employees' security behavior. Hence, the integration of these three theories to study employees' BYOD (smartphone) security behavior is justified.

4. Research Model and Hypothesis Development

We propose a new research model to understand how national cybersecurity policies and smartphone-specific security threats affect employees' information-security compliance. The ESSC model draws on protection

motivation theory (Rogers, 1983), general deterrence theory (Beccaria, 1963; Gibbs, 1975), and theory of reasoned action (Fishbein & Ajzen, 1975). It groups factors into four categories: national, organizational, technological (smartphone-specific), and personal (see Figure 1). In this section we explain the factors included in each category and propose hypotheses for how they influence employees' behavior.

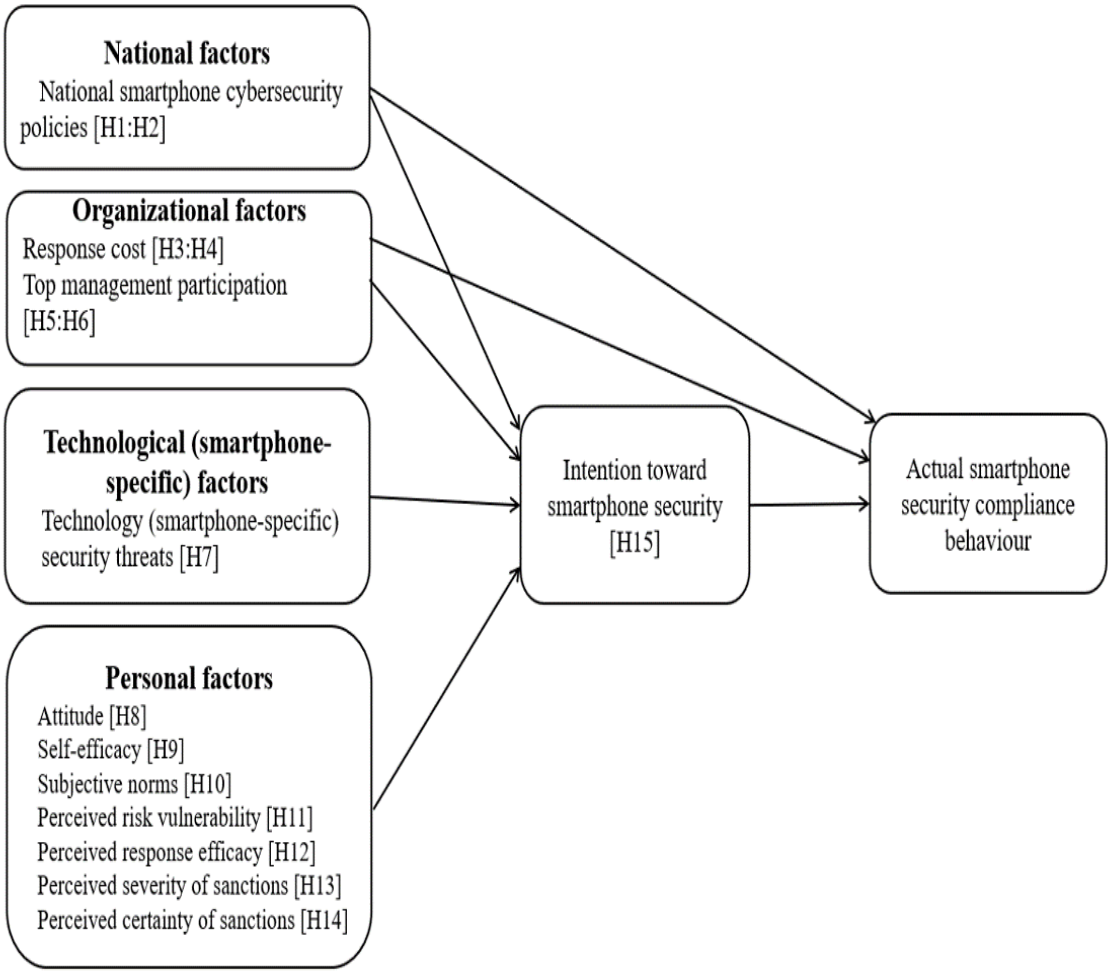

Figure 1. Proposed model

4.1 National Factors

4.1.1 National smartphone cybersecurity policies

National cybersecurity policies and regulations assist organizations to minimize security breaches and deal with those that they do encounter. The policies and regulations in individual countries have implications for any global company whose workforce is active in that country (Herrera et al., 2017). However, research has not yet investigated the influence of national policies on organizations' and employees' secure use of

BYODs. Furthermore, the theories that have been applied to research on information-security management presume that the external (or environmental) factors that may affect employees' cybersecurity behavior exist within the organization and are mainly related to the management (Soomro et al., 2016). Effective national cybersecurity policies influence company policy on BYOD. Since employees use these devices for personal purposes as well as at work, these national policies also affect how employees use smartphones outside the organization. Because different countries have different cybersecurity policies and they rank differently in the cybersecurity index, an employee's smartphone security behavior may depend on the country they live and work in. For example, the GDPR is not followed in all countries around the world, and it does not apply equally to all BYOD users. National cybersecurity policies give consumers the power to protect their information and may affect how networks are protected. An inconsistent or unenforced set of national cybersecurity policies guarantees poor security (CTIA, 2018). Hence, national cybersecurity policies can create variance in employees' smartphone-security compliance.

The GDPR has a significant impact on mobile security in European countries (Hanna, 2018; Holland, 2018). For example, companies must ensure that they protect personal data, whether that data is kept on servers, in the cloud, in mobile applications, or on company-owned mobile devices (Holland, 2018). This EU regulation also affects employees in other countries, because it applies to any company that does business with or monitors EU residents (Holland, 2018). In other words, when multinational and global companies based in other parts of the world (including the US and the UAE) deal with or target people in the EU or have employees in the EU (Malone, 2018), they must follow the GDPR. Businesses in the US have been taking steps to ensure that they comply with the new regulation (Endpoint Protector, 2018). Not all data protection legislation in the US meets the standards of the GDPR (Endpoint Protector, 2018). Hence, national smartphone security policies can be an important factor affecting employees' cybersecurity behavior.

The GDPR requires companies to be in full control of their data at all times (Wandera, 2018a). This makes the BYOD model (including smartphones) challenging because full control is "near impossible when the controller does not own the device where the data is being accessed or stored" (Wandera, 2018b). More importantly, the GDPR does not account for human error, so organizations can be held liable for errors made

by their employees (Wandera, 2018b). As explained by Act Systems (2018), the GDPR addresses four key areas of mobile security that organizations need to consider:

1. Information audits: Businesses need to know where all their data is and keep records of how and when a person gives the organization consent to store and use their personal information.
2. Visibility: At all times, organizations need to see which devices and mobile applications are accessing business services. This includes employees' personal devices.
3. Device security threats: Organizations need to ensure that appropriate security configurations, encryptions, and protection policies have been applied to the device.
4. Keeping personal and business data separate: Organizations need to set boundaries for employees on the overlap between personal and business smartphone use.

Hence, organizations are under pressure to ensure that employees are aware of and can follow a set of clear policies. In turn, this can have a significant impact on how employees intend to behave (their behavioral intention) and how they actually behave in the context of smartphone-security compliance. Although the UAE has no data protection law that compares with the GDPR in Europe and the US, the UAE Constitution gives citizens a general right to privacy (Dowle, 2018). Policy-makers in the UAE acknowledge that companies should adhere to the GDPR if they are connected to the EU in any way (Dowle, 2018). Thus, we propose the following two hypotheses:

H1. National smartphone cybersecurity policies affect employees' behavioral intention toward smartphone-security compliance.

H2. National smartphone cybersecurity policies affect employees' actual smartphone-security compliance.

4.2 Organizational Factors

4.2.1. Response cost

By organizational factors, we refer to the support that an organization provides to its employees to keep their smartphones safe and secure. Organizational support goes beyond building awareness; it also includes motivating employees and creating effective policies that are understood and easy to follow (Gagne & Deci,

2005; Pitichat, 2013). Organizational factors include response cost and top-management participation. Response cost is the cost to the employee of performing the recommended behavior (Rogers, 1983). In this context, it refers to the effort, overheads, and time required to comply with the organization's policy on using smartphones securely (Xiao et al., 2016). By providing support, organizations can reduce the response cost associated with using smartphones securely. We argue that response cost has a significant impact on employees' behavioral intention and their actual smartphone-security compliance. Therefore:

H3. Response cost affects employees' behavioral intention toward smartphone-security compliance.

H4. Response cost affects employees' actual smartphone-security compliance.

4.2.2 Top-management participation

The second organizational factor is top-management participation, which emerged in the management and organizational culture model developed by Hu et al. (2012). Top management play a critical role in managing information security and creating an organizational culture that encourages employees to keep their smartphones secure. Top managers influence employees' beliefs, which include their attitudinal, normative, and control beliefs (Puhakainen & Siponen, 2010; Soomro et al., 2016). Employees' own behavior may be influenced by their perceptions of top managers' behavior and actions in facilitating organizational actions (Liang & Xue, 2010). It can act as an important determinant of their behavioral intention and actual smartphone security compliance behavior. Thus:

H5. Top-management participation affects employees' behavioral intention toward smartphone-security compliance.

H6. Top-management participation affects employees' actual smartphone-security compliance.

4.3 Technological (smartphone-specific) factors

4.3.1 Technology (smartphone-specific) security threats

Technological (smartphone-specific) factors are the features that make smartphone security different than that of other devices, such as laptops and iPads. A smartphone can store personal data and business data,

including customer data (Olalere, Abdullah, Mahmod & Abdullah, 2015). The security threats that are specific to smartphones are associated with the device itself, its operating system, and the mobile applications that can be accessed through it. Smartphones are prone to particular security threats. These include losing the device, theft of personal and corporate data, phishing attacks[1], spyware attacks[2], financial malware attacks[3], third-party mobile applications[4], and attacks associated with the smartphone network (Murray, 2014). The Apple App Store for iOS and the Google Play Store for Android are the two largest distribution channels for mobile applications, but other vendors also develop and manage applications (Wandera, 2018c). This provides more opportunity for attacks and increases security threats. Such threats can create a sense of urgency that increases compliance. Thus:

H7. Technology (smartphone-specific) security threats affect employees' behavioral intention toward smartphone-security compliance.

4.4 Personal Factors

Personal factors refer to the personal characteristics of each employee. In our proposed model, these factors include: the employee's attitude, behavioral intention, subjective norms, self-efficacy, perceived risk vulnerability, and perceived response efficacy, perceptions of the severity and certainty of sanctions. We omitted the factor severity of the adverse consequences, which is used in protection motivation theory and refers to one's perception of the level of damage which may result from engaging in risky situations (Rogers, 1983). Previous studies found that this factor did not have a significant effect on behavioral intention (Ifinedo, 2012; Moody, Siponen & Pahnila, 2018; Salleh et al., 2012). Some of these studies identified an overlap between this factor and perceived risk vulnerability in that both factors represent a risk to the employee (Ifinedo, 2012; Moody et al., 2018; Nyre & Jaatun, 2013). Blythe Coventry and Little (2015) and Ifinedo (2012) attributed this overlap to differences in the conceptualization of severity in previous studies. That is,

[1] Phishing attacks occur when an attacker collects user credentials (such as passwords and credit card numbers) through fake mobile applications or through SMS or email messages that seem genuine (Murray, 2014; Shing et al., 2016).
[2] Spyware covers untargeted collection of personal information as opposed to targeted surveillance (Murray, 2014; Shing et al., 2016).
[3] Financial malware attacks occur when a smartphone is infected with programs designed for stealing credit card numbers, stealing online banking credentials, or subverting online banking or ecommerce transactions (Murray, 2014; Shing et al., 2016).
[4] Third-party mobile applications are mobile applications that are created by a vendor that is not the manufacturer of the device or its operating system (Wandera, 2018c).

perceived severity is not one overall construct but may comprise several implications (Blythe et al., 2015). Within the context of this study, one of these implications is the severity of sanctions received for noncompliance. Furthermore, severity of the adverse consequences does not play a role in all security behaviors (Moody et al., 2018). Hence, we focused on perceived risk vulnerability and perceived severity of sanctions (Moody et al., 2018; Nyre & Jaatun, 2013).

4.4.1 Attitude

Attitude refers to a person's belief that behaving in a certain way leads to specific outcomes and the person's evaluation of those outcomes (Ajzen & Fishbein, 1980). Within the context of smartphone-security compliance, attitude refers to the employee's view on whether the behavior is safe, unsafe, risky, or less risky (Pattinson et al., 2016). According to the theory of reasoned action, a person's attitude toward a certain behavior has a positive association with their intended behavior (Ajzen & Fishbein, 1980). Indeed, a positive attitude toward security is as important as having secure technology in place (Ismail, 2018). The belief that a security behavior (for example, keeping personal information secure) leads to positive outcomes may differ among employees according to their national culture. Hence, if an employee works in a country where there is more awareness of cybersecurity, and where national cybersecurity policies are more advanced, that employee is more likely to believe that they should behave in a way that maintains smartphone security and minimizes risks. Therefore, a positive attitude toward smartphone security can have a positive influence on an employee's intention to comply. Thus:

H8. Attitude affects employees' behavioral intention toward smartphone-security compliance.

4.4.2 Perceived self-efficacy

Self-efficacy refers to the individual's belief in their ability to perform a particular task (Rogers, 1983; Salleh et al., 2012). When an individual believes that they have the skills needed to do a task, they will take the necessary action (Lee, Larose & Rifon, 2008) and make extra effort to ensure the security of the system (Workman, Bommer & Straub, 2008). Self-efficacy, which is part of coping appraisal, is a significant predictor of security behavior because it is linked to the individual's confidence in performing that behavior (Hanus & Wu, 2016; van Bavel et al., 2019). Within social cognitive theory, it is an important determinant

of behavioral intention because it enables an individual to regulate their own behavioral intention (Rhee, Kim & Ryu, 2009). Education and training can increase a person's self-efficacy by improving their awareness of what to do to prevent or mitigate a security threat. Most countries with cybersecurity policies that aim to protect personal information also provide programs to improve awareness and knowledge (CTIA, 2018). In other words, in those countries the national culture supports people to keep their smartphones and other devices secure. Therefore, citizens of these countries are more likely to have confidence in their ability to protect their smartphones. Hence, self-efficacy can have a significant effect on employees' smartphone-security behavior, but this may vary according to the level of cybersecurity awareness in their country. This is because of the educational programs and awareness campaigns which employees can be exposed to in a more cybersecurity advanced country. This enables them to increase their self-confidence in their ability to keep their smartphones secure. Thus:

H9. Perceived self-efficacy affects employees' behavioral intention toward smartphone-security compliance.

4.4.3 Subjective norms

Subjective norms refer to a person's belief that specific individuals or groups think that the person should or should not behave in a certain way, and to the person's motivation to comply with those views (Ajzen & Fishbein, 1980). Researchers have used this factor to study people's interaction with smartphones and mobile applications (Ameen, 2017; Ameen & Willis, 2018a). In the context of our study, subjective norms refer to employees' perceptions of their managers' and colleagues' opinions on smartphone security and the measures that should be taken. Subjective norms are also linked to the society and national culture within which the company operates. For example, in collectivistic cultures such as the culture in the UAE, individuals are more influenced by the opinions, recommendations, and suggestions of others (Abbasi, Tarhini, Elyas, & Shah, 2015). In individualistic cultures such as the culture in the UK, on the other hand, individuals focus on their own perceptions and are usually less influenced by the opinions of others (Abbasi et al., 2015). Therefore, the significance of subjective norms—the opinions of others on BYOD (smartphone) security—may differ according to the level of collectivism in the country where the employee works. Subjective norms can have a significant effect on an employee's intention to comply with BYOD (smartphone) security in their

organization because they can be influenced by the opinions and recommendations of others around them. In summary, the significance of subjective norms can vary according to the employee's organizational culture, their national culture, and across different cultures in different countries. Therefore:

H10. Subjective norms affect employees' behavioral intention toward smartphone-security compliance.

4.4.4 Perceived risk vulnerability

Perceived risk vulnerability is a person's perception that they will experience negative consequences for behaving in a risky way (Rogers, 1983; Salleh et al., 2012). It also refers to how likely they perceive a security threat to be (Verkijika, 2018) and whether they perceive their device as susceptible to particular threats (Hanus & Wu, 2016). Within the context of smartphone security, perceived risk vulnerability refers to the likelihood that a smartphone is prone to a security threat (Verkijika, 2018). It also refers to the employee's belief that an unwanted incident will happen if they do not act to prevent it—which in turn affects security (Vance et al., 2012). In countries with a high level of cybersecurity awareness, individuals are more aware of the negative consequences of risky behavior. Therefore, the significance of this factor may be modified by national cybersecurity awareness, so it may differ in different countries. This factor contributes to a more proactive approach to smartphone security because it can lead to employees preventing threats before they happen. Thus:

H11. Perceived risk vulnerability affects employees' behavioral intention toward smartphone-security compliance.

4.4.5 Perceived response efficacy

Perceived response efficacy is the degree to which an individual believes that their response to a threat will alleviate it (Rogers, 1983). It focuses on the individual's belief in the effectiveness of the action that they take (Ifinedo, 2012; Rogers, 1983). Previous studies have shown that perceived response efficacy has a significant positive influence on information-security intentions (e.g. Doane et al., 2016; Ifinedo, 2012; Tsai et al., 2016). This factor is linked with employees' knowledge and awareness of the recommended action or behavior. In countries with a high level of national cybersecurity awareness, employees are more aware of

which action to take and, in turn, they are more likely to believe that the response will be effective. An employee who believes that their action is likely to reveal or reduce a threat to their smartphone (and the data stored in it) is more likely to intend to comply with their organization's smartphone-security policies. Therefore:

H12. Perceived response efficacy affects employees' behavioral intention toward smartphone-security compliance.

4.4.6 Perceived severity of sanctions

Perceived severity of sanctions refers to how serious a person thinks the penalties for noncompliance will be. In other words, it refers to an individual's belief that their deviant behavior will or will not be harshly punished (Cheng, Sims & Teegen, 2014). In the context of information security, an organization may penalize an employee for behavior that results in a security breach (Herath & Rao, 2009b). The more severe the individual thinks the punishment will be, the stronger their intention to comply (Siponen et al., 2010; Vance et al., 2012) and the weaker their intention to behave in an undesirable way (Peace et al., 2003). The severity of penalties issued by organizations may differ among countries. For example, in countries where organizations can be penalized for a data breach by law, organizations may issue severe penalties to the employees who are responsible (for example, terminating their employment). Thus:

H13. Perceived severity of sanctions affects employees' behavioral intention toward smartphone-security compliance.

4.4.7 Perceived certainty of sanctions

Perceived certainty of sanctions refers to how certain a person is that they will face a penalty for not behaving in the desired way (D'Arcy & Herath, 2009). In other words, it refers to how certain they are that they will be caught (Cheng et al., 2014) and punished by their organization (Herath & Rao, 2009b). When organizations make it clear that they will punish employees for security breaches caused by behaving inappropriately or misusing their device, their employees are more likely to intend to use their smartphones securely. The probability of being caught and punished has been identified as one of the most important

factors in criminology research (Cheng, Sims & Teegen, 1997; Herath & Rao, 2009b). Merhi and Ahluwalia (2019) explain that in information-security research, certainty refers to certainty of punishment and, more likely, certainty of detection. This factor is important is possibly more important in countries where there is a high level of cybersecurity awareness. When employees are certain that they will be punished due to a risky behavior that can affect the security of their BYOD (smartphone), they become more careful in terms of keeping their smartphones secure. Thus:

H14. Perceived certainty of sanctions affects employees' behavioral intention toward smartphone-security compliance.

4.4.8 Behavioral intention

Intention refers to the individual's mental readiness to behave in a certain way. Accordingly, how a person actually behaves depends on their intention (Ajzen & Fishbein, 1980). Research by Ameen et al. (2018) has found that this factor is significant in individuals' decision-making processes within the context of information technology. Other studies have found that the intention to behave in a way that promotes information security has a significant impact on individuals' actual compliance (e.g. Dang-Pham & Pittayachawan, 2015; Ifinedo, 2012; Tsai et al., 2016; Vance et al., 2012; Verkijika, 2018). Therefore:

H15. Behavioral intention affects employees' actual smartphone-security compliance.

5. Methodology and Data

5.1 Measures

We used multiple items to measure each factor. For each item we used a seven-point Likert scale with anchors ranging from "strongly disagree" to "strongly agree". An exception to this was the factor technological (smartphone-specific) security threats. For this construct, we asked the respondents to rank several smartphone-security threats using a seven-point Likert scale ranging from "extremely low" to "extremely high".

To increase validity, we adopted most of the measurement items from previous studies. We adopted the items for response cost and perceived response efficacy from Vance et al's. (2012) study. To measure perceived

risk vulnerability, we used the items from Putri and Hovav's (2014) study. We measured self-efficacy using three items from Herath and Rao's (2009b) study. To measure attitude, intention, and subjective norms, we adopted other items from Herath and Rao's (2009b) study; however, we modified some of these items to fit the context of this study. We adopted the items for perceived severity of sanctions and perceived certainty of sanctions from studies conducted by Herath and Rao (2009b), Knapp, Marshall, Rainer, & Ford (2005), and Peace et al. (2003). To measure the factor national smartphone cybersecurity policies, we adopted items from studies by Ameen (2017), Ameen and Willis (2018a), and Loch, Straub and Kamel (2003) and modified them to fit the context of national smartphone cybersecurity. We adopted the items for smartphone-specific security threats from recent studies on smartphone-security threats (Dimensional Research, 2017; Tu and Yuan, 2015). We adopted the items for actual behavior from Siponen et al. (2010). To ensure the validity of our research instrument, we carried out a pilot study by sending 30 questionnaires to employees in the UAE. We found no reliability or validity issues. Appendix A shows the final version of the measurement items used.

5.2 Data Collection-The Gen-Mobile Workforce

Previous studies have focused on the security of BYOD technology, including smartphones, tablets, laptops, and USB drives (Baillette et al., 2018; Tu & Yuan 2015; Vignesh & Asha, 2015; Zahadat, Blessner, Blackburn & Olson, 2015). However, research is lacking on cybersecurity issues associated with smartphone use by Gen-Mobile employees in international organizations, especially younger members of the Gen-Mobile workforce. Gen-Mobile employees are aged 18-35 and are heavy adopters of smartphones, which they use for work purposes (Aruba Networks, 2014). This generation of employees is making work life more flexible, with faster communication and greater reach. Despite the prevalence and benefits of using smartphones for work purposes, a report by the renowned Consumer News and Business Channel (CNBC) reveals that less than half of the companies in the US and UK are prepared for cybersecurity attacks (CNBC, 2017). A recent report in the US suggests that the BYOD market will reach nearly US$367 billion by 2022 (up from just US$30 billion in 2014) and that 59 percent of organizations allow employees to use their own devices for work (Lazar, 2017). The US is the world's biggest cybercrime hotspot, and companies in the country are no exception (Business Insider, 2017). In the UAE, 60 percent of the workforce works remotely every week

(Khaleej Times, 2018). According to Aruba Networks (2016), the UAE's Gen-Mobile employees are far more willing to share company data and are notably oblivious towards security. In 2015 the UAE was ranked 19th in the world for online infection risk, positioning it as a high risk country, and 53 percent of these infections came from local threats (Albawaba Business, 2015). This highlights the importance of ensuring smartphone-security compliance among UAE employees.

Available data shows that 95 percent of UK businesses struggle to secure mobile working, and a third of them experience data loss or data breach (Response Source, 2018). Half of UK employers believe that employees' security behavior is a major threat to their company (Fadilpašić, 2017). In addition, recent research has found that a quarter of senior managers and nearly a third of directors in the UK use their smartphones for personal and work purposes (Munarriz, 2018). In total, 14 million people in the UK use their smartphones for work purposes (Munarriz, 2018). However, only 54 percent of organizations in the UK have adopted formal BYOD policies (Jay, 2018). The UK is one of the ten biggest cybercrime hotspots in the world (Business Insider, 2017). It has the most breaches in Europe, with, 43 per cent of businesses reporting cyberattacks in 2017 (Vaidya, 2018). In spite of this fact, the IT security spend in the UK remains low compared with its EU counterparts (Thalese Security, 2018). Table 4 shows how the US, the UK, and the UAE rank according to Hofstede's cultural dimensions (Hofstede, 2018).

Table 4. US, UK, and UAE: Hofstede's cultural dimensions

Country	Power distance	Individualism	Masculinity	Uncertainty avoidance	Long-term orientation	Indulgence
US	40	91	62	46	26	68
UK	35	89	66	35	51	69
UAE	90	25	50	80	-*	-*

Source: Hofstede, 2018
Note: *data from the UAE was not available.

We selected the three countries in this study for the following reasons. First, they rank differently in the Global Cyber-Security Index, which helps reveal how the proposed model fits in different countries with different cybersecurity environments. Second, they contain a large number of global organizations. Third, they rank differently according to Hofstede's cultural dimensions, which allows us to investigate employees' behavior in different organizational settings. To achieve the aim of this study, we collected data from

employees within the Gen-Mobile workforce (aged 18-35) who were working for international companies, owned a smartphone, and had mobility in their approach to work. The companies were in several different industries. We targeted employees in the UK (London), the US (Boston), and the UAE (Dubai). Furthermore, the participants worked for international businesses in different industries in these countries.

5.3 Sampling and Data Screening

We adopted purposive sampling in this research. Using this method enabled us to collect data from participants in the target age group who worked for international companies. Purposive sampling was effective in previous studies within the information systems domain and with target samples who had certain characteristics (Abdel-Wahab, 2008; Ndubisi, 2006). The participants are chosen based on their possession of certain qualities (Etikan, Musa & Alkassim. 2016). That is, they must meet certain criteria in order to be selected (Etikan et al., 2016). Hence, it is different from convenience sampling, in which the participants are selected based on their availability at a given time (Dörnyei, 2007). Purposive sampling is suitable for both quantitative and qualitative techniques (Tongco, 2007). We used two criteria to select the participants. They had to be: (1) aged 18-35 (in the Gen-Mobile workforce); and (2) employees of international companies. Using this purposive sampling method, we distributed 650 questionnaires to participants face to face in London, Boston, and Dubai. We received 579 completed questionnaires from the respondents in the UK, 602 in the US, and 554 in the UAE. The response rate was 89 percent in the UK, 93 percent in the US, and 85 percent in the UAE. Distributing the questionnaires face to face helped us to achieve these high response rates.

We screened the completed responses to ensure that no issues could affect the analysis and the results. To do so, we assessed the data for common method variance and normality issues using the Statistical Package for the Social Sciences (SPSS) version 24. Podsakoff, MacKenzie, Lee and Podsakoff (2003, p. 879) define common method variance as “Variance that is attributable to the measurement method rather than to the construct the measures represent”. This exaggerates the relationships in the theoretical model. Because this study is quantitative and common method variance can be a problem in self-reported studies, we also conducted a Harman’s test. The results did not reveal any issues. To assess for normality, we used the

Kolmogorov-Smirnov test and Shapiro-Wilks test. When skewness and kurtosis are present, it can be assumed that the data are not normally distributed. Some researchers assume that values greater than 3.0 indicate that the data are extremely skewed (Kline, 2005). Our analysis showed that the collected data in the three countries were not normally distributed.

6. Data Analysis and Results

We collected data on demographic factors, such as the respondents' age, gender, and industry type. We also asked the respondents whether they were aware of any BYOD policies in their country. We analyzed the data using PLS-SEM (Hair, Sarstedt, Ringle, & Gudergan, 2017). This method has been used in other studies on information systems and decision-making (e.g. Warkentin, Goel & Menard, 2013; Wu et al., 2014). In addition, PLS-SEM is suitable when the data are not normally distributed (Dijkstra & Henseler, 2015; Henseler, Ringle & Sinkovics, 2009), as is the case in our study. Furthermore, when used with complex models PLS-SEM is more effective than covariance-based structural equation modelling (CB-SEM) (Hair, Hult, Ringle, & Sarstedt, 2014). Therefore, PLS-SEM was justified by the complexity of the model (due to the number of factors included) and the fact that the data are not normally distributed. We conducted the analysis in two stages, assessing the measurement model and then the structural model. We conducted a separate analysis for each country. We present the results in the following sections.

6.1 Descriptive Statistics

For the UK sample, 44 percent of the respondents were aged 18-22, and 56 percent were aged 23-35. Forty-one percent of the respondents were male, while 59 percent were female. The respondents worked in the following industries: automotive (24%), finance (20%), transport (16%), construction (14%), health (11%), utilities (10%), and media (4%). Three respondents did not indicate the industry they worked in. All the respondents were aware of the GDPR and national cybersecurity policies on smartphone use in the UK. They all used their personal smartphones for work purposes. For the US sample, 49 percent of the respondents were aged 18-22, and 51 percent were aged 23-35. Forty-two percent were male and 58 percent were female. The respondents worked in the following industries: finance (15%), transport (15%), construction (14%), automotive (13%), health (11%), manufacturing (11%), education (9%), utilities (7%), and media (4%). Five respondents did not indicate the industry they worked in. Almost all (99%) the respondents were aware of

national cybersecurity policies in the US. They were all aware of the GDPR and they all used their personal smartphones for work purposes. For the UAE sample, 41 percent of the respondents were aged 18-22, while 59 percent were aged 23-35. Most of the respondents (79%) were male and 21 percent were female. The respondents worked in the following industries: finance (34%), utilities (25%), automotive (24%), education (11%), and media (4%). Forty-five percent of the respondents were aware of national cybersecurity policies in the UAE, and 80 percent were aware of the GDPR. All the respondents used their personal smartphones for work purposes. Table 5 shows the descriptive statistics for all three samples.

Table 5. Demographic profile: UK, US, and UAE samples

	UK (%)	US (%)	UAE (%)
Age			
18-22	44	49	41
23-35	56	51	59
Gender			
Male	41	42	79
Female	59	58	21
Industry			
Education	0	9	11
Utilities	10	7	25
Construction	14	14	0
Health	11	11	0
Finance	20	15	34
Transport	16	15	0
Automotive	24	13	24
Manufacturing	0	11	0
Media	4	4	4
Other	0	0	0
Awareness of national policies that can affect BYOD security			
Yes	100	99	45
No	0	1	55
Awareness of the GDPR			
Yes	100	100	80
No	0	0	20
Use of smartphone for work purposes			
Yes	100	100	100
No	0	0	0

6.2 Measurement Model

We tested the measurement model by assessing its reliability, convergent validity, and discriminant validity (Hair et al., 2014; Hair et al., 2017). We analyzed the collected data using SmartPLS 3 software.

Table 6. Reliability and validity assessments: UK, US, and UAE samples

	UK			US			UAE		
	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
AC	0.848	0.908	0.766	0.727	0.844	0.644	0.874	0.941	0.888
ATT	0.754	0.858	0.669	0.808	0.886	0.721	0.679	0.861	0.756
INT	0.809	0.887	0.723	0.717	0.841	0.638	0.867	0.919	0.790
NSCP	0.874	0.914	0.726	0.770	0.866	0.684	0.808	0.887	0.723
PCS	0.798	0.906	0.829	0.859	0.910	0.772	0.873	0.922	0.798
PSS	0.801	0.883	0.715	0.825	0.917	0.847	0.861	0.935	0.878
PV	0.762	0.863	0.677	0.680	0.859	0.753	0.870	0.920	0.794
RC	0.663	0.814	0.593	0.838	0.887	0.663	0.853	0.931	0.872
RE	0.680	0.814	0.594	0.845	0.888	0.613	0.861	0.900	0.644
SE	0.730	0.846	0.648	0.798	0.905	0.827	0.677	0.860	0.754
SN	0.783	0.873	0.697	0.811	0.913	0.841	0.833	0.900	0.750
SSF	0.867	0.904	0.653	0.893	0.918	0.693	0.894	0.934	0.826
TMP	0.791	0.905	0.827	0.832	0.898	0.747	0.793	0.906	0.829

Note: AC = Actual smartphone security compliance behavior; ATT = Attitude; INT = Behavioral intention; NSCP = National smartphone cybersecurity policies; PCS = Perceived certainty of sanctions; PSS = Perceived severity of sanctions; PV = Perceived risk vulnerability; RC = Perceived response cost; RE = Perceived response efficacy; SE = Self-efficacy; SN = Subjective norms; SSF = Smartphone-specific security threats; TMP = Top-management participation.

We assessed the reliability and convergent validity of the measurement model in the UK, US, and UAE samples (see Table 6). All the AVE values for all three samples are higher than the threshold value of 0.5 (Hair et al., 2017). In addition, the Cronbach's alpha values for most of the measurement items are higher than 0.7 (Hair et al., 2017). Exceptions are RC (0.663) and RE (0.680) in the UK sample, PV (0.680) in the US sample, and ATT (0.679) and SE (0.677) in the UAE sample. These values are only slightly lower than 0.7, hence we kept them. There are no issues in terms of factor loadings. In addition, all composite reliability values are higher than the threshold of 0.7 in all three samples (Hair et al., 2014; Hair et al., 2017). We assessed discriminant validity in the three samples by using the Fornell-Larcker criterion. The results show that the constructs share more variance with their own indicators than they share with the indicators of the other constructs, so there are no issues in terms of discriminant validity (Hair et al., 2014). Our assessment of the cross-loadings shows that each construct loads higher on its own indicators than on the indicators of the other constructs. Some of the factor loadings are lower than the threshold value of 0.7 (Hair et al., 2014). Hence, we deleted these items. We assessed collinearity using the variance inflation factor (VIF) with a threshold value of 5 (Hair et al., 2014). All VIF values are lower than the threshold value of 5. We used these VIF values to assess multicollinearity. All VIF inner values are lower than 5.

6.3 Structural Model

To test the structural model, we assessed the significance and magnitude of the hypothesized relationships by following the bootstrapping procedure in PLS (Hair et al., 2014). Table 7 summarizes the results of the assessment for all three samples.

Table 7. Hypotheses testing: UK, US, and UAE samples

		UK			US			UAE		
Hypothesis	Relationship	T statistic (|O/STDEV|)	p value	Result	T statistic (|O/STDEV|)	p value	Result	T statistic (|O/STDEV|)	p value	Result
H1	NSCP -> INT	0.534	0.593	Not supported	4.365	0.000	Supported	3.748	0.000	Supported
H2	NSCP -> AC	2.673	0.008	Supported	1.108	0.268	Not supported	2.577	0.010	Supported
H3	RC -> INT	1.872	0.062	Not supported	1.974	0.047	Supported	8.310	0.000	Supported
H4	RC -> AC	3.901	0.000	Supported	1.592	0.112	Not supported	6.078	0.000	Supported
H5	TMP -> INT	3.218	0.001	Supported	3.669	0.000	Supported	5.193	0.000	Supported
H6	TMP -> AC	0.600	0.549	Not supported	2.035	0.042	Supported	2.701	0.007	Supported
H7	SSF -> INT	0.911	0.363	Not supported	1.400	0.162	Not supported	7.515	0.000	Supported
H8	ATT -> INT	2.343	0.020	Supported	3.943	0.000	Supported	3.844	0.000	Supported
H9	SE -> INT	1.990	0.047	Supported	1.163	0.245	Not supported	1.450	0.148	Not supported
H10	SN -> INT	2.884	0.004	Supported	0.124	0.901	Not supported	2.467	0.014	Supported
H11	PV -> INT	4.500	0.000	Supported	0.845	0.399	Not supported	1.372	0.171	Not supported
H12	RE -> INT	1.731	0.084	Not supported	1.971	0.049	Supported	1.554	0.121	Not supported
H13	PSS -> INT	9.684	0.000	Supported	0.762	0.447	Not supported	0.601	0.548	Not supported
H14	PCS -> INT	0.962	0.337	Not supported	2.274	0.023	Supported	11.608	0.000	Supported
H15	INT -> AC	8.655	0.000	Supported	2.279	0.023	Supported	3.254	0.001	Supported

For the UK sample, H2 (*p* value=0.008), H4 (*p* value=0.000), H5 (*p* value=0.001), H8 (*p* value=0.020), H9 (*p* value=0.047), H10 (*p* value=0.004), H11(*p* value=0.000), H13 (*p* value=0.000), and H15 (*p* value=0.000) are supported. H1 (*p* value=0.593), H3 (*p* value=0.062), H6 (*p* value=549), H7 (*p* value=363), H12 (*p* value=0.084), and H14 (*p* value=0.337) are not supported because their p values are greater than 0.05 (Hair et al., 2017). For the US sample, H1 (*p* value=0.000), H3 (*p* value=0.047), H5 (*p* value=0.000), H6 (*p* value=0.042), H8 (*p* value=0.000), H12 (*p* value=0.049), H14 (*p* value=0.023), and H15 (*p* value=0.023) are supported. H2 (*p* value=0.268), H4 (*p* value=0.112), H7 (*p* value=0.162), H9 (*p* value=0.245), H10 (*p* value=0.901), H11 (*p* value=0.399), and H13 (*p* value=0.447) are not supported. For the UAE sample, H1 (*p* value=0.000), H2 (*p* value=0.010), H3 (*p* value=0.000), H4 (*p* value=0.000), H5 (*p* value=0.000), H6 (*p* value=0.007), H7 (*p* value=0.000), H8 (*p* value=0.000), H10 (*p* value=0.014), H14 (*p* value=0.000), and H15 (*p* value=0.001) are supported. H9 (*p* value=0.148), H11 (*p* value=171), H12 (*p* value=0.121), and H13 (*p* value=0.548) are not supported.

The results show that the model can explain 67 percent (R^2=0.667) of behavioral intention and 40 percent (R^2=0.398) of actual smartphone-security compliance among employees in the UK. It can explain 79 percent (R^2=0.794) of behavioral intention and 57 percent (R^2=0.571) of actual smartphone-security compliance among employees in the US. In the UAE, it can explain 83 percent (R^2=0.832) of behavioral intention and 58 percent (R^2=0.578) of actual smartphone-security compliance. The model's explanatory power is highest in the UAE.

6.4 Multi-Group Analysis

To test the differences across all three samples, we used partial least squares-multi group analysis (PLS-MGA). This nonparametric method of analysis, introduced by Henseler et al. (2009), tests the differences between the path coefficients of two groups (Henseler et al., 2009; Sarstedt, Henseler & Ringle, 2011). PLS-MGA directly compares group-specific bootstrap estimates from each bootstrap sample. A *p* value of the difference between the path coefficients lower than 0.05 or higher than 0.95 at the 5 percent level indicates that there are significant differences between specific path coefficients across two groups (Henseler et al., 2009; Sarstedt et al., 2011). We compared the groups in pairs (UK vs US, UAE vs UK, and US vs UAE).

The results of the PLS-MGA analysis (Table 8) support the differences in path significance between the three samples included in the study.

Table 8. Multi-group analysis across samples

		UK vs US		UAE vs UK		US vs UAE	
Hypothesis	Relationship	Path coefficients: difference	*p* value	Path coefficients: difference	*p* value	Path coefficients: difference	*p* value
H1	NSCP -> INT	0.287	1.000	0.151	0.000	0.136	0.019
H2	NSCP -> AC	0.012	0.572	0.172	0.039	0.160	0.950
H3	RC -> INT	0.121	0.051	0.287	0.091	0.166	0.999
H4	RC -> AC	0.085	0.098	0.266	0.000	0.351	1.000
H5	TMP -> INT	0.081	0.948	0.049	0.091	0.032	0.252
H6	TMP -> AC	0.061	0.834	0.071	0.188	0.010	0.541
H7	SSF -> INT	0.027	0.311	0.216	0.218	0.244	1.000
H8	ATT -> INT	0.154	0.998	0.115	0.991	0.269	0.999
H9	SE -> INT	0.019	0.375	0.113	0.991	0.094	0.072
H10	SN -> INT	0.098	0.025	0.151	0.952	0.047	0.868
H11	PV -> INT	0.143	0.011	0.145	0.998	0.001	0.507
H12	RE -> INT	0.099	0.975	0.080	0.019	0.019	0.352
H13	PSS -> INT	0.387	0.072	0.351	0.330	0.082	0.055
H14	PCS -> INT	0.066	0.160	0.469	0.998	0.417	0.996
H15	INT -> AC	0.341	0.330	0.780	0.999	0.439	0.000

Note: p values in bold indicate a significant difference

There are significant differences between all three samples for H1 (NSCP -> INT). For H2 (NSCP -> AC), there are significant differences between the UAE and UK, and between the US and the UAE. For H3 (RC -> INT), there are significant differences between the UK and US, and between the US and the UAE. For H4 (RC -> AC), there are significant differences between the UAE and UK, and between the US and the UAE. There are no significant differences between the samples for H5 (TMP -> INT) and H6 (TMP -> AC). For H7 (SSF -> INT), there are significant differences between the US and the UAE. For H8 (ATT -> INT), there are significant differences among all three samples. For H9 (SE -> INT), there are significant differences between the UAE and the UK. For H10 (SN -> INT), there are significant differences between the UK and

the US, and between the UAE and the UK. For H11 (PV -> INT) and H12 (RE -> INT), there are significant differences between the UK and the US, and between the UAE and the UK. There are no significant differences between the samples for H13 (PSS -> INT). For both H14 (PCS -> INT) and H15 (INT -> AC), there are significant differences between the UAE and the UK, and between the US and the UAE. Overall, the PLS-MGA analysis confirms the differences in the structural model in each separate country. Therefore, the results show that there are significant differences between the samples.

7. Discussion

This study deepens our understanding of how employees' information-security compliance behavior is influenced by national cybersecurity policies and security threats that are specific to smartphones. It proposes the holistic ESSC model, which accounts for national, organizational, technological (smartphone-specific) and personal factors. To the best of our knowledge, the current study is the first to investigate the effects of national cybersecurity policies and smartphone-specific security threats on employees' smartphone-security compliance in a cross-cultural context. In doing so it fills a gap in the literature, which has mainly focused on the organizational context. Our findings show that employees' behavior is influenced by not only their personalities and their organizations but also national cybersecurity policies and security threats that are specific to smartphones. In addition, our findings reveal that there are differences in employees' smartphone-security behavior in the UK, the US, and the UAE. National cybersecurity policies have significant effects on behavioral intention (H1) among employees in both the US and the UAE, but not in the UK. They have a significant effect on actual smartphone-security compliance (H2) among employees in the UK and the UAE. However, almost half of employees surveyed in the UAE are not aware of national policies that are specific to BYOD security; they are aware of the GDPR only. Because BYODs are used within and outside organizations for personal and work purposes, their secure use is covered by policies and regulations beyond the organizational context. Laws and regulations such as the GDPR in Europe require companies to report all suspected security breaches, which puts pressure on companies and their employees, influencing their behavior. Our findings suggest that employees in all three countries are aware of the impact of these laws and regulations on smartphone security and how they affect the secure use of these devices. This factor is particularly important for employees in the UAE because it has a significant effect on their behavioral

intention and their actual smartphone-security compliance. National cybersecurity policies differ among countries and national advances in cybersecurity. However, they have a significant influence on employees' smartphone-security compliance. These findings show that national policies do not only affect the adoption of smartphones as indicated in Ameen et al.'s (2018) study but they also affect post-adoption issues, more specifically, smartphone security behavior.

Response cost has a significant effect on behavioral intention (H3) in the US and the UAE, but not in the UK. However, this factor has a significant effect on actual smartphone security compliance (H4) in the UK and the UAE, but not in the US. Employees in the UK and the UAE consider the amount of effort and time they need to put in to ensure smartphone security as an important factor. This is consistent with the findings of studies conducted by Rogers (1983) and Xiao et al. (2016). Surprisingly, employees in the US are not concerned with how much time or effort they need to invest to keep their smartphones secure. In addition, support from the top management has a significant effect on behavioral intention (H5) among employees in all three countries. This is consistent with the findings of Liang et al. (2007) and Hu et al. (2012). Therefore, to increase employees' intention to comply, managers need to articulate a clear vision and strategy for smartphone security, and they should establish clear goals and objectives for achieving a high level of security. Similarly, this factor has a significant effect on actual smartphone-security compliance (H6) among employees in the US and the UAE, but not in the UK. The insignificant effect of support from top managers on employees in the UK is surprising.

It is also surprising that smartphone-specific security threats do not have a significant effect on behavioral intention (H7) among employees in the UK or in the US. However, this remains a salient factor in young employees' smartphone-security compliance in the UAE. A possible explanation for these results is that employees in the UK and the US are more used to using smartphones; because they are more familiar with the related security threats, those threats may have less influence on their intention to comply with smartphone-security policies. Employees in the UAE are less aware of the security issues associated with using smartphones, as stated in studies by Olalere et al. (2015) and Murray (2014). Examples of threats associated with smartphones include the operating system, mobile applications, and cyberattacks (e.g. phishing, malware, and spyware) targeted at the device and its applications (Wandera, 2018c). In addition,

in all three countries, employees' attitude to smartphone-security compliance has a significant influence on their behavioral intention (H8). This is consistent with the findings of the studies conducted by Ismail (2018) and Pattinson et al. (2016). Employees are more likely to want to comply with policies on smartphone security if they believe that doing so will benefit them and their organizations. This is strengthened by a belief that it is important to enforce their organization's smartphone-security policies, practices, and use of associated technologies.

Self-efficacy has a significant effect on behavioral intention (H9) among employees in the UK only. Previous studies have found that employees make more effort to secure their devices when they have confidence in their ability to deal with a security threat (Hanus & Wu, 2016; Salleh, 2012; Workman et al., 2008; van Bavel, 2019). Our analysis shows that employees in the US and the UAE lack this confidence; they do not feel that they have the skills needed to follow their organization's smartphone-security policies, and they do not feel comfortable with doing so without assistance. Furthermore, subjective norms have a significant effect on behavioral intention (H10) among employees in the UK and the UAE, which indicates that they pay attention to their colleagues' opinions on whether they should follow smartphone-security policies. This contradicts the findings of the studies conducted by Ameen (2017) and Ameen and Willis (2018a), who found that the opinions of others do not affect how people use smartphones. The UK is an individualistic society, so our findings also contradict the assumption that employees in individualistic cultures are not influenced by other people's opinions and recommendations.

Perceived risk vulnerability has a significant effect on behavioral intention (H11) among employees in the UK only. This suggests that employees in the UK are aware of the negative consequences that are likely to result from using smartphones in a way that puts information security at risk. Meanwhile, employees in the US and the UAE are not as aware of the threats that result from using smartphones inappropriately or not complying with their organization's smartphone-security policies. This contradicts the findings of previous studies (e.g. Hanus & Wu, 2016; Salleh et al. 2012; Verkijika, 2018). Furthermore, response efficacy has a significant effect on behavioral intention (H12) among employees in the US only. This suggests that these employees believe that acting in line with their organization's smartphone-security policies will reduce security threats to their companies and themselves. This significant effect is consistent with the findings of

previous research (e.g. Doane et al., 2016; Ifinedo, 2012; Tsai et al., 2016). In addition, perceived severity of sanctions has a significant effect on behavioral intention (H13) among employees in the UK only. Employees in the US and the UAE do not seem to be affected by the possibility of being penalized by their organizations for noncompliance; they assume that the penalties are not severe for using their smartphones in a way that may lead to a data breach. This is inconsistent with the findings of Siponen et al. (2010) and Vance et al. (2012). In contrast, employees in the UK fear the penalties they may face for behavior that could put their organization's information security at risk. This difference may be associated with the enforcement of the GDPR in the UK. Furthermore, perceived certainty of sanctions has a significant effect on behavioral intention (H14) among employees in the US and the UAE, but not in the UK. Therefore, for employees in the UAE and the US, their view on the likelihood of being caught and punished is an important determinant of their intended smartphone-security compliance. This is consistent with the findings of previous studies (e.g. Cheng et al., 2014; Herath & Rao, 2009; Merhia & Ahluwalia, 2019). The situation is the opposite for employees in the UK, whose behavioral intention is influenced by their perceptions of the severity rather than the certainty of the related sanctions. Finally, in all three countries, employees' intention to comply with their organization's smartphone-security policies has a significant effect on how they actually behave (H15).

Our findings support the applicability of our proposed holistic model which integrates national, organizational, technological (smartphone-specific) and personal factors, despite differences in the significance of the factors in a cross-cultural context. The following factors determine employees' smartphone-security compliance in organizations in all three countries: national cybersecurity policies, attitude, and top-management participation. Among employees in the UK, the following factors are also significant: self-efficacy, subjective norms, response cost, perceived risk vulnerability, and perceived severity of sanctions. In the US, the following additional factors are significant: response cost, response efficacy, and perceived certainty of sanctions. Finally, in the UAE, significant factors also include response cost, technology (smartphone-specific) security threats, subjective norms, and perceived certainty of sanctions. This shows the variance in the significance of the determinants of employees' BYOD security compliance. The findings also show that the effects of national factors (national cybersecurity policies) and

organizational factors (top management support) remain significant in different countries despite the differences in their cybersecurity readiness.

8. Theoretical and Practical Contributions

8.2 New Theoretical Contributions

This study makes three contributions to theory. First, our research serves as the leading effort to understand how national cybersecurity policies and BYOD (smartphone) specific security threats affect employees' smartphone-security compliance. This addresses the gap in the literature created by focusing on only the individual, organizational, and (more recently) group levels (e.g. Cram et al., 2017; Dang-Pham & Pittayachawan, 2015; Hu et al., 2012; Hwang & Cha, 2018; Janmaimool, 2017; Johnston et al., 2019; Olalere et al., 2015; Putri & Hovav, 2014; Salleh et al., 2012; Siponen, 2006; Tu & Yuan, 2015). Furthermore, our study is the first to focus on national factors and technology-specific security threats (in this case, threats specific to smartphones).

National policies and advances in cybersecurity vary by country, but our findings suggest that these factors have a significant influence on employees' smartphone-security compliance and the content of associated organizational policies. These national level policies also create variance in employees' behavior. Furthermore, security threats that are specific to BYODs (smartphones) have a significant influence on employees even if they work in a country that is less advanced in cybersecurity.

Second, our research responds to calls for an approach that covers all the important aspects of information security in organizations (Soomro et al., 2016). Our new theoretical model, the ESSC, combines and extends three well-known theories that apply to information-security behavior: protection motivation theory (Rogers, 1983), general deterrence theory (Beccaria, 1963; Gibbs, 1975), and theory of reasoned action (Fishbein & Ajzen, 1975). Our model extends these theories by integrating national cybersecurity policies and BYOD (smartphone)-specific security threats. It groups the factors into national, organizational, technological (smartphone-specific) and personal categories. This contributes to a better understanding of the main areas to consider when studying employees' smartphone-security compliance. Our findings suggest that future

research should also go beyond the individual, group, and organizational phenomena when studying this behavior.

Third, our findings show that a positive attitude among employees, support from top managers, and national cybersecurity policies have a significant influence on employees, regardless how advanced a country is in cybersecurity. The findings of our cross-cultural study challenge existing theories on information security within organizations. Previous studies have reported that the following factors have a significant impact: response cost, self-efficacy, subjective norms, perceived risk vulnerability, response efficacy, perceived severity of sanctions, and perceived certainty of sanctions (Doane et al., 2016; Herath & Rao, 2009a; Herath & Rao, 2009b; Ismail, 2018; Ifinedo, 2012; Rhee et al., 2009; Tsai et al., 2016; Vance et al., 2012). However, our findings reveal important differences in the significance of these factors among employees in different countries. Therefore, theories on information security should consider these differences.

8.3 Managerial and Policy Implications

We have found that there are significant differences in smartphone-security behavior among employees in the UK, the US, and the UAE. This is a major challenge for managers in international companies with different teams in different countries. Simply having a BYOD cybersecurity policy is not enough; managers and policy-makers need to adjust their approach to communicating and implementing the policy in line with the needs, skills, and preferences of employees in different regions of the world.

Managers who support smartphone-security programs and policies are more likely to make employees feel motivated to actively ensure that their smartphones and the data that can be accessed through these devices are secure. We have found that support from top management and employees' attitude to smartphone security are important factors for smartphone security in all three countries. Our results have major implications for policy-makers and company managers who are developing smartphone-security policies. Employees in the UAE lack awareness of specific national BYOD security policies rather than lacking awareness of the GDPR only. They are less aware of the security threats that are related to using their smartphones. Hence, policy-makers and managers need to collaborate to develop effective national cybersecurity policies that focus on BYODs, especially smartphones, and ensure that employees are aware of the requirements of these policies.

This is important because national policies on smartphone security have a significant effect on employees' smartphone-security compliance.

Managers in organizations in the US and in the UAE should develop training programs and coaching sessions to build employees' confidence and ability in following company policies on smartphone security and dealing with related security threats. Our research suggests that employees in these two countries find it difficult to follow these policies because they lack self-efficacy. Therefore, improving their knowledge and skills is important for ensuring smartphone security and minimizing data breaches. Similarly, managers need to develop programs to raise awareness of smartphone security among employees in the US and the UAE. Our findings suggest that these employees lack awareness of the threats to information security that are associated with using smartphones inappropriately. Programs are needed to educate these employees on the latest trends in cyberattacks and how to protect their devices. We found that in general, employees have a positive attitude to smartphone security, which suggests that awareness-raising programs will improve their compliance. Managers should tailor the programs to suit the preferences and needs of employees in specific countries. Such an approach will help to build positive subjective norms on smartphone security, which proved to have a strong influence on employees in the UAE and the UK.

Our results reveal that the introduction of the GDPR has encouraged international organizations to improve their measures for keeping business and customer information secure, including on smartphones. The act plays an important role in putting pressure on organizations to ensure information security to protect their data and their customers' data. This includes companies in the EU region (for example in the UK) and any company outside the EU region (for example in the US and UAE) that targets or deals with this region. However, the regulation does not account for human error, which is a major security issue for organizations. Our results show that national smartphone cybersecurity policies have a significant effect on behavioral intention and actual smartphone-security compliance among employees in all three countries. Therefore, managers should continue to emphasize the importance of following these policies. Doing so will raise employee awareness of the penalties and other consequences that their organizations may face in the case of a data breach. Also, this study has found that response efficacy has no effect on employee compliance in the UK or the UAE, which suggests that these employees do not wholly believe that following their

organizations' smartphone-security policies will reduce the threat of information breaches. Therefore, organizations operating in the UK or the UAE need to assess the reasons behind this and identify ways to improve their smartphone-security policies or communicate the effectiveness of their existing policies to employees. Moreover, in the US and UAE, where the mobile workforce is an important employee segment, organizations should clarify the likelihood of the information-security threats associated with noncompliant use of smartphones.

9. Limitations and Future Research

Although this study provides interesting results and insights, it has some limitations. First, it focuses on Gen-Mobile employees. Future research is needed on older employees, who may use smartphones less extensively and may not be as experienced in using them securely. Comparing the results with our findings may identify interesting differences. Second, our results show that employees behave differently in the three countries we selected. Future research is needed on other countries and compare the findings to the findings of our study. Third, our study focused on employees who worked in large international companies in three advanced markets: the UK, the US and the UAE. Fourth, while our model provides a holistic overview of employees' mobile security behavior in the three countries by integrating three of the most well-known theories in the area of security behavior and it mirrors the complexity of the issue the research attempted to tackle, it includes a high number of hypotheses and factors which we have categorized into: national, organizational, technological and personal factors. Future studies can focus on the factors proved to have significant effects in our study to avoid complexities in developing models on employees' security behavior. Fifth, our findings were based on data collected from employees working in international companies in different industries namely: education, utilities, construction, health, finance, transport, automotive, manufacturing and media. We believe that collecting data from employees in different industries has had an impact on our results. Future studies can focus further on the moderating effects of industry type on employees' BYOD (smartphone) security compliance behavior and industry type-based differences in terms of the impact of the GDPR on this behavior.

10. Conclusion

This study represents a pioneering effort in the information-security literature to analyze the effects of national, organizational, technological (smartphone-specific), and personal factors in order to deepen the understanding of information-security behavior among Gen-Mobile employees in a cross-cultural context. The study also contextualizes and validates extant theories on individuals' information-security behavior by combining and extending three widely used theories in this domain (protection motivation theory, general deterrence theory, and theory of reasoned action) to develop a new model: the ESSC. The findings show interesting variations across the three countries investigated (US, UK, and UAE) in the significance of the factors included in the ESSC. Our study reveals important differences in smartphone-security compliance in international companies on the national level. Therefore, managers and policy-makers need to take a more holistic approach to ensuring smartphone-security compliance among Gen-Mobile employees in different countries by focusing on interventions on the national, organizational, technological (smartphone-specific) and personal levels. In addition, they should develop more effective smartphone-security policies that account for human error and build awareness of these policies among employees. Overall, this study contributes to a better understanding of how national cybersecurity policies and smartphone-specific security threats influence employees' information-security compliance behavior.

Appendix A. Measurement items

Factor/item	Source
Top management participation	Hu et al. (2012)
TMP1: Senior managers of our company have articulated a clear vision about smartphone security.	
TMP2: Senior managers of our company have formulated a clear strategy for achieving a high degree of smartphone security.	
TMP3: Senior managers of our company have established clear goals and objectives for achieving a high degree of smartphone security.	
Attitude	Herath and Rao (2009b)
ATT1: I believe that it is beneficial for an organization to establish clear smartphone-security policies, practices, and technologies.	
ATT2: I believe that it is useful to for an organization to enforce its smartphone-security policies, practices, and technologies.	
ATT3: I believe that it is a good idea for an organization to establish clear smartphone-security policies, practices, and technologies.	

Subjective norms	Herath and Rao (2009b)
SN1: People who are influential to me would think that I should follow the policies and procedures and use the security technologies for smartphones.	
SN2: People who are important to me would think that I should follow the policies and procedures and use the security technologies for smartphones.	
SN3: People whom I respect would think that I should follow the policies and procedures and use the security technologies for smartphones.	
Behavioral intention	Herath and Rao (2009b)
INT1: I intend to follow the smartphone-security policies and practices for using smartphones at work.	
INT2: I intend to use the smartphone-security technologies for using smartphones at work.	
INT3: It is possible that I will comply with organizational smartphone-security policies to protect the organization's data.	
Self-efficacy	Herath and Rao (2009b)
SE1: I would feel comfortable following most of the smartphone-security policies on my own.	
SE2: If I wanted to, I could easily follow smartphone-security policies on my own.	
SE3: I would be able to follow most of the smartphone-security policies even if there was no one around to help me.	
Perceived risk vulnerability	Putri and Hovav (2014)
PV1: I could be subjected to an information-security threat, if I don't comply with my organization's smartphone-security policy.	
PV2: A security problem to my organization's information could occur if I don't comply with my organization's smartphone-security policy.	
PV3: A security problem to my personal data could occur if I don't comply with my organization's smartphone-security policy.	
Response cost	Vance et al. (2012)
RC1: Complying with smartphone-security policy interferes with my work.	
RC2: Complying with smartphone-security policy interferes with the personal use on my device.	
RC3: There are too many overheads associated with complying with smartphone-security policies.	
RC4: Complying with smartphone-security policy would require considerable investment of effort other than time.	

RC5: Complying with smartphone-security policy would take considerable amount of my working time.	
RC6: Complying with smartphone-security policy would take considerable amount of my personal time.	
Perceived response efficacy	Vance et al. (2012)
RE1: Complying with smartphone-security policy reduces the security threat to my organization's information.	
RE2: Complying with smartphone-security policy reduces the security threat to my personal data.	
RE3: If I comply with smartphone-security policy, mobile security problems in my organization will be scarce.	
RE4: If I comply with smartphone-security policy, my mobile device related security problems will be scarce.	
RE5: Compliance with smartphone-security policy helps to reduce IS security problems in my organization.	
RE6: Compliance with smartphone-security policy helps me reduce security problems with my own personal data.	
Perceived severity of sanctions	Herath and Rao (2009b); Knapp et al. (2005); Peace et al. (2003).
PSS1: The organization disciplines employees who break information-security rules.	
PSS2: My organization terminates employees who repeatedly break security rules.	
PSS3: If I were caught violating organization information-security policies, I would be severely punished.	
Perceived certainty of sanctions	Herath and Rao (2009b); Knapp et al. (2005); Peace et al. (2003).
PCS1: Employee computer practices are properly monitored for policy violations.	
PCS2: If I violate organization security policies, I would probably be caught.	
National smartphone cybersecurity policies	Ameen (2017); Ameen and Willis (2018a); Loch et al. (2003)
NSCP1: I am aware of the smartphone-security policies in my country.	
NSCP2: I find the smartphone-security policies in my country effective.	
NSCP3: I believe the smartphone-security policies in my country influence my awareness of smartphone security in my organization.	
NSCP4: The Government's cybersecurity initiatives are working well.	
Actual smartphone security compliance behavior	Siponen et al. (2010); D'Arcy and Greene (2014)

AC1: I comply with smartphone-security recommendations	
AC2: I do my best to strictly follow smartphone security rules and procedures	
AC3: I am certain that I will follow organizational smartphone security recommendations (if they exist)	
Smartphone-specific security threats	Dimensional Research (2017); Tu and Yuan (2015)
SSF1: Threat of physical loss of the device	
SSF2: Threats associated with connecting to different networks	
SSF3: Threats associated with using different mobile applications	
SSF4: Threats associated with data breaches	
SSF5: The mixed use of smartphones for personal and business purposes	
SSF6: Privacy issues	

References

Abbasi, M. S., Tarhini, A., Elyas, T., & Shah, F. (2015). Impact of individualism and collectivism over the individual's technology acceptance behaviour: A multi-group analysis between Pakistan and Turkey. *Journal of Enterprise Information Management*, 28(6), 747–768.

Abdel-Wahab, A. G. (2008). Modeling students' intention to adopt e-learning: A case from Egypt. *The Electronic Journal of Information Systems in Developing Countries*, 34(1), 1–13.

Accenture. (2017). Cost of cyber crime study 2017 insights on the security investments that make a difference. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf// (Accessed 4 April 2020).

Act Systems. Mobile devices and GDPR – how will you manage?. (2018). https://www.actsystems.co.uk/2018/05/14/mobile-devices-and-gdpr-how-will-you-manage /(Accessed 22 September 2019).

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl, J. Beckmann, Action control (11–39). Berlin, Heidelberg: Springer.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32(4), 665–683.

Ajzen, I. (2005). Attitudes, personality, and behavior. London, UK: McGraw-Hill Education.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Albawaba Business. Kaspersky Lab reports UAE among the top-20 countries facing the greatest risk of online infection in 2015. (2015). http://www.albawaba.com/business/pr/kaspersky-lab-reports-uae-among-top-20-countries-facing-greatest-risk-online-infection-2 (Accessed 22 September 2019).

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42, 56–65.

Amankwah-Amoah, J. & Wang, X., (2019). Opening editorial: contemporary business risks: an overview and new research agenda. *Journal of Business Research*, 97 (1), 208-211.

Ameen, N. (2017). Arab users' acceptance and use of mobile phones: A case of young users in Iraq, Jordan and UAE (Doctoral dissertation, Anglia Ruskin University).

Ameen, N., & Willis, R. (2018a). A generalized model for smartphone adoption and use in an Arab context: A cross-country comparison. *Information Systems Management*, 35(3), 254–274.

Ameen, N., & Willis, R. (2018b). An examination of the role of national IT development and infrastructure in models for smartphone adoption and use: The cases of Iraq, Jordan and the UAE. In Y. K. Dwivedi, N. P. Rana, E. L. Slade, M. A. Shareef, M. Clement, A. Simintiras, B. Lal (Eds), Emerging markets from a multidisciplinary perspective: Challenges, opportunities and research agenda (161–194). Cham: Springer.

Ameen, N., Willis, R., & Shah, M. H. (2018). An examination of the gender gap in smartphone adoption and use in Arab countries: A cross-national study. *Computers in Human Behavior*, 89, 148–162.

Arage, T., Belanger, F., & Tesema T. (2016). Investigating the moderating impact of national culture in information systems security policy violation: The case of Italy and Ethiopia. Mediterranean Conference on Information Systems (MCIS) Proceedings (1-9). http://aisel.aisnet.org/mcisI016/56 (Accessed 22 September 2019).

Aruba Networks. Are you ready for #gen mobile? How a new group is changing the way we work, live and communicate. (2014). https://www.arubanetworks.com/pdf/solutions/GenMobile_Report.pdf (Accessed 22 September 2019).

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management*, 43, 76–84.

Bandura, A. (1986). Social foundations of thought and action. Englewood Cliffs, NJ: US: Prentice-Hall, Inc.

Bauer, S. (2016). The role of information security awareness for promoting information security policy compliance in banks (Doctoral dissertation, WU Vienna University of Economics and Business).

Beccaria, C. (1963). On crimes and punishment. New York, NY: Macmillan.

Bing, C. (2018). New global cybersecurity center announced at Davos. https://www.cyberscoop.com/new-global-cybersecurity-center-announced-davos//Accessed 22 September 2019.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, 87, 87–97.

Blythe, J. M., Coventry, L. M., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. Symposium on Usable Privacy and Security (SOUPS) 2015, July 22- 24, 2015, Ottawa, Canada, 103-122.

Brewster, C., Chung, C., & Sparrow, P. (2016). Globalizing human resource management. Global HRM, 2nd ed. Routledge, New York.

British Telecom. People, productivity and the digital workplace: How mobile and collaboration services can boost productivity. Digital employee research (2018). 2018. https://www.globalservices.bt.com/content/dam/globalservices/documents/whitepapers/people-productivity-and-the-digital-workplace-13th-march-2018.pdf (Accessed 22 September 2019).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study on rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.

Business Insider. The world's 10 biggest cybercrime hotspots in 2016, ranked. (2017). https://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5?r=UK&IR=T (Accessed 22 September 2019).

Cheng, H., Sims, R., & Teegen, H. (1997). To purchase or to pirate software: An empirical study. *Journal of Management Information Systems*, 13(4), 49–60.

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, 38, 220–228.

Cho, S., & Walton, L. (2009). Integrating emotion and the theory of planned behavior to explain consumers' activism in the Internet web site. In Yamamura, K., Proceedings of the Twelfth Annual International Public Relations Research Conference, Florida, 95-101.

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, 12(6), 659–673.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2), 189–211.

Connolly, L., Lang, M., & Tygar, D. (2014). Managing employee security behaviour in organisations: The role of cultural factors and individual values. In N. Cuppens-Boulahia, Cuppens F., Jajodia S., Abou El Kalam A., Sans T. (eds) ICT Systems Security and Privacy Protection. Proceedings of the IFIP International Information Security Conference (417–430). Berlin, Heidelberg: Springer.

CNBC. Cybercrime costs the global economy $450 billion: CEO. (2017). https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (Accessed 22 September 2019).

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6), 605–641.

CTIA. Today's mobile cybersecurity: Protected, secured and unified. (2018). http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf (Accessed 22 September 2019).

Cyber Security Insiders. Insider threat: 2018 report. (2018). https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (Accessed 22 September 2019).

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, 48, 281–297.

D'Arcy, J. & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*. 22(5), 474-489.

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.

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., Garcia-Sanchez, P., Fernandez-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. Computer Communications, 68, 83–95.

Department for Digital, Culture, Media and Sport. (2019). Cyber Security Breaches Survey 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875799/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised.pdf (Accessed 4 April 2020).

Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modelling. *MIS Quarterly*, 39(2), 297–316.

Dimensional Research. The growing threat of mobile device security breaches: A global survey of security professionals. (2017). https://blog.checkpoint.com/wpcontent/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf (Accessed 22 September 2019).

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of protection motivation theory. *Computers in Human Behavior*, 60, 508–513.

Doargajudhur, M. S., & Dell, P. (2018). Impact of BYOD on organizational commitment: An empirical investigation. *Information Technology & People*. doi:10.1108/ITP-11-2017-0378.

Dörnyei, Z. (2007). Research methods in applied linguistics. New York, NY: Oxford University Press.

Dowle, C., Data protection in United Arab Emirates: Overview. (2018). https://uk.practicallaw.thomsonreuters.com/0-518-8836?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1 (Accessed 22 September 2019).

El-Den, J., & Dangi, K. (2016). A comparative study and analysis between the (positive traits and personal strengths) PP model and current security compliance models. Proceedings of the Eighth European Conference on Intellectual Capital (p. 79). ECIC 2016 Venice, Italy, 12-13 May 2016. Academic Conferences and Publishing.

Endpoint Protector. EU vs US: How do their data privacy regulations square off?. (2018). https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off (Accessed 22 September 2019).

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4.

European Commission. Bring your own device: A major security concern. (2017). https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_BYOD%20-%20a%20major%20security%20concern%20v1.pdf (Accessed 22 September 2019).

Fadilpašić, S. Want to blame someone for a data breach? Blame mobile workers. (2017). https://www.itproportal.com/news/want-to-blame-someone-for-a-data-breach-blame-mobile-workers (Accessed 22 September 2019).

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Frost and Sulivan. The smartphone productivity effect. (2016). https://www.samsung.com/us/business/short-form/the-smartphone-productivity-effect/?CampaignCode=082316-sho-na-nasmartphonegated content/? cid=artpromo-041916&cid=com-btb-sky-blg-122001 (Accessed 22 September 2019).

Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior*, 26, 331–362.

Gibbs, J. (1975). Crime, punishment, and deterrence. New York, NY: Elsevier.

Global Web Index. United Kingdom GWI market report (2017). 2017. https://cdn2.hubspot.net/hubfs/304927/Downloads/UK-Market-Report-2017.pdf (Accessed 22 Sepetmber 2019).

Gozman, D. & Willcocks, L., (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research*, 97, 235-256.

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., Jr., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). Advanced issues in partial least squares structural equation modeling. Thousand Oaks, CA: Sage.

Hamlin, J. E. (1988). The misplaced role of rational choice in neutralization theory. *Criminology*, 26(3), 425–438.

Hanna, T. BYOD Policies and GDPR: How do you comply? (2018). https://solutionsreview.com/mobile-device-management/byod-policies-and-gdpr-how-do-you-comply (Accessed 22 September 2019).

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2–16.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing*, 20(1), 277–319.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125.

Herrera, A. V., Ron, M., & Rabadão, C. (2017). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. Information Systems and Technologies (CISTI) Twelfth Iberian Conference (1-4). IEEE.

Hofstede. Compare countries. (2018). https://www.hofstede-insights.com/product/compare-countries (Accessed 22 September 2019).

Holland, T. From data privacy to mobile security: How Europe's GDPR is overhauling the web. (2018). https://mobilebusinessinsights.com/2018/04/from-data-privacy-to-mobile-security-how-europes-gdpr-will-overhaul-the-web (Accessed 22 September 2019)

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, 49(2), 99–110.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615–660.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, 81, 282–293.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95.

International Telecommunication Union. Global cybersecurity index (GCI) (2018). 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (Accessed 22 September 2019).

Ismail, N. Employee attitude is as important as technology when securing data. (2018). https://www.information-age.com/employee-attitude-important-technology-securing-data-123471157 (Accessed 22 September 2019).

Janmaimool, P. (2017). Application of protection motivation theory to investigate sustainable waste management behaviors. *Sustainability*, 9(7), 1079–1090.

Jaques, A. Securing the organisation against the fines of the GDPR. (2017). https://www.itproportal.com/features/securing-the-organisation-against-the-fines-of-the-gdpr (Accessed 22 September 2019).

Jarrahi, M. H., Nelson, S. B., & Thomson, L. (2017). Personal artifact ecologies in the context of mobile knowledge workers. *Computers in Human Behavior*, 75, 469–483.

Jay, J. Are UK firms violating GDPR by not implementing BYOD policies?. (2018). https://www.teiss.co.uk/information-security/byod-policies-uk-firms-gdpr (Accessed 22 September 2019).

Johnston, A. C., Di Gangi, P. M., Howard, J., & Worrell, J. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems*, 20(3), 186–212.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566.

Karacay, G., Bayraktar, S., Kabasakal, H., & Dastmalchian, A., (2019). Role of Leaders as Agents of Negotiation for Counterbalancing Cultural Dissonance in the Middle East and North Africa Region. *Journal of International Management*, 25(4), 1-12.

Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. *Information & Computer Security*, 24(5), 418–451.

Khaleej Times. 60% of UAE workforce skip office to work elsewhere. (2018). https://www.khaleejtimes.com/news/general/60-of-uae-workforce-skip-the-office-to-work-elsewhere (Accessed 22 September 2019).

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*. doi:10.1155/2014/463870

Kline, R. B. (2005). Principles and practice of structural equation modeling (2nd ed.). New York, NY: Guilford Press.

Knapp, K. J., Marshall T. E., Rainer R. K., & Ford F. N. (2005). Managerial dimensions in information security: A theoretical model of organizational effectiveness. Palm Harbor, FL and Auburn, AL: ISC2.

Kshetri, N., (2015). Success of crowd-based online technology in fundraising: An institutional perspective. *Journal of International Management*, 21(2), 100-116.

Lanier, M. M., & Henry, S. Neutralization theory: learning rationalizations as motives. Essential Criminology, 168–176. (2004). http://fliphtml5.com/crja/qbxl/basic (Accessed 22 September 2019).

Lazar, M. BYOD Statistics provide snapshot of future. (2017). https://www.insight.com/en_US/learn/content/2017/01182017-byod-statistics-provide-snapshot-of-future.html (Accessed 22 September 2019).

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behavior. *Behaviour & Information Technology*, 27(5), 445–454.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394–413.

Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and technological culturation. *IEEE transactions on engineering management*, 50(1), 45–63.

Malone, L. How Europe's data privacy regulations will affect U.S. businesses. (2018). https://www.business.com/articles/how-gdpr-will-affect-us-businesses (Accessed 22 September 2019).

McAfee. Mobile threat report: The next 10 years. (2018). https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf (Accessed 22 September 2019).

McCole, P., Ramsey, E. & Williams, J., (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63(9-10), 1018-1024.

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior*, 92, 37–46.

Miller, N. E., & Dollard, J. (1941). Social learning and imitation. New Haven, CT: Yale University Press.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285–311.

Montaño, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In K. Glanz, B. K. Rimer, K. "V." Viswanath (Eds.), Health behavior: Theory, research, and practice (95–124). San Francisco, CA: Jossey-Bass.

Munarriz, A. Is BYOD a GDPR risk?. (2018). https://www.thehrdirector.com/features/gdpr/byod-gdpr-risk (Accessed 22 September 2019).

Murray, C. (2014). Smartphone security risks: The extent of user security awareness (Doctoral dissertation, University of Dublin). https://scss.tcd.ie/publications/theses/diss/2014/TCD-SCSS-DISSERTATION-2014-062.pdf (Accessed 22 September 2019).

Ndubisi, N. (2006). Factors of online learning adoption: A comparative juxtaposition of the theory of planned behaviour and the technology acceptance model. *International Journal on E-learning*, 5(4), 571–591.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *Sage Open*, 5(2), 1–11.

Palmer, D. (2019). Cybersecurity: Under half of organisations are fully prepared to deal with cyberattacks. https://www.zdnet.com/article/cybersecurity-under-half-of-organisations-believe-theyre-fully-prepared-to-deal-with-cyber-attacks (Accessed 22 September 2019).

Paternoster R., & Bancman, R. (2001). Explaining criminals and crime. Los Angeles, California: Roxbury.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, 30(3), 549–584.

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.

Peace, A. G., Galletta, D. F., & Thong, J. Y. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, 20(1), 153–177.

Pitichat, T. (2013). Smartphones in the workplace: Changing organizational behavior, transforming the future. *LUX*, 3(1), 1–10.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903.

Prud'Homme, D., & von Zedtwitz, M., (2019). Managing "forced" technology transfer in emerging markets: The case of China. *Journal of International Management*, 25(3), 1-14

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(3), 757–778.

Putri, F., & Hovav, A. (2014). Employees' compliance with BYOD security policy: Insights from reactance. Proceedings of the Twenty-second European Conference on Information Systems, 1-17.

Response Source. 95% of UK businesses struggle with secure mobile working; one third have experienced data loss or breach (Apricorn study). (2018). https://pressreleases.responsesource.com/news/95695/of-uk-businesses-struggle- with-secure-mobile-working-one-third (Accessed 22 September 2019).

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816–826.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. E. Petty (Eds.), Social Psychophysiology (153–176). New York, NY: Guilford Press.

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., & Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities*, 1–11. doi:10.5171/2012.281869

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multi-group analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results. *Advances in International Marketing*, 22, 195–218.

Shaw, A. Protection motivation theory. (2012). http://www.strategic-planet.com/2012/12/protection-motivation-theory (Accessed 22 September 2019).

Sheridan, K. The Best and Worst Tasks for Security Automation. (2018). https://www.darkreading.com/operations/the-best-and-worst-tasks-for-security-automation/d/d-id/1332074 (Accessed 22 September 2019).

Shing, L. P., Shing, L. H., Tech, V., Chiang, M. C., Yang, C. W., & Lu, T. (2016). Smartphone security risks: Android. *International Journal of Electronics and Electrical Engineering*, 4(4), 346–350.

Silva, P. M., & Dias, G. A. (2007). Theories about technology acceptance: Why the users accept or reject the information technology? *Brazilian Journal of Information Science: Research Trends*, 1(2), 69–86.

Simpson, S. S. (2002). Corporate crime, law, and social control. Cambridge University Press.

Singh, D. (2010). Managing cross-cultural diversity: Issues and challenges in global organizations. IOSR *Journal of Mechanical and Civil Engineering*, 43–50. http://www.iosrjournals.org/ (Accessed 7 July 2020).

Siponen, M. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information systems*, 7(1), 19–35.

Siponen, M., Pahnila, S., & Mahmood, M. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64–71.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225.

Spokephone. Turn mobile phones into your business phone system. (2018). https://www.spokephone.com (Accessed 22 September 2019).

Strategy Analytics. Global mobile workforce forecast update 2016–2022. (2016). https://www.strategyanalytics.com/access-services/enterprise/mobile-workforce/market-data/report-detail/global-mobile-workforce-forecast-update-2016-2022#.WbFXfMiGPuE (Accessed 22 September 2019).

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664–670.

Thalese Security. UK the most breached country in Europe, but organisations aren't feeling the threat. News release. (2018). https://www.thalesesecurity.co.uk/about-us/newsroom/news-releases/uk-the-most-breached-country-in-europe-but-organisations-arent-feeling-the-threat (Accessed 22 September 2019).

Tomlinson, K. An examination of deterrence theory: Where do we stand?. (2016). http://www.uscourts.gov/sites/default/files/80_3_4_0.pdf (Accessed 22 September 2019).

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications*, 5, 147–158.

Tung, R. L., & Verbeke, A. (2010). Beyond Hofstede and GLOBE: Improving the quality of cross-cultural research. *Journal of International Business Studies*. 41, 1259–1274

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138–150.

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2018). Complying with BYOD security policies: A moderation model. Proceedings of MWAIS 2018 (paper 25). https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1024&context=mwais2018 (Accessed 22 September 2019).

Tu, Z., & Yuan, Y. (2015). Coping with BYOD security threat: From management perspective. Proceedings of the International Conference on Information Systems (ICIS) (pp.1-6). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.897.2564&rep=rep1&type=pdf (Accessed 22 September 2019).

Vaidya, R. 2018. Cyber security breaches survey (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf (Accessed 22 September 2019).

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 12(3), 29–39.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(4), 190–198.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, 77, 860–870.

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science*, 50, 511–516.

Wandera. Understanding the mobile threat landscape in 2018. (2018a). http://staxxsolutions.com/wp-content/uploads/2018/05/Understanding_the_mobile_threat_landscape.pdf (Accessed 22 September 2019).

Wandera. Why GDPR is a compliance nightmare for your BYOD fleet. (2018b). https://www.wandera.com/mobile-data-policy/gdpr-compliance/byod-is-bad-for-gdpr (Accessed 22 September 2019).

Wandera. An insight into third party app stores. (2018c). https://www.wandera.com/mobile-security/mobile-malware/third-party-app-stores (Accessed 22 September 2019).

Warkentin, M., Goel, S., & Menard, P. (2017). Shared benefits and information privacy: What determines smart meter technology adoption? *Journal of the Association for Information Systems*, 18(11), 758–786.

Weber, L., & Rudman, R. J. (2018). Addressing the incremental risks associated with adopting bring your own device. *Journal of Economic and Financial Sciences*, 11(1), 13–32.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816.

World Economic Forum. World Economic Forum Annual Meeting. 2018. https://www.weforum.org/events/world-economic-forum-annual-meeting-2018/sessions/a0Wb0000009yYXjEAM (Accessed 4 April 2019).

Wu, Y., Choi, B., Guo, X., & Chang, K. T. (2014). Understanding user adaptation toward a new IT system in organizations: A social network perspective. *Journal of the Association for Information Systems*, 18(11), 787–813.

Xiao, H., Peng, M., Yan, H., Gao, M., Li, J., Yu, B., Wu, H., & Li, S. (2016). An instrument based on protection motivation theory to predict Chinese adolescents' intention to engage in protective behaviors against schistosomiasis. *Global Health Research and Policy*, 1(1), 15–32.

Yang, X., Wang, X., Yue, W.T., Sia, C.L. & Luo, X., (2019). Security Policy Opt-in Decisions in Bring-Your-Own-Device (BYOD)–A Persuasion and Cognitive Elaboration Perspective. *Journal of Organizational Computing and Electronic Commerce*, 29(4), 274-293.

Zafirovski, M. (1999). What is really rational choice? Beyond the utilitarian concept of rationality. *Current Sociology*, 47(1), 47–113.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, 55, 81–99.