Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Information security policies compliance in a global setting: An employee's perspective

Mansour Naser Alraja[a,*], Usman Javed Butt[b], Maysam Abbod[b]

[a] Newcastle Business School, Northumbria University, Newcastle, UK
[b] Brunel University, Electronic and Electrical Engineering, London, UK

ARTICLE INFO

Article history:
Received 6 August 2022
Revised 26 November 2022
Accepted 25 March 2023
Available online 29 March 2023

Keywords:
Information security policies compliance
UMISPC
Neutralization
Fear
Habit and role values
And reactance

ABSTRACT

Information security threats have a severe negative impact on enterprises. Organizations rely on employee compliance with information security policies to eliminate or reduce these hazards. The Unified Model of Information Security Policies Compliance (UMISPC) is employed to identify the factors that may affect employees' intention towards compliance with information systems security policy and reactance in a global setting. The study was assessed in two phases. The model's validity and measurement reliability were evaluated in the first phase, while in the second phase, all preliminary model relationships were appraised. This was achieved utilizing structural equation modelling to establish whether the proposed constructs, i.e. neutralization, response efficacy, fear, threat, habit and role values were good predictors for intention or reactance towards compliance with information systems security policy. Participants included 348 employees from 7 nations, i.e. the USA, the UK, Oman, India, Pakistan, Malaysia, and the Philippines. SmartPLS v. 3.3.9 was used for data analysis. The models' measurement reliability and validity were affirmed. Fear and role values have a significant influence on intention toward ISPC. RE significantly predicted threat which in turn significantly predicted fear, and the latter demonstrated a significant effect on reactance as well as Neutralization predicted reactance. In contrast, habit failed to reach a significant influence on intention towards ISPC. The implications are presented, together with proposals for further studies. Our findings are helpful for ISS literature and application by supporting the crucial functions of role values in encouraging employees to behave in a compliant manner. Additionally, it is regarded as the first empirical attempt to estimate intended compliance concerning ISPs in higher education from a worldwide viewpoint.

1. Introduction

In the modern world, information is a valuable commodity. Thus, professional bodies need to prioritize policies relating to information systems security (ISS) (Bansal et al., 2020; Karlsson et al., 2022; Liu et al., 2020; Silic and Lowry, 2020). According to Koohang et al. (2020), 59% of businesses in the US and UK reported security issues in 2019. Data breaches surged by 160% between 2006 and 2019, affecting 25,575 records in that year alone. At the same time, 230,000 new malware samples are created every day, and more than 4000 ransomware assaults take place each day. Ninety-one per cent of these infiltrate businesses using spear phishing emails, with 2019 damage costs exceeding $11.5 billion globally. Information security threats have a severe negative impact on enterprises. Organizations rely on employee compliance with information security policies to eliminate or reduce these hazards (Koohang et al., 2020). Employee noncompliance with an organization's information security policy (ISP) puts organisational resources at risk and creates information system vulnerability (Koohang et al., 2020). Information security breaches that employees cause have become common occurrences in many organizational contexts and are expected to increase soon (Vance et al., 2020; Verison, 2020). There is a universally high incidence of employee-generated ISS transgressions, including in higher education establishments (Khatib and Barki, 2020). Published data shows an ongoing increase in risk to information security, especially from within institutions. Most leaks occur due to a lack of user compliance with ISS guidelines. Thus, it has become essential to initiate, instigate and upgrade efficacious information security management systems (Bansal et al., 2020; Guan and Hsu, 2020; Gwebu et al., 2020; Kang et al., 2022; Li et al., 2019; Szczepaniuk et al., 2020). Establishments currently view the protection of information from security

[*] Corresponding author.
E-mail address: mansour.alraja@northumbria.ac.uk (M.N. Alraja).

https://doi.org/10.1016/j.cose.2023.103208

hazards as paramount (Bhaharin et al., 2019; Gwebu et al., 2020; Koohang et al., 2019; Mirtsch et al., 2021). An ISS policy (ISP) is an official paper that documents a dedicated process to achieve an institution's goals to guarantee the safety of valuable information and technical data (Angraini et al., 2019). ISP compliance (ISPC) is the degree to which company staff observe the regulations within their roles (Hou et al., 2018; Jaeger et al., 2020; Vance et al., 2013). Many employees continue to engage in noncompliant behaviours such as sharing passwords, copying sensitive data on the universal serial bus (USB) drives or leaving their computers unlocked (Moody et al., 2018; Siponen and Vance, 2010a). One study has reported recent increases in higher education institutional data transgression and stealing of intellectual assets in the United States (US); at the affected centres, there was a notable lack of implemented ISPs (Weidman and Grossklags, 2019). An analysis of 32,002 security alerts in 81 institutions affirmed 3950 genuine. Personnel within the organization were responsible in approximately a third of cases; in 8%, authorized staff misused the system (Verison, 2020). In the educational sector, 228/819 data hacks were initiated in-house, and 30% of the data exposed comprised credentials (Verison, 2020). Furthermore, according to the UK National Cyber Security Centre Government, Education and Healthcare were the top three affected industries globally from January to November 2021, which showed a 25% increase from the same period in 2020 (NCSC, 2021). Ransomware insurance claims in the US increased by 150% from 2018 to 2021 (Zandt, 2021). The COVID-19 pandemic in 2020 meant criminals could take advantage of an increase in homeworking and IT services moving the cloud in the UK. The percentage of homeworkers in the US also increased from 6% to 35% in 2020, and attacks on homeworkers increased from 12% to 60% in the first six weeks of the lockdown (NCSC, 2021). The impact of COVID-19 on hospitals, governments and education also made them more likely to pay ransoms to avoid further disruption to their systems (Aubley et al., 2021). In addition to that pressure, NIST cites people as the main facilitators of ransomware attacks. End-users engaging in risky behaviour, administrators configuring insecure systems, and developers uneducated in secure development practices (Europol, 2021). CISA has identified spearphishing as a commonly used technique for gaining initial access to an information technology (IT) network. The attacker can pivot to an operational technology (OT) network (NIST, 2022). However, ISS research has demonstrated that organizational personnel rarely comply with security policy procedures, preferring to take risks despite being cognizant of company guidelines. Such undesirable behaviour has been investigated in past research, which recommended many actions to be applied to deter them (D'Arcy et al., 2009; D'Arcy and Herath, 2011; Koohang et al., 2020). Still, many employees continue to engage in noncompliant behaviours to accomplish their tasks more efficiently (Khatib and Barki, 2020). For example, copying confidential data on an insecure USB can enable an employee to work extra hours from home (which will likely benefit both the employee and the organization). Similarly, leaving one's computer turned on can help reduce the time lost while waiting for it to restart after shutting it down. Sharing passwords with colleagues can enable an employee to complete an urgent task. Understanding the factors that affect employees' reactance or/and intention to comply with ISPs can be a helpful objective and help information security managers improve information security management in their organization. Thus, an essential field of ISS work is exploring and elucidating the rationale underlying employee non-conformity with ISPs (Angraini et al., 2019; Bulgurcu et al., 2010; Chen and Liang, 2019; Chen and Zahedi, 2016; D'Arcy et al., 2009; Herath and Rao, 2009; Johnston and Warkentin, 2010; Khokhar et al., 2021; Moody et al., 2018; West, 2008).

Numerous studies were undertaken in the context of ISP, e.g. to elicit a set of needs for computerized tools that help ISP design (Rostami et al., 2020). The focus should move toward organization-specific information security requirements for cutting-edge ISP development (Paananen et al., 2020), influencing whether employees perceive deterrents and want to abide by information security policies (Xu et al., 2021). Determine the internal motivation and outside pressure that drive employees to abide by information security regulations (Jaeger et al., 2020). The degree to which the employee is self-interested in adhering to the organization's ISPs (Wang et al., 2022). Moreover, how diverse motivating variables influence certain ISP compliance behaviours (Chen et al., 2022).

Furthermore, compliance with ISPs has been recognized as a standard and essential problem in organizations. However, with some exceptions (Hovav and D'Arcy, 2012; Karjalainen et al., 2013; Vance et al., 2020), previous research on ISP violations has been conducted using subjects from a single country only (Aggarwal and Dhurkari, 2023). Consequently, our knowledge of how these local findings can be generalized across countries is limited. This information is essential because IS security behaviour is a worldwide, rather than a local, problem (Chen and Zahedi, 2016). The fact that ISP violations are a global problem and that previous research has found or suggested cultural differences amongst these theories stress the need to examine whether the models of ISP violations are generally consistent across cultures (Vance et al., 2020). UMISCP is perhaps at the top of the list for three reasons when selecting candidate theories for this cross-cultural investigation. First, it is developed based on the most used theories in IS research. Second, to study the intention to comply with ISPs, it investigated the reactance to explore the active adverse reaction to an employee's external behavioural influencer. Third, it considered the work environment and relevance of the ISP guidelines to the profession through the newly added variable role values (Moody et al., 2018). The UMISPC is not validated in a similar or alternative scenario before. The reliability, validity and strength of the modified parameters were evaluated by Koohang et al. (2020). Although testing of 187 personnel from a moderately sized US university proved these model features to be robust, only five constructs, i.e. role values, response efficacy, threat, neutralization and reactance, were significant indicators of intention towards ISPC. In contrast, the constructs of habit and fear failed to reach significance (Koohang et al., 2020). Role values reached significance only when four constructs were extracted from the assessment due to low indicator loading. Furthermore, in contrast to the initial results of the model, fear was observed to have a negative effect on reactance.

Moody et al. (2018) recommended further testing for the tentative UMISPC on three categories of ISP infringements to determine the degree to which UMISPC can give or provide assistance in varying contexts. It also identifies to what extent the UMISPC required modification according to the ISP breach classification and applies to infringements additional to those tested. Specifically, assessing the UMISPC in various situations to identify its perimeters and contexts in which its application may be unsuccessful and determine the relevance of each construct in a range of scenarios. In the current study, the eight constructs (refined UMISPC) model assessed 348 employees of diverse nationalities, i.e., US, United Kingdom (UK), Oman, India, Pakistan, Malaysia and the Philippines. The aim is to investigate whether the UMISPC is robust and can be generalized and identify the factors that may affect employees' intention toward compliance with information systems security policy and reactance in a global setting. The study has two phases: assessing measurement reliability and validity. The second stage evaluates UMISPC model relationships using PLS structural equation modelling (SEM). To investigate whether the postulated constructs, i.e. neutralization, response efficacy, fear, threat, habit, and role values, are reliable prognostic indicators for intention towards ISPC and reactance.

Additionally, the possibility that neutralization and fear may influence reactance. Both will be analysed to explore the degree to which fear is anticipated through the observed threat, how the threat is indicated by response effectiveness, and whether the same (or different) factors affect employees' intention to comply with ISPs and reactance. Our results have the potential to contribute to IS research and practice by confirming the critical roles of role values in motivating employees' compliance behaviour. First empirical attempts at estimating intended compliance concerning ISPs in higher education by evaluating the UMISCP, and showing the extent to which UMISCP is empirically supported across national borders.

The paper is organized as follows: firstly, an introduction to the study is presented, then the ISP in global settings is discussed, followed by a literature review to define each construct. Then proceed with the research methodology, followed by the analysis of results, discussion of findings, and conclusions.

2. Theoretical research framework and research hypotheses

Behavioural research into ISS has offered diverse rival models based on various hypotheses. Venkatesh et al. (2003) are one of several research groups who have proposed that many hypotheses should be condensed into a single paradigm (Venkatesh et al., 2003). Moody et al. (2018) concurred and examined eleven models (see below) that can describe workers' variation in attitude and action towards ISP conformity, aiming to delineate unifying and complementary features of each paradigm. An initial study evaluated these models' fundamental and intellectual parallels and presented a single amalgamated hypothesis, termed the unified model of information security policy compliance (UMISPC). The model is composed of nine independent variables and two dependant variables. The preliminary model was evaluated with varying data methodologies. Only six independent variables, i.e. habit, role values, response efficacy, threat, fear, and neutralization, influenced the reactance construct and/or intention to comply with ISPs. The remaining three, i.e. punishment, cost/rewards and facilitating conditions, demonstrated no significant effect. This paper is based on previous studies of UMISPC (Moody et al., 2018), which is established on eleven pre-existing theories (see Fig. 1) that have to date, underpinned earlier ISS behaviour models.

Therefore, UMISPC (see Fig. 2) was thus employed in the present work as an underpinning theory to address the persistent research gaps and to assess the empirical validity of this model in predicting IS compliance behaviours (1) Reactance and (2) Compliance intention on a global scale.

2.1. Reactance

Institutions may attain negative consequences from draconian controlling ISPs, particularly since rewards and penalties are often incorporated in formalised guidelines (Lowry and Moody, 2015). The usual result in fear appeal research is message approval, distrustful evasion or reactance (Witte, 1992). Witte and Allen (2000) demonstrated that defensive reactions are positively correlated to the size of fear appeals and inversely related to hazard-control responses and efficient communications (Witte and Allen, 2000). The threat was positively related to psychological reactance (Quick et al., 2018). Suppose an anticipated threat is greater than the perceived efficacy. In that case, the individuals try to regulate the emotion of fear through maladaptive behavioural reactions, e.g. threat denial, communication trivialisation, source denouncement and reactance (Witte, 1992).

In contrast to evasion, reactance is an active adverse reaction to a worker's external behavioural influencer. Whilst deliberately discarding the fear-inciting information, the person is driven to distrust and contest the cause of their issue rather than hiding their conflict (Moody et al., 2018), (Lee and Lee, 2009; Lowry and Moody, 2015). Individuals frequently refuse to alter their demeanour and may act perversely (S.-Y. Kim et al., 2017). Hence, the importance of ISPs (Karlsson et al., 2022) has emphasised the end user's involvement in security compliance (McLeod and Dolezel, 2022).

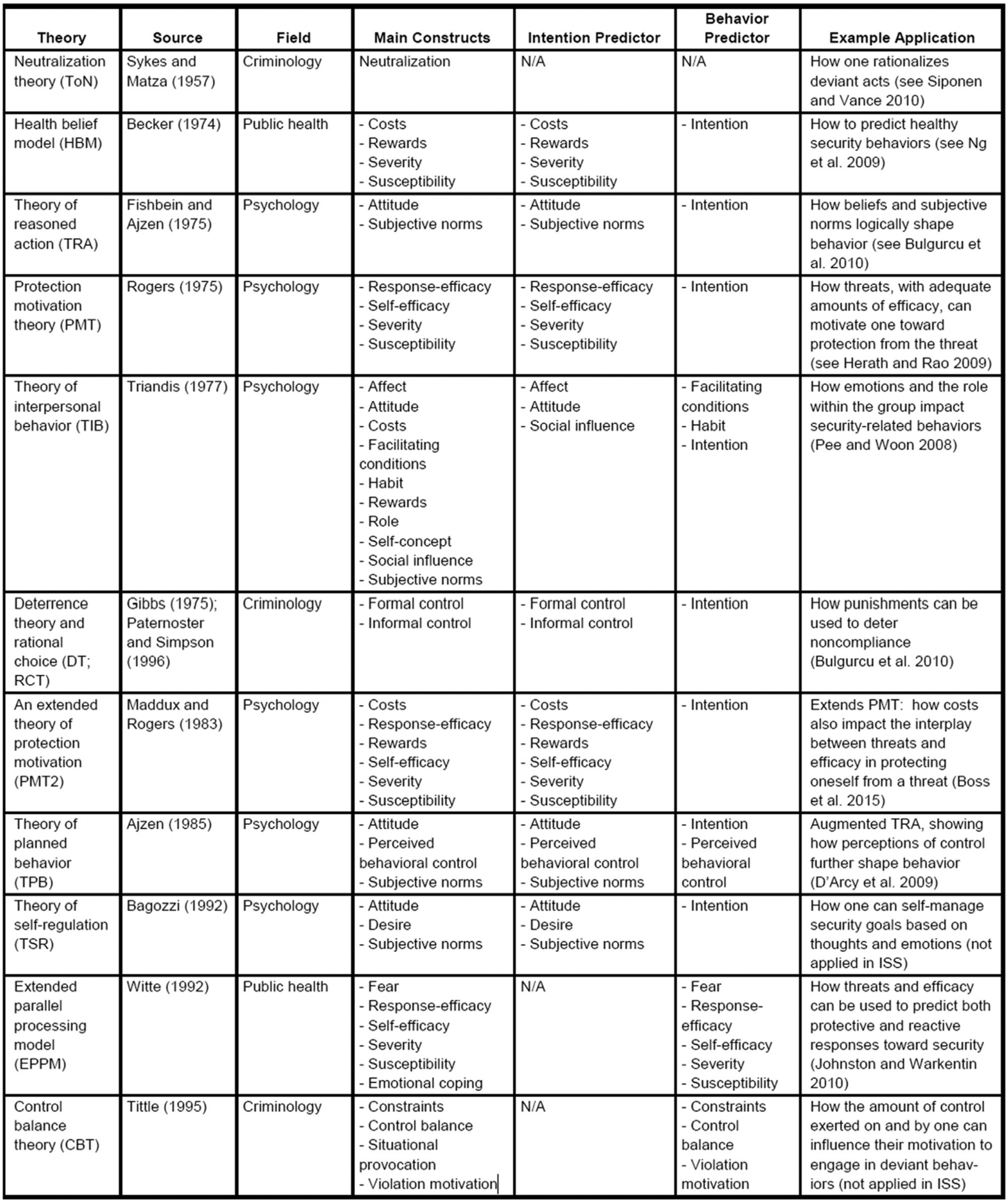
2.2. Compliance intention

Instigation of an ISP may fail if safeguarding requisites are not followed. Individual factors, i.e. direct or indirect, can influence intention towards ISPC and their general attitude concerning ISS (Angraini et al., 2019; Verkijika, 2018; Yoon et al., 2020). Successful ISPC intention is the result of the establishment's industry towards ISS, i.e. it reflects a worker's intention to safeguard institutional assets from possible security infringements (Hu et al., 2011; Hwang et al., 2017) and their inclination towards ISPC and fulfilling their personal responsibilities in this area (Koohang et al., 2020). Most publications in this sector concentrate on intention as a leading indicator for ISPC. The range of evaluated constructs which impact ISPC and ongoing behavioural intention towards upholding policy guidelines include; fear (Boss et al., 2015; Crossler et al., 2013), threat (Putri and Hovav, 2014; Siponen et al., 2014), response efficacy, and habit (Johnston et al., 2015b; Sommestad et al., 2014; Tsohou et al., 2015), neutralization (Bansal et al., 2020), reactance (Youn and Kim, 2019) and role values (Koohang et al., 2020). These are all incorporated into the UMISPC (Moody et al., 2018). A description of each construct within the scenario of ISS behaviour is given below.

2.3. Habit

Habits are reflex, automatic behaviours which often lack cognitive input and are triggered as a routine. Iterative response to a particular scenario or contextual factors (Keikhosrokiani, 2020; Mouakket and Sun, 2019; Triandis, 1980) they can be a mechanism through which specific objectives may be achieved (Limayem et al., 2007; Verplanken et al., 1997). This situational behaviour sequence is relevant to the utilization of ISS (Limayem and Hirt, 2003). In the information systems sector, habit is referred to as the "extent to which people tend to perform behaviours (use ISS) automatically because of learning" (Limayem et al., 2007), p. 709]. The intuitive nature of habit is induced through reiterative behaviour. Habits have been studied in alternative scenarios to business, e.g. in psychology (Verplanken et al., 1998), health (Gardner, 2015) and travel (Bamberg and Schmidt, 2003). Since behaviours relating to ISS are continuous, habit is an anticipated precursor. Maddux (1993) has highlighted that situational indicators and habits influence decisions made concerning safeguarding behaviours (Maddux, 1993). An IT habit is the degree to which prior education influences individuals to automatically select a specific IT (Zhang et al., 2015).

Previous studies have demonstrated that habit plays an essential role in an individual's perception of information systems (Wu et al., 2016), diminishing the focus on trust-risk thought processes when deciding on IS-related behavioural options (Vance et al., 2012). It also influences the information required by shoppers. Electronic device ownership and social capital can also generate habitual behaviour (Bhatnagar and Papatla, 2019). PMT is affected by ISPC habits, although ongoing usage is only anticipated for vital habitual behaviours (Lankton et al., 2010). The prin-



Theory	Source	Field	Main Constructs	Intention Predictor	Behavior Predictor	Example Application
Neutralization theory (ToN)	Sykes and Matza (1957)	Criminology	Neutralization	N/A	N/A	How one rationalizes deviant acts (see Siponen and Vance 2010)
Health belief model (HBM)	Becker (1974)	Public health	- Costs - Rewards - Severity - Susceptibility	- Costs - Rewards - Severity - Susceptibility	- Intention	How to predict healthy security behaviors (see Ng et al. 2009)
Theory of reasoned action (TRA)	Fishbein and Ajzen (1975)	Psychology	- Attitude - Subjective norms	- Attitude - Subjective norms	- Intention	How beliefs and subjective norms logically shape behavior (see Bulgurcu et al. 2010)
Protection motivation theory (PMT)	Rogers (1975)	Psychology	- Response-efficacy - Self-efficacy - Severity - Susceptibility	- Response-efficacy - Self-efficacy - Severity - Susceptibility	- Intention	How threats, with adequate amounts of efficacy, can motivate one toward protection from the threat (see Herath and Rao 2009)
Theory of interpersonal behavior (TIB)	Triandis (1977)	Psychology	- Affect - Attitude - Costs - Facilitating conditions - Habit - Rewards - Role - Self-concept - Social influence - Subjective norms	- Affect - Attitude - Social influence	- Facilitating conditions - Habit - Intention	How emotions and the role within the group impact security-related behaviors (Pee and Woon 2008)
Deterrence theory and rational choice (DT; RCT)	Gibbs (1975); Paternoster and Simpson (1996)	Criminology	- Formal control - Informal control	- Formal control - Informal control	- Intention	How punishments can be used to deter noncompliance (Bulgurcu et al. 2010)
An extended theory of protection motivation (PMT2)	Maddux and Rogers (1983)	Psychology	- Costs - Response-efficacy - Rewards - Self-efficacy - Severity - Susceptibility	- Costs - Response-efficacy - Rewards - Self-efficacy - Severity - Susceptibility	- Intention	Extends PMT: how costs also impact the interplay between threats and efficacy in protecting oneself from a threat (Boss et al. 2015)
Theory of planned behavior (TPB)	Ajzen (1985)	Psychology	- Attitude - Perceived behavioral control - Subjective norms	- Attitude - Perceived behavioral control - Subjective norms	- Intention - Perceived behavioral control	Augmented TRA, showing how perceptions of control further shape behavior (D'Arcy et al. 2009)
Theory of self-regulation (TSR)	Bagozzi (1992)	Psychology	- Attitude - Desire - Subjective norms	- Attitude - Desire - Subjective norms	- Intention	How one can self-manage security goals based on thoughts and emotions (not applied in ISS)
Extended parallel processing model (EPPM)	Witte (1992)	Public health	- Fear - Response-efficacy - Self-efficacy - Severity - Susceptibility - Emotional coping	N/A	- Fear - Response-efficacy - Self-efficacy - Severity - Susceptibility	How threats and efficacy can be used to predict both protective and reactive responses toward security (Johnston and Warkentin 2010)
Control balance theory (CBT)	Tittle (1995)	Criminology	- Constraints - Control balance - Situational provocation - Violation motivation	N/A	- Constraints - Control balance - Violation motivation	How the amount of control exerted on and by one can influence their motivation to engage in deviant behaviors (not applied in ISS)

Fig. 1. the reviewed theories while developing UMISCP. Source (Moody et al., 2018, pp. 288).

cipal characteristics of a habit are the semi-automated response behaviour, assistance in preserving mental effectiveness and employees conforming with security policy guidelines daily such that these measures become entrenched. Thus, if university academic staff perform unhabitual behaviour, they may not fully consider the consequences and ignore the potential impact of failing ISPC. The following hypotheses are postulated:

H1: Habits positively affect employees' intention to comply with ISPs.

2.4. Role values

The addition of role values is founded on the interpersonal behaviour theory, control balanced theory, the extended parallel

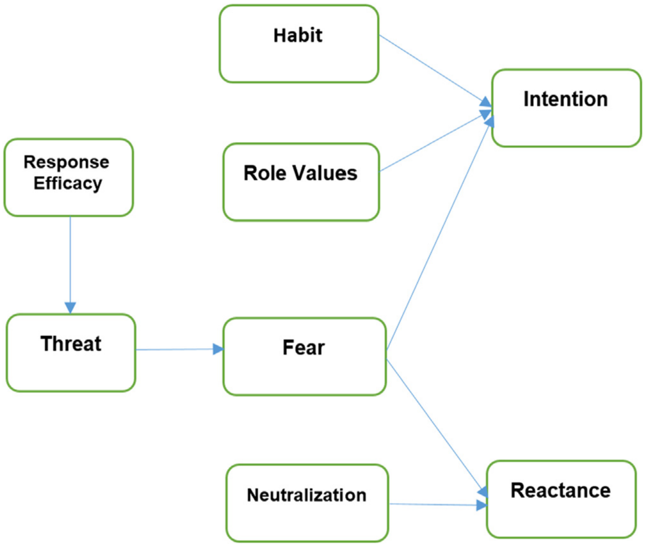


Fig. 2. the UMISPC developed by Moody et al. (2018).

processing model and UMISCP. In particular, the initial TIB postulates that subjective norms, roles and self-concept give rise to social factors. However, Moody et al. (2018) noted that the latter failed to persist in their developed model. Thus, based on their data, they postulated the concept of role values, i.e. ISPC is a relevant, vindicated and reasonable act (ethical descriptions and self-concept), considering the profession and individual's job (role) (Koohang et al., 2020). They noted that this construct offered the most significant validation for ISPC.

Furthermore, adding it to the model diminished the part played by punishment severity. Hence, this variable was incorporated into UMISCP. Since ISPC exists concerning the work environment, the higher the relevance of the ISP guidelines to the profession, the greater their approval and credence, considering ISS climate and philosophy (Moody et al., 2018). However, when Koohang et al. (2020) revisited UMISCP, indicator reliability failed to be attained since the outer loadings of four indicators for the role values latent variable were less than 0.7, leading to their eradication. Data review showed that role values significantly impacted intention towards ISPC (Koohang et al., 2020). University department members will perceive that enacting ISPC is relevant, justified and reasonable if it is associated with their scholarly activities. Thus, they will engage in safeguarding and ISPC. Thus, the following two hypotheses are postulated:

H2: Role values will have a significant positive influence on employees' intention towards ISPC.

2.5. Response efficacy

Response efficacy (RE) expresses how an individual comprehends the ability of a specific response to deal with a specific threat, e.g. ISPC (Menard et al., 2017), and the certainty that behaviour will mitigate the likelihood of an adverse incident (Hanus and Wu, 2016). Perceived effectiveness is the evaluation of strategies necessary for ISPs, i.e. their efficacy in deflecting ISS threats (Liang and Xue, 2009). A threat triggers cognitive pathways; the objective is to sway the individual towards threat-diminishing actions. RE influences the thought processes relating to presumed behavioural benefits (Rogers et al., 1983; Verkijika, 2018) and their impact on self-preservation and peers' safety (Hassandoust and Techatassanasoontorn, 2019). In the ISS sector, RE reflects that ISPC is an efficacious strategy for identifying a threat to an established ISS portfolio (Ifinedo, 2012). It is also determined by an individual's outcome expectations, i.e. how much an individual perceives a threat can be diverted following a specific behaviour (Hanus and Wu, 2016). RE has been demonstrated to be a significant determinant and robust indicator of safeguarding actions (Crossler, 2010; Hanus and Wu, 2016; Woon et al., 2005). It was crucial in clarifying the variation in password manager installation objectives (Menard et al., 2017) and a negative influence on intention towards ISPC (Vance et al., 2012). If the anticipated outcome from ISPC is highly beneficial to workers, then ISPC is improved, i.e. RE is a coping appraisal mechanism (Ifinedo, 2012). Confidence that appropriate security behaviours will benefit the institution's ISS strategy has been shown to enhance positive security choices (Herath and Rao, 2009). This principle also predicts secure online intentions (Doane et al., 2016) and internet use (Tsai et al., 2016). However, RE failed to impact personal online (Thompson et al., 2017) or smartphone security intentions (Verkijika, 2018) and does not influence compliance behaviour (Liu et al., 2020). In the present work, employees who appreciated the response from the guidelines noted the specific threat to security which enabled them to evade or reduce it. The following hypotheses have therefore been proposed:

H3: RE positively affects employees' perceived threat.

2.6. Threat

The threat is a phenomenon that poses the risk of physical or mental injury (Junglas et al., 2008). Published data has demonstrated that cyber threats in public and private domains incorporate the utilization of advanced and malicious software, and perturbing actions from online activists, nationalist factions, organized criminals and espionage undertakings (Nam, 2019). An apparent threat positively affects security-tightening behaviours (Menard et al., 2017). In the public sector, threat recognition to ISS can reduce the incidence of its realization since appropriate precautions can be installed (Szczepaniuk et al., 2020). The goal of instituting password management software is unaffected by the two components of threat, i.e. severity and susceptibility (Menard et al., 2017); desktop security behaviour is also independent of threat appraisal (Hanus and Wu, 2016). Concerning bring-your-own-device (BYOD) systems, a security threat fails to influence the institution of a disturbance-handling strategy. However, it has a negative effect on the self-preservation strategy (Baillette and Barlette, 2020). A potential threat has no impact on ISPC (Liu et al., 2020); this was noted amongst university workers (Rajab and Eydgahi, 2019). The threat was a significant precursor to fear; those that opt to exhibit ISPC did so through fear associated with an apparent threat (Burns et al., 2017; Moody et al., 2018). employees, those who wished to violate compliance objectives would be aware of the danger of personal harm as a consequence of ISPC infringement. Transgressors often failed to correctly assess the consequences of their actions or were confident they could ride them. The following hypotheses are proposed:

H4: Perceived threat will positively influence an employee's identified fear.

2.7. Fear

Fear is described as a "relational construct, aroused in response to a situation that is judged as dangerous and toward which protective action is taken" (Rogers, 1975) p.96]. May (2004) observed that conformity is principally described by fears associated with the negative impact of being apprehended for protocol breach (May 2004). Conversely, Karjalainen et al. (2019) indicated that ISPC resulted from an individual appraisal of policy relevance (Karjalainen et al., 2019). Publications relating to the ISS sector have evaluated fear from the hypothetical angle of safeguarding rationale, highlighting the impact of fear as a retort to threats (Herath and Rao, 2009; Johnston et al., 2015a; Lee and Larsen, 2009; Siponen et al., 2014). Jansen and Shaik (2019) reinforced earlier work that postulated that threat is a precursor of fear and that fear per se does not affect users' protective online information-divulging actions. However, threat promotion can uplift intentions (Jansen and Schaik, 2019), (Lazarus, 1991). A modified PMT model delineated fear as a partial core mediator, e.g. between threat and intention towards ISPC (Floyd et al., 2000; Rogers and Prentice-Dunn, 1997). Thus, if university workers view noncompliance as hazardous, they will protect themselves and demonstrate conformity. Furthermore, since threat and fear are not identical, assessment of the former without the latter is an issue (Boss et al., 2015). Two hypotheses are therefore postulated:

H5: Employees' perceived fear will positively affect their intention towards ISPC.

If employees appreciate compliance as an indicator of fear, they may discard this behavioural option. Concerning ISPC, strict control of workers' safeguarding requirements may induce reactance and thus diminish conformity (Wall et al., 2013). Reactance also negatively correlates with intent towards ISPC (Lowry and Moody, 2015). Thus, there are two pathways seated within UMISPC in addition to reactance. In addition, the extended parallel process model reinforces the proposed route of response efficacy, which precedes threat, an antecedent to fear, which then leads to reactance. Witte (1996) noted that if an individual's efficiency assessment leads them to believe that they do not have the skill to evade the threat, then they will diminish fear by indulging in fear control responses, i.e. "coping responses that diminish fear, such as defensive avoidance, denial, and reactance" (Witte, 1996). One further hypothesis is proposed:

H6: Fear has a negative effect on employees' reactance.

2.8. Neutralization

Skyes and Matza (1957) proposed that 'neutralization' encompasses a means through which individuals can invalidate and contravene normal behaviours by making excuses for their actions (Siponen and Vance, 2010a) and utilizing reasons or specific mental processes to persuade themselves and their peers that irregular behaviour is acceptable and defensible (Cheng et al., 2014), (D'Arcy and Teh, 2019). Neutralization techniques are standard and effective within institutions; their exact nature varies according to the situation or policy (Silic et al., 2017). Concerning ISS, workers may defend their assumed right to breach ISP through their positive employee status or to perform salvage (Bansal et al., 2020). Neutralization also enables the individual to claim a "temporary period of irresponsibility or an episodic relief from moral constraint" (Bansal et al., 2020; Maruna and Copes, 2005). Thus inhibiting moral discernment and sanctioning immoral actions (Kim et al., 2020). Persuading the individual that his course causes no harm and assuaging guilt and feelings of responsibility (Sykes and Matza, 1957). Issues relating to ISS include password sharing, USB use and failing to lock computers; neutralization is a significant factor in excusing such infringements (Moody et al., 2018) and a positive influence on the intention to breach ISPs (Vance et al., 2020).

In contrast, neutralization has a negative correlation with compliance; extreme tiredness is an associated risk status during which there is an increased probability that the employees will rationalize the acceptability of a breach (D'Arcy and Teh, 2019). In the present study, infringements of ISPC were explained by an imprecise policy, failure to believe perpetrators were doing harm and the apparent need to perform a beneficial task for the university. These assumptions are therefore made:

H7: Neutralization will positively influence employees' reactance (denying the possible ISS problem).

3. Methodology

An experiment-scenario method was used in the present work to investigate ISP violations. Participants were presented with a hypothetical situation. They were asked to rate their likelihood of behaving in such a way under similar circumstances. It is the most commonly used method in ISP compliance studies, which is why it was selected in the present research (Siponen and Vance, 2014). Consequently, our research is comparable with many other studies that have explored the same topic. This method is less confrontational to understand and assess ISP intentions than directly asking employees to indicate their policy violation (D'Arcy et al., 2009; Siponen and Vance, 2010b; Vance et al., 2020).

Moreover, the generalizability of results found using experiment scenarios is often higher because various situations can be included (Siponen and Vance, 2014). Siponen and Vance (2014) also point out that experiment scenarios are beneficial for assessing prospective future behaviours whilst avoiding using generic measures, which have many drawbacks. For example, they cannot measure specific types of behaviour (e.g., IS policy violation). Moreover, different responses can be presented in different situations, and generic measures cannot assess this (Siponen and Vance 2014). Experiment scenarios are commonly applied in ISS research (Koohang et al., 2020, 2020; Moody et al., 2018; Siponen and Vance, 2014). It is important to note that the realism of the scenarios largely influences the practical applicability of the approach (Siponen and Vance, 2014). Three different scenarios (taken from recommendations by Moody et al. (2018)) were thus included in Siponen and Vance's (2010) work. The latter researchers developed their scenarios based on information obtained through interviews with 54 information security managers. The managers highlighted these three behaviours as most likely impacting compliance with ISS policies in their companies. The present work aims to assess Moody et al.'s proposed UMISPC (2018) global applicability.

For this reason, this study adopted the same measures used in Moody et al. (2018) research. We used the same scenarios and validated items incorporated in these studies. Except for replacing the name used in Moody et al.'s questionnaire with the letter X, no other modifications were made to the items.

Most studies investigating ISP compliance have involved participants who use IT in their work-related tasks. Thus, in most cases, participants have extensive educational backgrounds (with most possessing at least a Bachelor's degree (Kam et al., 2015)). Two hundred seventy-four participants held master's degrees and high levels of experience (Moody et al., 2018). Other participants are university employees, 70% of whom possess master's (40%) or doctoral (30%) degrees (Rajab and Eydgahi, 2019). Approximately 70% of those occupying managerial positions have Bachelor's or postgraduate degrees (Yazdanmehr et al., 2020). It was found that most alums of the MIS and MBA programs in one of the USA's more prominent public universities were employed in managerial roles (Hu et al., 2012).

Additionally, 237 participants from US universities were involved in the study, and 52% were faculty members (Koohang et al., 2020). In a different study exploring the validity, reliability, and robustness of a unified ISS compliance model, the sample consisted of 187 faculty and staff members from a mid-sized US university. This study involved eight constructs impacting information security policy compliance (Koohang et al., 2020). Moreover, other studies have used participants from the educational industry (da Veiga et al., 2020; Hovav and D'Arcy, 2012; Koohang et al., 2020, 2020; Rajab and Eydgahi, 2019). We only included participants with solid academic backgrounds because such individuals tend to be more proficient in using technological devices (at least two desktop devices are used in each faculty). For example, faculty members are usually required to access their work accounts on a laptop and cell phone. They may also have to use flash drives to move presentations between devices, and a personal password may be required to access the desktop computer in the classroom.

Moreover, faculty members are usually required to enter a username and password to access their university emails, office and classroom computers. Most participants used a browser-based password management system, meaning they could use saved passwords to log in to the system after initially logging in to it via their university account. This password enables them to access various materials, including emails and university information systems. Additionally, if they were to lose their flash drive or forget their login details (or if their login details were compromised), this leaves them at significant risk of a third party interfering with their emails and information. For this reason, we believe that using participants with academic backgrounds (as recommended by Moody et al. (2018)) is most suitable in the present work context. To choose the sample, a random sampling approach was used. i.e. based on a randomly prepared list of Universities from many different countries. The electronic link of our questionnaire was submitted to all Universities that have an available email or any other electronic communication method like WhatsApp. Full-time University employees working in the UK, USA, India, Pakistan, Oman, Malaysia, and the Philippines were thus engaged as participants in the study, and data were obtained through questionnaires.

Moreover, employees are typically targeted as study participants in the ISCPs. Additionally, it has been noted that most of the conducted studies were done in North America (Aggarwal and Dhurkari, 2023). For instance, 134 responders from the USA were mainly spread out over the Southeast (27%), Midwest (23%), and Northeast (24%) geographical regions of the country (McLeod and Dolezel, 2022). Two hundred sixty-nine participants were targeted (Liu et al., 2020) to assess employees' ISP compliance in the Chinese environment and 334 cases from Chinese hotel employees (Xu et al., 2021). In contrast, 615 people from 48 different nations working for a big international corporation took part in the study to examine the connection between sanctions and the desire to break ISPs (Vance et al., 2020). English was the primary language used by all participants in the study, and thus the questionnaire was presented in English. Nonetheless, English was not the primary language of some countries included in the study (such as Malaysia and Oman). We thus ensured that we only recruited participants from universities that taught their classes in English.

In order to prevent any possible common method bias (CMB), the guidance of Ping (2004) was followed to judge the first draft of the instrument in terms of validity, reliability and consistency (Ping, 2004); five faculty members from different scientific disciplines consulted and requested to read the adopted scenario and its structure and content. Consequently, a minor modification was made based on their feedback. Second, we used the sampling purposive method to select 25 respondents (they belong to different nations) to conduct the pilot study. This help ensures the validity and reliability of the instrument before disturbing it at a significant scale (van Teijlingen and Hundley, 2002). After ensuring the same understanding of the adopted scenario and related items, the final instrument was ready. Afterwards, the constructs were separated randomly in the final distributed questionnaire. Participation was voluntary, and no financial incentive was offered.

Moreover, there were no foreseeable risks associated with participation in the research, and participants were not required to provide any personal or identifying information. Participants were encouraged to provide honest answers but were informed of their right to withdraw from the study if they felt uncomfortable. Moreover, participants' responses will remain strictly confidential, and data will only be used for research purposes. The data obtained in the study will be reported in aggregate. After gathering data, researchers used Harman's single-factor test to determine whether CMB was present. The test revealed that the most significant variance was less than 50% (Podsakoff et al., 2012), indicating no CMB-related issue in the current study (Alraja, 2022; Imran et al., 2022).

Table 1
Sample characterization.

Characterization		Frequency	Per cent
Gender	Male	191	54.9
	Female	157	45.1
Country	USA	55	15.8
	UK	34	9.8
	Oman	65	18.7
	India	83	23.9
	Pakistan	42	12.1
	Malaysia	36	10.3
	Philippine	33	9.5
Major	IT and computer science	133	38.
	IS and data science	56	16.1
	Engineering	77	22.1
	Business	822	23.6
Age	20 to less than 30	59	17
	30 to less than 40	127	36.5
	40 to less than 50	120	34.5
	50 and more	42	12.1
Experience	less than 5	63	18.1
	5 to less than 10	97	27.9
	10 to less than 15	80	23
	15 and more	108	31

The complex model employed comprises 11 constructs, 51 indicators and 11 hypotheses. Thus, the composite-founded SEM, also termed partial least squares SEM (PLS-SEM), was deployed as the principal method to test the study model. PLS-SEM offer a good fit for this model type (Hair et al., 2010) and are thus appropriate for theory appraisal and prediction (Richter et al., 2016). The measurements and structure model were assessed using SmartPLS version 3. However, all the received questionnaires were screened carefully using SPSS 23. Altogether, 409 individuals responded to the invitation to participate in the study, and 348 (85%) met the inclusion criteria. This is pretty much in line with the samples of previous studies (Koohang et al., 2020, 2020; Moody et al., 2018), As well as considered suitable for analysing the data using partial least squares (PLS) (Hair et al., 2016). Two main phases were followed to examine the adopted model validity: measurement validation (corrected item-total correlations, skewness and kurtosis, outer loading criterion, Cronbach's alpha, composite reliability, average variance extracted (AVE), Fornell-Larcker criterion, Cross-loadings, and heterotrait-monotrait (HTMT) ratio). While the structural model was tested using Structural Equation modelling (SEM) after confirming the model validity using the following tests: variance inflation factor (VIF), Model's predictive accuracy, Effect size (F^2), and Predictive Relevance Q^2.

4. Analysis and results

4.1. Sample characterization

In order to test the measurement model, an appraisal protocol was performed incorporating the steps outlined below:

Step 1: The analysis of skewness and kurtosis for each item yielded results from +2 to −2 (Table 2), indicating a normal distribution.

Table 2
Results of measurement assessment.

Variable	Item	Mean	Standard Deviation	Excess Kurtosis	Skewness	$\alpha \geq 0.70$	CR $\geq$ 0.70	AVE $\geq$0.50	VIF	Outer Loading
Fear	Fea2	4.75	1.44	−0.64	−0.37	0.73	0.85	0.65	1.39	0.77
	Fea3	4.71	1.49	−0.57	−0.35				1.64	0.85
	Fea4	4.68	1.51	−0.27	−0.59				1.40	0.80
Habit	Hab2	5.10	1.43	0.14	−0.77	0.89	0.90	0.57	2.19	0.74
	Hab3	5.07	1.52	−0.46	−0.62				2.03	0.72
	Hab4	5.03	1.54	−0.33	−0.73				2.16	0.72
	Hab5	5.14	1.40	0.05	−0.73				2.55	0.76
	Hab6	4.86	1.54	−0.68	−0.49				1.66	0.85
	Hab7	4.99	1.46	−0.41	−0.54				2.66	0.80
	Hab8	4.89	1.50	−0.47	−0.52				2.00	0.71
Intention	Int1	4.36	1.55	−0.74	−0.27	0.84	0.92	0.86	2.09	0.91
	Int2	4.18	1.88	−1.11	−0.18				2.09	0.95
Neutralization	Neu1	4.26	1.80	−1.06	−0.17	0.83	0.90	0.75	1.66	0.83
	Neu2	3.89	1.86	−1.20	−0.01				2.70	0.91
	Neu3	4.08	1.78	−0.98	−0.10				2.21	0.86
Reactance	Rea1	4.89	1.49	−0.58	−0.40	0.83	0.92	0.85	1.99	0.94
	Rea2	4.73	1.46	−0.84	−0.29				1.99	0.91
Response Efficacy	RE1	4.93	1.45	−0.33	−0.39	0.83	0.90	0.75	1.74	0.81
	RE2	4.93	1.41	−0.51	−0.30				2.60	0.92
	RE3	4.96	1.42	−0.56	−0.35				2.06	0.87
Role Values	RV1	4.63	1.69	−0.59	−0.54	0.87	0.91	0.66	2.54	0.84
	RV2	4.63	1.48	−0.51	−0.49				2.34	0.81
	RV3	4.72	1.47	−0.39	−0.41				1.54	0.72
	RV4	4.45	1.71	−0.87	−0.25				2.71	0.86
	RV5	4.26	1.65	−0.77	−0.17				2.22	0.82
Threat	Thr1	4.79	1.47	−0.52	−0.37	0.82	0.88	0.64	1.70	0.77
	Thr2	4.86	1.44	−0.51	−0.40				1.79	0.81
	Thr3	4.97	1.38	−0.31	−0.52				1.91	0.83
	Thr4	5.06	1.41	−0.55	−0.51				1.79	0.81

Step 2: The following criteria were deployed to determine research model reliability:

(1) Indicator reliability: outer loading criterion $\geq$ 0.70 (Hair et al., 2010). Indicators with loadings of $<$ 0.70 were removed from the analysis, i.e. role values latent variable: indicators RV6, RV7, RV8 and RV9 (0.54, 0.56, 0.57, and 0.39) respectively, Hab1 (0.59) Fea1 (0.65). These were eradicated from the dataset, the data were re-analysed, and indicator reliability was attained. Except for these eliminated items, all remaining original items from the UMISPC could proceed with the analysis.

(2) Internal consistency reliability: two tests were employed, i.e. Cronbach's alpha (α) and composite reliability (CR). Each had a cut-off value of $\geq$ 0.70 (Hair et al., 2019); this was achieved for all latent variables (Table 2).

Step 3: The following criteria were applied to appraise the research model validity:

(1) Convergent validity: the criterion for the average variance extracted (AVE) is $\geq$ 0.50 (Fornell and Larcker, 1981; Hair et al., 2016). AVE for all items was greater than this threshold value, thus confirming convergent validity.

(2) Discriminant validity: this was assessed using three analytical methods, i.e.

- Fornell-Larcker criterion (Fornell and Larcker, 1981): The correlation matrix is illustrated in Table 4; the square root of the AVE for each latent variable is greater than its maximum correlation with any other latent variable.
- Cross-loadings: an indicator's outer loading shown in Table 2 on a latent variable is greater than all its cross-loadings with other latent variables (Hair et al., 2019)
- The heterotrait-monotrait (HTMT) ratio (Henseler et al., 2015): Optimal results are HTMT values $<$ 0.85, as seen for all items in Table 5. This index is used to compensate for the lack of sensitivity of the Fornell-Larcker criterion and cross-loading methods to document discriminant validity.

Table 4
The Fornell-Larcker discriminant validity correlation matrix.

Constructs	Fea	Hab	Int	Neu	Rea	RE	RV	Thr
Fear	**0.81**							
Habit	0.53	**0.76**						
Intention	0.31	0.24	**0.93**					
Neutralization	0.30	0.17	0.69	**0.87**				
Reactance	0.35	0.42	0.41	0.35	**0.92**			
Response Efficacy	0.48	0.59	0.13	0.07	0.49	**0.87**		
Role Values	0.26	0.21	0.63	0.56	0.27	0.07	**0.81**	
Threat	0.49	0.58	0.11	0.09	0.35	0.51	0.15	**0.80**

Table 5
The HTMT correlation matrix.

Constructs	Fea	Hab	Int	Neu	Rea	RE	RV	Thr
Fear								
Habit	0.65							
Intention	0.39	0.21						
Neutralization	0.38	0.17	0.81					
Reactance	0.44	0.49	0.50	0.42				
Response Efficacy	0.62	0.72	0.17	0.12	0.59			
Role Values	0.34	0.18	0.72	0.65	0.33	0.10		
Threat	0.63	0.68	0.16	0.13	0.42	0.61	0.19	

4.2. Measurement assessment

The results of these three methods demonstrate the presence of discriminant validity.

4.3. Analysis of the structural model

Before path analysis was performed, a multicollinearity test was applied using the variance inflation factor (VIF) method to exclude

Table 6
VIFs, R^2 and F^2.

Construct	Multicollinearity test				Model's predictive accuracy		Effect size (F^2)			
	Fear	Intention	Reactance	Threat	R^2	Adj R^2	Fear	Intention	Reactance	Threat
Fear		1.43	1.10		0.24	0.23		0.02	0.08	
Habit		1.39						0.00		
Intention					0.42	0.41				
Neutralization			1.10						0.08	
Reactance					0.18	0.18				
Response Efficacy				1						0.35
Role Values		1.08						0.451		
Threat	1				0.26	0.26	0.31			

Table 7
Results of Q^2 level assessment.

Constructs	Predictive Relevance Q^2, Q^2 (=1-SSE/SSO)			
	Construct Crossvalidated Communality		Construct Crossvalidated Redundancy:	
Fear	0.30	Moderate predictive power	0.15	Moderate predictive power
Habit	0.43	Strong predictive power		
Intention	0.48	Strong predictive power	0.34	Strong predictive power
Neutralization	0.48	Strong predictive power		
Reactance	0.47	Strong predictive power	0.15	Moderate predictive power
Response Efficacy	0.49	Strong predictive power		
Role Values	0.49	Strong predictive power		
Threat	0.40	Strong predictive power	0.16	Moderate predictive power

errors possibly originating from high correlations between the latent variables (Hair et al., 2010). With PLS-SEM, a collinearity issue is indicated by VIF $\geq$ 5 (Hair et al., 2010; Richter et al., 2016). Table 6 depicts all VIF values below this threshold, thus excluding multicollinearity problems.

The explained variance of the latent dependant variables relative to the total variance was evaluated using the coefficient of determination, R^2. Role values and fear described 42% of the variance in intention towards ISPC. 18% of reactance was explicated by fear and neutralization. RE was the principal determinant of threat, accounting for 26% of the variance within the threat construct. The threat was responsible for a 24% variance in the fear construct.

The relative influence of a predictor variable on an endogenous variable can be appraised through the effect size, f^2 (Hair et al., 2017; Hair et al., 2010); small, medium and large impacts are demonstrated by f^2 values of 0.02, 0.15 and 0.35, respectively (Richter et al., 2016). The f^2 values (< 0.02) revealed no influence from the construct habit ($f^2 = 0.00$) on intention towards ISPC. A small effect was seen with fear ($f^2 = 0.02$; 0.08) on intention and reactance, respectively, and the most dominant influence was from role values ($f^2 = 0.451$). The relative influences of RE on threat and of threat on fear were large and medium, i.e. $f^2 = 0.35$ and $f^2 = 0.31$, respectively. Furthermore, a small effect was seen from neutralization on reactance ($f^2 = 0.08$). Blindfolding in smartPLS was utilized to appraise the predictive relevance, Q^2, results (Table 7). The omission distance, D, was 7 (Hair et al., 2017). All Q^2 values were > 0, which was the cut-off level. The ability of the path model to predict the endogenous parameters indirectly from their relevant latent variables employing associated structural relations was determined using cross-validated redundancy. Weak, moderate and strong predictive relevance was indicated by Q^2 values of 0.02, 0.15 and 0.35, respectively (Hair et al., 2017). A high predictive relevance for intention ($Q^2 = 0.34$) was seen, whereas moderate predictive ability was noted for fear ($Q^2 = 0.15$), threat ($Q^2 = 0.16$) and reactance ($Q^2 = 0.15$).

To assess the predictive relevance of cross-validated commonality, the measurement model's ability to evaluate the path model directly from the relevant latent variable facilitated Q^2 computation. Seven demonstrated strong predictive power; one had moderate predictive power (Table 7). The model appears to have considerable predictive power based on these two methods. The path coefficients (β values) from the model's construct relationships are shown in Fig. 3.

A bootstrapping algorithm in PLS was used to determine significance; 5000 bootstrap samples were produced (Table 9).

Significance at 5% error probability for the (β values) was appraised from t and p values, i.e. $p \leq 0.05$ validated the hypothesis; t value > 1.96. Significance was achieved for the influence of fear and role values on intention towards ISPC, i.e. $\beta = 0.131$; $p \leq 0.05$; $\beta = 0.582$; $p \leq 0.05$. Thus, H1 and H6 were approved. Habit failed to reach significance on intention towards ISPC, i.e. $\beta = 0.049$; $p > 0.05$, so H3 was rejected. RE significantly predicted threat, i.e. $\beta = 0.511$; $p \leq 0.05$, so H7 was retained. Threat significantly predicted fear, i.e. β =0.486; $p \leq 0.05$. Therefore H5 was approved. Neutralization predicted reactance, i.e. $\beta = 0.267$; $p \leq 0.05$. Thus H4 were retained. Fear demonstrated significance with reactance, i.e. $\beta = 0.266$; $p > 0.05$, so H2 was accepted.

5. Discussion

The results from this study reinforced the refined UMISPC constructed by Moody et al. (2018), although the indicator number in the role values and habit constructs was adjusted in this study. Indicator reliability and internal consistency suggested model reliability. Convergent and discriminant validity assessments demonstrated strong model support. No multicollinearity was detected using the VIF values and the parameters for endogenous construct variance, R^2, were satisfactory. Blindfolding-based cross-validated redundancy parameter values, Q^2, and the construct cross-validated communality testing met the criteria. The effect size, f^2, demonstrated the relative impacts of the constructs.

This research has appraised the UMISPC. The data are summarized in Table 11, and for the most part, reinforced the UMISPC along both paths, i.e. (i) intention towards ISPC compliance, where fear and role values were essential predictors, and (ii) reactance which was predicted by fear and neutralization. Fear was predicted by perceived threat; RE anticipated threat. In parallel with the original study, no influence on intention towards ISPC was seen with habits. The latter construct was contrary to the findings of Moody et al. (2018). Thus, the present data provide evidence

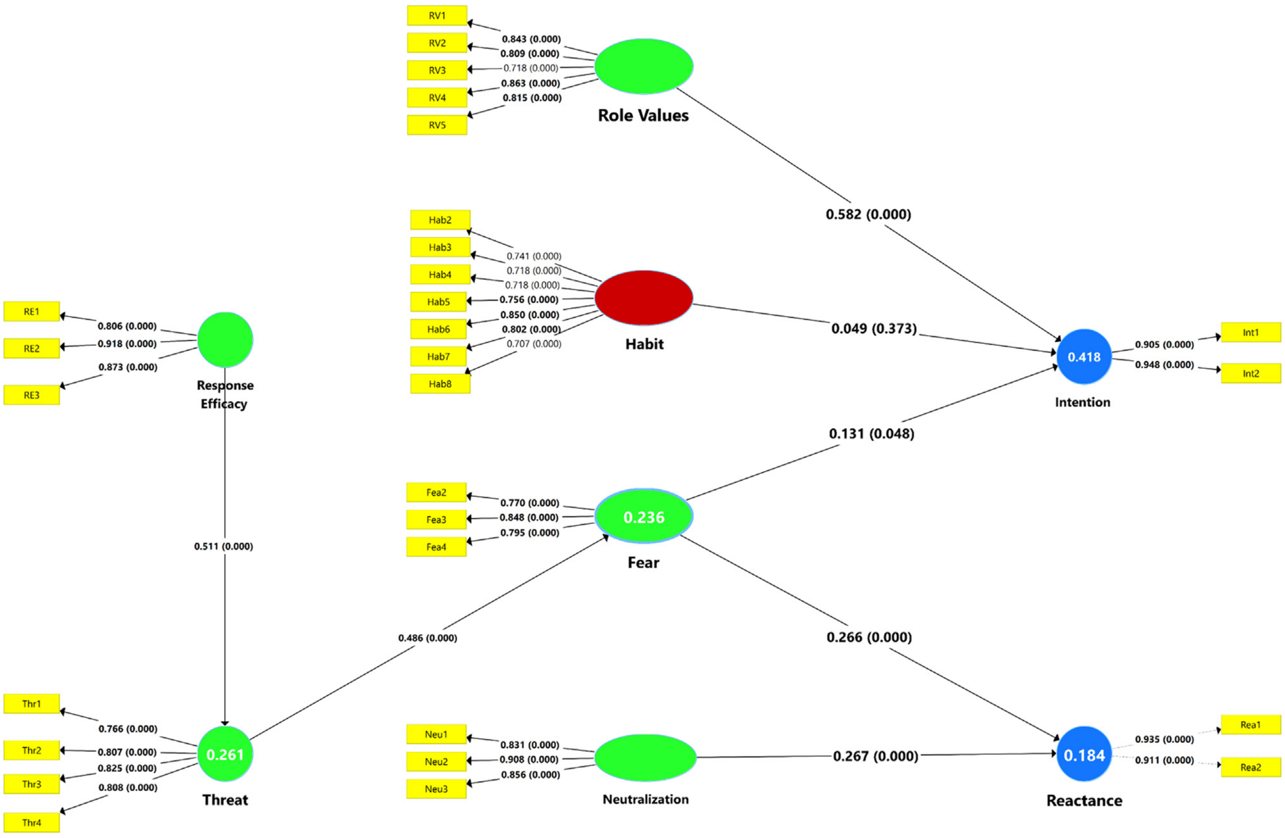


Fig. 3. Structural model path coefficients.

Table 9
Results of hypotheses testing.

Hypothesis	Path	β coefficients	T Statistics	P Values	Result
H1	Fear → Intention	0.131	1.98	0.048	Support
H2	Fear → Reactance	0.266	5.017	0	Support
H3	Habit → Intention	0.049	0.893	0.373	**Reject**
H4	Neutralization → Reactance	0.267	5.056	0	Support
H5	Response Efficacy → Threat	0.511	11.138	0	Support
H6	Role Values → Intention	0.582	14.165	0	Support
H7	Threat → Fear	0.486	9.347	0	Support

Table 11
Comparing the current findings with the UMISPC's results.

Path	UMISPC	Current results
Fear → Intention	Supported	Supported
Fear → Reactance	Supported	Supported
Habit → Intention	Supported	**Not supported**
Neutralization → Reactance	Supported	Supported
Response Efficacy → Threat	Supported	Supported
Role Values → Intention	Supported	Supported
Threat → Fear	Supported	Supported

that intentions to perform safeguarding behaviour are elucidated through the constructs, role values and fear.

Only one out of the seven relations disagreed with the findings from Moody et al. (2018). Hence, the final model is presented in Fig. 4 below. The relevance of these findings and their importance for research and practice are discussed in the implications section.

The main goal was to determine if the UMISPC is reliable and generalizable and to pinpoint the variables that could influence employees' intentions and reactance towards information systems security policy compliance in a global setting. i.e. Examine if neutralization, response effectiveness, fear, threat, habit, and role values are accurate predictors of reactance and intention towards ISPC. Additionally, the possibility that neutralization and fear may influence reactance. This will be explored by analysing the degree to which fear is anticipated through the observed threat and how the latter is indicated by response effectiveness. Another goal is to determine if the same (or different) factors influence employees' desire to follow ISPs and reactance. More specifically, we draw attention to the results that follow.

First, prior studies (even though very limited) have had consistent findings when applying UMISCP to employees' intentions and reactance toward compliance with ISP (Koohang et al., 2020; Moody et al., 2018), which may be attributable to the model's generalizability. The current study, involving 348 participants from 7 countries, shows that the effect of habits on employees' intention to comply with ISPs is statistically insignificant. This result leads to rejecting H1, which is similar to Koohang et al. (2020) and opposite to many previously conducted research (Bhatnagar and Papatla, 2019; Hanus and Wu, 2016; Lankton et al., 2010; Moody et al., 2018; Vance et al., 2012; Zhang et al., 2015) demonstrated that vital role played by habits. This may be explained as follows, employees in higher education institutions may perform an un-habitual be-

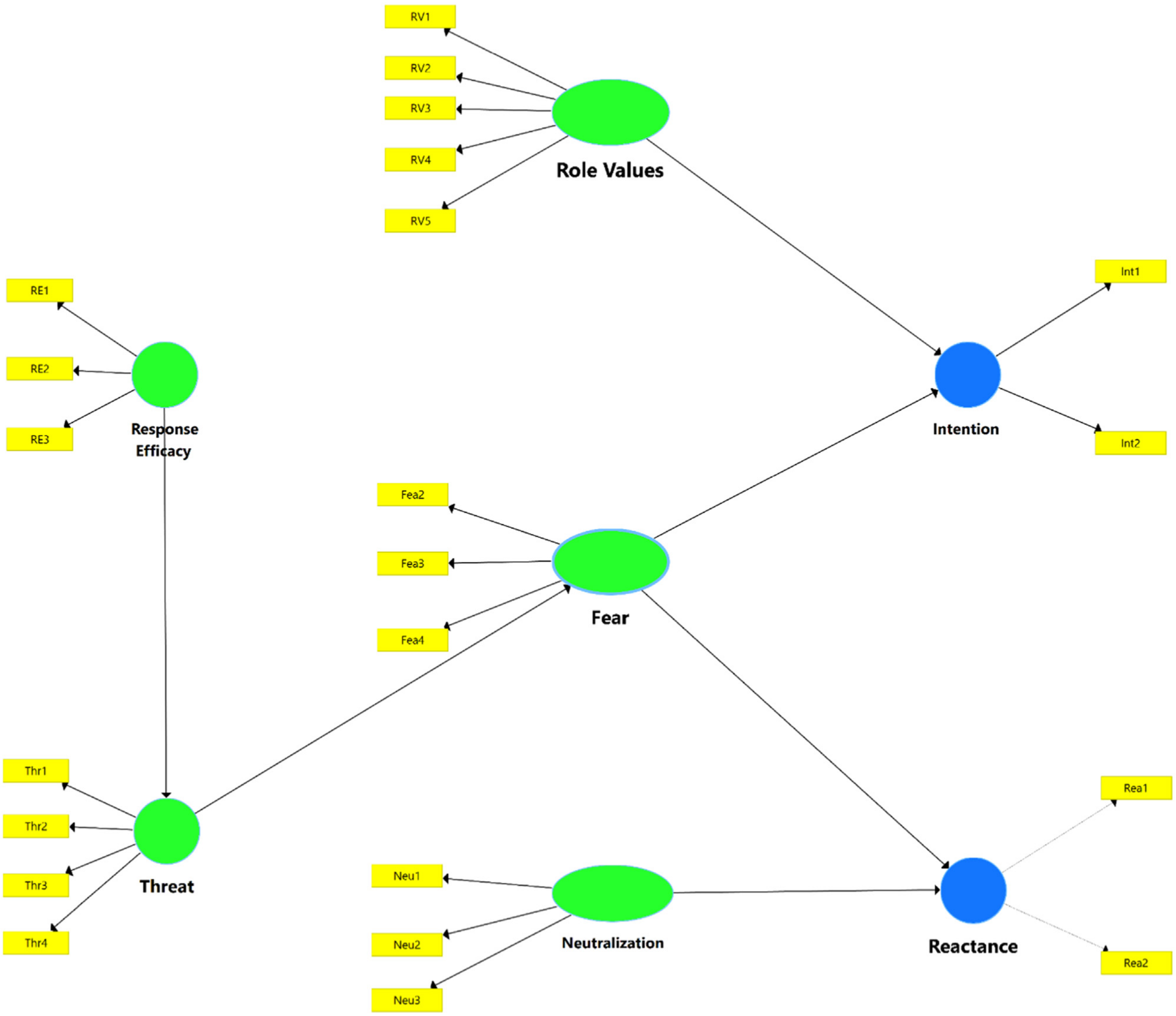


Fig. 4. final model is presented.

haviour because of their job nature and movement. Therefore, developing such automated response behaviour (habit) may be challenging. Thereby, it will not be entrenched behaviour.

Second, our findings indicate that fear and role values positively influenced the intention to comply with the ISP, leading to support H5 and H2. For fear, if employees view non-compliance as hazardous, they will protect themselves and demonstrate conformity. This result agrees with the findings of previous research (Herath and Rao, 2009; Johnston et al., 2015; Lee and Larsen, 2009; Siponen et al., 2014), especially when fear is a retort to threats, and in contrast with (Koohang et al., 2020). While role values (which have the most substantial effect in the tested model), as stated by Moody et al. (2018), are the beliefs/principles/standards associated with the nature of the work individuals perform. This result also aligns with the previous research (Koohang et al., 2020, 2020; Moody et al., 2018) as role values consider the profession and the individual's job (role). Therefore, when employees perceive that enacting ISPC is relevant, justified, and reasonable, they will comply with ISPs.

Third, our results indicate that threat was a significant precursor to fear, i.e., H4 supported. This result is in line with previous research results (Burns et al., 2017; Moody et al., 2018). those that opt to exhibit ISPC do so through fear associated with an apparent threat. Employees who wished to violate compliance objectives would be aware of the danger of personal harm due to ISPC infringement. Transgressors often failed to correctly assess the consequences of their actions or were confident they could ride them.

Fourth, our results indicate that Response efficacy is a good predictor of threat, leading to accepting H3. This finding is similar to the findings (Koohang et al., 2020; Moody et al., 2018) studies. Thus, employees who appreciated the response from the guidelines noted the specific threat to security which enabled them to evade or reduce it.

Fifth, our findings indicate that fear and neutralization positively influenced reactance, leading to accepting H6 and H7. For fear, if an individual's efficiency assessment leads them to believe they do not have the skill to evade the threat, they will diminish fear by indulging in fear-control responses such as defensive avoidance, denial, and reactance. This result agrees with the findings of previous research (Moody et al., 2018) and partially with (Koohang et al., 2020) as fear significantly affected reactance but negatively. Neutralization, as stated by Moody et al. (2018) significant factor in excusing many ISS infringements such as password sharing, USB use, and failing to lock computers. This result aligns with (Koohang et al., 2020; Moody et al., 2018). That may be because the infringements of ISPC were explained by an imprecise policy, failure to believe perpetrators were doing harm, and the apparent need to perform a beneficial task for the organization.

The present study is the most comprehensive investigation into how specific factors (i.e. UMISPC) relating to different global settings can impact employees' compliance with information security. The study thus fills the void in research, where most studies have only concentrated on a single country (e.g., Moody et al., 2018). In this paper, employees' attitudes and compliance with ISPC were examined globally, generating a more profound insight into the key factors that impact employee compliance with such policies. The study's findings highlight the importance of further investigating the revised model internationally and considering cultural factors. Future researchers should also consider investigating the topic in different industries. After reassessing the refined framework, it has been found that the following one factor has no significant effect on employees' compliance with ISP, i.e. habits. Our research thus supports the revised UMISPC as a valid model for use in global settings. In addition to the implications mentioned above, to the author's knowledge, the presented research makes the following contributions to existing publications on ISPC:

(1) It is the first study to relate UMISPC to an international data sample (i.e. seven countries).
(2) The work shows that UMISPC alone can be applied in place of the eleven original theoretical concepts to elucidate the rationale relating to workers' ISP transgressions or intentions. In addition, the UMISPC proved to be theoretically sound within the three examined scenarios.
(3) The study results indicate that UMISPC is a valid model that can be generalized and applied to investigate intention towards ISPC and reactance.
(4) This research focuses on a homogeneous group of users from a specific workplace with similar job descriptions, i.e. university employees, rather than on a heterogeneous population.

5.1. Implications for practice

41.2% of the variance in intention towards ISPC can be accounted for through a combination of role values and fear. The construct of role values had the most substantial influence, indicating that participants were cognizant of their ISP, felt it appropriate to their job description and were ethically obliged to conform, results which are consistent with previous studies (Koohang et al., 2020, 2020; Moody et al., 2018). Four indicators were excluded; these were the same as those eradicated by Koohang et al. (2020). Thus, only five of the original nine were utilized owing to the low indicator loading of the eliminated four items. ISPC is relevant in occupational settings, which is where transgressions occur. The role values construct indicators are all related to intrinsic worker beliefs. These, in turn, are associated with workers' psychological and moral traits rather than hierarchical strategies. These elements can be gradually altered temporally. It would benefit managers to focus on methods to introduce, inspire, nurture and bolster role values amongst their employees, particularly when creating ISP.

Furthermore, new personnel should only be selected if they reflect this doctrine and security-centric atmosphere. Workplace guidelines should incorporate processes that complement job descriptions and daily activities. Furthermore, training on ISP requirements concerning specific work aspects will increase compliance. The data for RE indicated that this variable has a significant positive influence on threat prediction, accounting for 26.1% of the threat construct variance. On the same path, the threat has the most positive effect on fear, i.e. 23.6% of fear's variance, although fear has a minor influence on intention towards ISPC and a medium impact on reactance.

Previous studies have also found that RE influences threat; the latter subsequently impacts fear (Jansen and Schaik, 2019; Koohang et al., 2020; Moody et al., 2018). However, the only difference with the results of Moody et al. (2018) in this study is that fear positively impacted intention towards ISPC. The latter was also opposed to the findings of Koohang et al. (2020). The presented data are, therefore, novel; the majority of reviewed publications have associated RE (Ifinedo, 2012; Liu et al., 2020; Thompson et al., 2017) and threat (Liu et al., 2020) (Rajab and Eydgahi, 2019) with intention towards ISPC. Fear was tested in this work as a precursor for intentional behaviour in a different area, not in the original setting of health psychology, where it was associated with health threat evasion (D'Arcy and Herath, 2011), and also as a construct in an alternative model from PMT. This is in contrast to earlier work where other constructs, e.g. threat, were antecedent and had RE as a precursor.

In keeping with proposals from the original study, the present research noted that RE significantly influenced the threat. Establishments need to encourage workers' trust such that ISPC reduces security transgressions. The message should communicate that this does not just affect workers, i.e. the whole institution could be at risk if ISPC is not followed. An equilibrium between threat and efficacy needs to be maintained. However, if the balance tips towards the former, the contrary effect may occur, causing reactance. Reactance may also arise from incidences where workers cannot see evidence of a real threat, e.g. anti-malware warnings, deceleration of computer performance or a rise in software crashing.

ISCP intention was not significantly influenced by habit. Furthermore, no relative effects of these constructs were seen. This neutral construct is usually related to executive activities (Cram et al., 2019) and is thought to be more readily engineered at hierarchical levels. These results align with previous publications (Alasmari and Zhang, 2019; Ifinedo, 2012; Moody et al., 2018; Pee et al., 2008; Vance et al., 2020; Verkijika, 2018).

Habit influenced ISPC, a finding that agreed with Koohang et al. (2020) but was at odds with Moody et al. (2018). One cause for this could be that university staff utilize their passwords daily throughout their job, and more than 80% claimed over five years of experience (Table 1). Thus, password sharing, USB use and locking computers may be performed automatically, and users may not thoughtfully reflect on potential transgression consequences. Thus, institutions should take workers' habits into account when instigating ISPs.

Over a quarter of reactance variance was explicated by a combination of neutralization and fear. Neutralization had a moderate influence on reactance, so it is a good predictor of intention to infringe ISPs (Moody et al., 2018; Vance et al., 2020). Previous studies (Moody et al., 2018; Puhakainen, 2006; Siponen and Vance, 2010b) have recommended that institutions instigate frequent consultations and educational opportunities to apprise workers regarding anticipated harm from ISP non-conformity and present case examples of the consequences. Line managers should also assist their team by heightening their appreciation of possible harm to the entire establishment. If security is breached, avoid giving overt or tacit permission to workers for shortcuts to complete urgent time-sensitive tasks that may require a security infringement. Their party line should be that no reason is sufficient for compliance failure and that security responsibility requires everyone, without exception, to follow ISPs.

5.2. Limitations and opportunities for future research

First, although this study's respondents came from seven different countries and worked for various organizations, showing strong geographic generalizability in comparison to earlier studies, its context generalizability still needs further research because our paper did not examine the differences between those various samples. Future research may use the same comparison approach to demonstrate how cultural differences influence and determine ISP compliance behaviour. The second possible limitation is that this study did not include any mediatory role in the investigated model. Thus, future work may include the mediatory role of fear between RE/threat and ISPC /reactance. In addition, there is a question of how companies can assist skill development amongst workers and thus improve RE?

Third, the current study did not extend the UMISCP by adding any other proper variable, as the primary purpose was to examine the model's reliability in global settings. Hence, it is suggested that additional constructs, e.g. job role, could be explored as potential moderators of the associations between habit and ISPC. Fourth, as technology and its implementations change continuously, further work is required to develop and use alternative scenarios with more complicated ISS activities. Finally, the current study tested neutralization as one component. Therefore, it is essential to investigate its components (method) and identify which one, i.e. denial of responsibility, denial of injury, denial of victim, condemnation of the condemners and appeal to higher loyalties, are predictive of the reactance construct. In addition, the question regarding how ISPC can become integral to the institutional ethos requires a solution. The path of the relationship, i.e. neutralization with reactance, differed according to the subjects' experience. Thus, more research is required to explore the possibility that experience could be a moderator for this relationship.

6. Conclusions

This study aimed to evaluate the original UMISPC, constructed by Moody et al. (2018), comprised of eight constructs relating to ISPC, i.e., role values, habit, neutralization, threat, fear, response efficacy, reactance, and compliance intention. The UMISPC was applied to a novel data sample ($n = 348$) from multi-national sources. The findings reinforced the refined UMISPC within the three examined ISS transgressions in this global setting. Path modelling verified the reliability and validity of the UMISPC. Findings affirmed the original study's results, i.e. that habit was not influential in intention towards ISPC. The novel construct, role values, significantly impacted intention towards ISPC. In the path model, RE affected threat, which itself impacted fear, and fear subsequently influenced intention towards ISPC and reactance. The latter was affected by neutralization also. Our findings are helpful for ISS literature and application by supporting the crucial functions of role values in encouraging employees to behave in a compliant manner. Additionally, it is regarded as the first empirical attempt to estimate intended compliance concerning ISPs in higher education from a worldwide viewpoint.

Author statement

Mansour Alraja: Conceptualization, Methodology, Data collection and analysis, Project administration, Funding acquisition, Writing- Reviewing and Editing. **Usman Javed Butt**: Writing- Original draft preparation, Writing- Reviewing and Editing. **Maysam Abbod**: Writing- Reviewing and Editing,

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgement

This work is supported by The Research Council (TRC), Sultanate of Oman (Block Fund-Research Grant), BFP/RGP/ICT/21/132.

References

Aggarwal, A., Dhurkari, R.K., 2023. Association between stress and information security policy non-compliance behavior: a meta-analysis. Comput. Secur. 124, 102991. doi:10.1016/J.COSE.2022.102991.

Alasmari, T., Zhang, K., 2019. Mobile learning technology acceptance in Saudi Arabian higher education: an extended framework and A mixed-method study. Educ. Inf. Technol. 24 (3), 2127–2144. doi:10.1007/s10639-019-09865-8.

Alraja, M., 2022. Frontline healthcare providers' behavioural intention to Internet of Things (IoT)-enabled healthcare applications: a gender-based, cross-generational study. Technol. Forecast. Soc. Change 174, 121256. doi:10.1016/J.TECHFORE.2021.121256.

Angraini, Alias, R.A., Okfalisa, 2019. Information security policy compliance: systematic literature review. Procedia Comput. Sci. 161, 1216–1224. doi:10.1016/j.procs.2019.11.235.

Aubley, C., Bowen, E., Frank, W., Golden, D., Morris, M., Norton, K., 2021. The Future of Cybersecurity and AI: Augmenting security Teams With Data and Machine Intelligence. Deloitte Insights https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html.

Baillette, P., Barlette, Y., 2020. Coping strategies and paradoxes related to byod information security threats in France. J. Glob. Inf. Manag. 28 (2), 1–28. doi:10.4018/JGIM.2020040101.

Bamberg, S., Schmidt, P., 2003. Incentives, Morality, Or Habit? Predicting Students' Car Use for University Routes With the Models of Ajzen, Schwartz, and Triandis. Environ. Behav. 35 (2), 264–285. doi:10.1177/0013916502250134.

Bansal, G., Muzatko, S., Shin, S.I., 2020. Information system security policy noncompliance: the role of situation-specific ethical orientation. Inf. Technol. People doi:10.1108/ITP-03-2019-0109.

Bhaharin, S.H., Mokhtar, U.A., Sulaiman, R., Yusof, M.M., 2019. Issues and trends in information security policy compliance. *International Conference on Research and Innovation in Information Systems, ICRIIS, December-2019* doi:10.1109/ICRIIS48246.2019.9073645.

Bhatnagar, A., Papatla, P., 2019. Do habits influence the types of information that smartphone shoppers seek? J. Bus. Res. 94, 89–98. doi:10.1016/j.jbusres.2018.09.012.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P., 2015. What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Q. 39 (4), 837–864. doi:10.25300/MISQ/2015/39.4.5.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. (3) 34. https://misq.org/information-security-policy-compliance-an-empirical-study-of-rationality-based-beliefs-and-information-security-awareness.html.

Burns, A.J., Posey, C., Roberts, T.L., Benjamin Lowry, P., 2017. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Comput. Hum. Behav. 68, 190–209. doi:10.1016/j.chb.2016.11.018.

Chen, D.Q., Liang, H., 2019. Wishful Thinking and IT Threat Avoidance: an Extension to the Technology Threat Avoidance Theory. IEEE Trans. Eng. Manage. 66 (4), 552–567. doi:10.1109/TEM.2018.2835461.

Chen, Y., Xia, W., Cousins, K., 2022. Voluntary and instrumental information security policy compliance: an integrated view of prosocial motivation, self-regulation and deterrence. Comput. Secur. 113, 102568. doi:10.1016/J.COSE.2021.102568.

Chen, Y., Zahedi, F.M., 2016. Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. MIS Q. 40 (1), 205–222. doi:10.25300/MISQ/2016/40.1.09.

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. Comput. Hum. Behav. 38, 220–228. doi:10.1016/j.chb.2014.05.043.

Cram, W.A., D'Arcy, J., Proudfoot, J.G., 2019. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Q. 43 (2), 525–554. doi:10.25300/MISQ/2019/15117.

Crossler, R.E., 2010. Protection motivation theory: understanding determinants to backing up personal data. In: Proceedings of the Annual Hawaii International Conference on System Sciences doi:10.1109/HICSS.2010.311.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101. doi:10.1016/j.cose.2012.09.010.

D'Arcy, J., Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur. J. Inf. Syst. 20 (6), 643–658. doi:10.1057/ejis.2011.23.

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

D'Arcy, J., Teh, P.L., 2019. Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization. Inf. Manag. 56 (7), 103151. doi:10.1016/j.im.2019.02.006.

da Veiga, A., Astakhova, L.V., Botha, A., Herselman, M., 2020. Defining organisational information security culture—perspectives from academia and industry. Comput. Secur. 92, 101713. doi:10.1016/j.cose.2020.101713.

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. Comput. Hum. Behav. 60, 508–513. doi:10.1016/j.chb.2016.02.010.

Europol. (2021, December). *Covid-19: ransomware*. https://www.europol.europa.eu/covid-19/covid-19-ransomware.

Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. 30 (2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x.

Fornell, C., Larcker, D.F., 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J. Market. Res. 18 (1), 39. doi:10.2307/3151312.

Gardner, B., 2015. A review and analysis of the use of 'habit' in understanding, predicting and influencing health-related behaviour. Health Psychol. Rev. 9 (3), 277–295. doi:10.1080/17437199.2013.876238.

Guan, B., Hsu, C., 2020. The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. Internet Res. doi:10.1108/INTR-06-2019-0260.

Gwebu, K.L., Wang, J., Hu, M.Y., 2020. Information security policy noncompliance: an integrative social influence model. Inf. Syst. J. 30 (2), 220–269. doi:10.1111/isj.12257.

Hair, J., Hollingsworth, C.L., Randolph, A.B., Chong, A.Y.L., 2017. An updated and expanded assessment of PLS-SEM in information systems research. Ind. Manag. Data Syst. 117 (3), 442–458. doi:10.1108/IMDS-04-2016-0130.

Hair, J.F., Anderson, R.E., Tatham, R.L., Black, W.C., 2010a. Multivariate Data Analysis, 7th ed. Prentice-Hall, Inc https://dl.acm.org/citation.cfm?id=207590.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2016. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed. Sage Publishing doi:10.1007/s10995-012-1023-x.

Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M., 2019. When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. 31 (1), 2–24. doi:10.1108/EBR-11-2018-0203/FULL/XML.

Hanus, B., Wu, Y., 2016. Impact of Users' Security Awareness on Desktop Security Behavior: a Protection Motivation Theory Perspective. Inf. Syst. Manag. 33 (1), 2–16. doi:10.1080/10580530.2015.1117842.

Hassandoust, F., Techatassanasoontorn, A.A., 2019. Understanding users' information security awareness and intentions: a full nomology of protection motivation theory. In: Cyber Influence and Cognitive Threats. Elsevier, pp. 129–143. doi:10.1016/B978-0-12-819204-7.00007-5.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43 (1), 115–135. doi:10.1007/s11747-014-0403-8.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125. doi:10.1057/ejis.2009.6.

Hou, Y., Gao, P., Nicholson, B., 2018. Understanding organisational responses to regulative pressures in information security management: the case of a Chinese hospital. Technol. Forecast. Soc. Change 126, 64–75. doi:10.1016/J.TECHFORE.2017.03.023.

Hovav, A., D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Inf. Manag. 49 (2), 99–110. doi:10.1016/j.im.2011.12.005.

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*. Decis. Sci. 43 (4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x.

Hu, Q., Xu, Z., Dinev, T., Ling, H., 2011. Does deterrence work in reducing information security policy abuse by employees? Commun. ACM 54 (6), 54–60. doi:10.1145/1953122.1953142.

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

Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31 (1), 83–95. doi:10.1016/j.cose.2011.10.007.

Imran, R., Alraja, M.N., Khashab, B., 2022. Sustainable Performance and Green Innovation: green Human Resources Management and Big Data as Antecedents. IEEE Trans. Eng. Manage. 1–16. doi:10.1109/tem.2021.3114256.

Jaeger, L., Eckhardt, A., Kroenung, J., 2020. The role of deterrability for the effect of multi-level sanctions on information security policy compliance: results of a multigroup analysis. Inf. Manag., 103318 doi:10.1016/j.im.2020.103318.

Jansen, J., Schaik, P.V., 2019. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. Int. J. Hum. Comput. Stud. 123, 40–55. doi:10.1016/j.ijhcs.2018.10.004.

Johnston, A.C., Warkentin, M., 2010. Fear appeals and information s ecurity behaviors: an empirical study. MIS Q. 34 (3), 549–566. doi:10.2307/25750691, SPEC. ISSUE.

Johnston, A.C., Warkentin, M., Siponen, M., 2015a. An Enhanced Fear Appeal Rhetorical Framework: leveraging Threats to the Human Asset Through Sanctioning Rhetoric. MIS Q. 39 (1), 113–134. doi:10.25300/MISQ/2015/39.1.06.

Johnston, A.C., Warkentin, M., Siponen, M., 2015b. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. 39 (1), 113–134. doi:10.25300/MISQ/2015/39.1.06.

Junglas, I.A., Johnson, N.A., Spitzmüller, C., 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur. J. Inf. Syst. 17 (4), 387–402. doi:10.1057/ejis.2008.29.

Kam, H.-J., Katerattanakul, P., Hong, S., 2015. A Tale of Two Cities: policy Compliance of the Banks in the United States and South Korea. Twenty-Third European Conference on Information Systems (ECIS) https://www.researchgate.net/publication/274194565_A_Tale_of_Two_Cities_Policy_Compliance_of_the_Banks_in_the_United_States_and_South_Korea.

Kang, M., Miller, A., Jang, K., Kim, H., 2022. Firm performance and information security technology intellectual property. Technol. Forecast. Soc. Change 181, 121735. doi:10.1016/J.TECHFORE.2022.121735.

Karjalainen, M., Sarker, S., Siponen, M., 2019. Toward a theory of information systems security behaviors of organizational employees: a dialectical process perspective. Inf. Syst. Res. 30 (2), 687–704. doi:10.1287/isre.2018.0827.

Karjalainen, M., Siponen, M., Puhakainen, P., Sarker, S., 2013. One Size Does Not Fit All: different Cultures Require Different Information Systems Security Interventions. In: PACIS 2013 Proceedings.

Karlsson, F., Kolkowska, E., Petersson, J., 2022. Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis. Comput. Secur. 114, 102578. doi:10.1016/J.COSE.2021.102578.

Keikhosrokiani, P., 2020. Emotional-persuasive and habit-change assessment of mobile medical information Systems (mMIS). In: Perspectives in the Development of Mobile Medical Information Systems. Elsevier, pp. 101–109. doi:10.1016/b978-0-12-817657-3.00006-7.

Khatib, R., Barki, H., 2020. An activity theory approach to information security noncompliance. Inf. Comput. Secur. doi:10.1108/ICS-11-2018-0128.

Khokhar, R.H., Iqbal, F., Fung, B.C.M., Bentahar, J., 2021. Enabling secure trustworthiness assessment and privacy protection in integrating data for trading person-specific information. IEEE Trans. Eng. Manage. 68 (1), 149–169. doi:10.1109/TEM.2020.2974210.

Kim, H.M., Bock, G.W., Kim, H.S., 2020. A new perspective on online malicious comments: effects of attention and neutralization. Inf. Technol. People doi:10.1108/ITP-04-2019-0179.

Kim, S.-.Y., Levine, T.R., Allen, M., 2017. The Intertwined Model of Reactance for Resistance and Persuasive Boomerang. Commun. Res. 44 (7), 931–951. doi:10.1177/0093650214548575.

Koohang, A., Anderson, J., Nord, J.H., Paliszkiewicz, J., 2019. Building an awareness-centered information security policy compliance model. Ind. Manag. Data Syst. 120 (1), 231–247. doi:10.1108/IMDS-07-2019-0412.

Koohang, A., Nord, J.H., Sandoval, Z.V., Paliszkiewicz, J., 2020a. Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. J. Comput. Inf. Syst. doi:10.1080/08874417.2020.1779151.

Koohang, A., Nowak, A., Paliszkiewicz, J., Nord, J.H., 2020b. Information Security Policy Compliance: leadership, Trust, Role Values, and Awareness. J. Comput. Inf. Syst. 60 (1), 1–8. doi:10.1080/08874417.2019.1668738.

Lankton, N.K., Wilson, E.V., Mao, E., 2010. Antecedents and determinants of information technology habit. Inf. Manag. 47 (5–6), 300–307. doi:10.1016/j.im.2010.06.004.

Lazarus, R.S., 1991. Progress on a cognitive-motivational-relational theory of emotion. Am. Psychol. 46 (8), 819–834. doi:10.1037/0003-066X.46.8.819.

Lee, G., Lee, W.J., 2009. Psychological reactance to online recommendation services. Inf. Manag. 46 (8), 448–452. doi:10.1016/j.im.2009.07.005.

Lee, Y., Larsen, K.R., 2009. Threat or coping appraisal: determinants of SMB executives′ decision to adopt anti-malware software. Eur. J. Inf. Syst. 18 (2), 177–187. doi:10.1057/ejis.2009.11.

Li, Y., Pan, T., Zhang, N., 2019. From hindrance to challenge: how employees understand and respond to information security policies. J. Enterprise Inf. Manag. 33 (1), 191–213. doi:10.1108/JEIM-01-2019-0018.

Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS Q. 33 (1), 71–90. doi:10.2307/20650279.

Limayem, M., Hirt, S., 2003. Force of Habit and Information Systems Usage: theory and Initial Validation. J. Assoc. Inf. Syst. 4 (1), 65–97. doi:10.17705/1jais.00030.

Limayem, M., Hirt, S.G., Cheung, C.M.K., 2007. How habit limits the predictive power of intention: the case of information systems continuance. MIS Q. 31 (4), 705–737. doi:10.2307/25148817.

Liu, C., Wang, N., Liang, H., 2020. Motivating information security policy compliance: the critical role of supervisor-subordinate guanxi and organizational commitment. Int. J. Inf. Manage. 54, 102152. doi:10.1016/j.ijinfomgt.2020.102152.

Lowry, P.B., Moody, G.D., 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Inf. Syst. J. 25 (5), 433–463. doi:10.1111/isj.12043.

Maddux, J.E., 1993. Social cognitive models of health and exercise behavior: an introduction and review of conceptual issues. J. Appl. Sport Psychol. 5 (2), 116–140. doi:10.1080/10413209308411310.

Maruna, S., Copes, H., 2005. What Have We Learned from Five Decades of Neutralization Research? Crime Justice 32, 221–320. doi:10.2307/3488361.

May, P.J., 2004. Compliance Motivations: affirmative and Negative Bases. Law <html_ent Glyph="@amp;" Ascii="&"/>Society Review 38 (1), 41–68. doi:10.1111/j.0023-9216.2004.03801002.x.

McLeod, A., Dolezel, D., 2022. Information security policy non-compliance: can capitulation theory explain user behaviors? Comput. Secur. 112, 102526. doi:10.1016/J.COSE.2021.102526.

Menard, P., Bott, G.J., Crossler, R.E., 2017. User Motivations in Protecting Information Security: protection Motivation Theory Versus Self-Determination Theory. J. Manag. Inf. Syst. 34 (4), 1203–1230. doi:10.1080/07421222.2017.1394083.

Mirtsch, M., Kinne, J., Blind, K., 2021. Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: a Web Mining-Based Analysis. IEEE Trans. Eng. Manage. 68 (1), 87–100. doi:10.1109/TEM.2020.2977815.

Moody, G.D., Siponen, M., Pahnila, S., 2018. Toward a Unified Model of Information Security Policy Compliance. MIS Q. 42 (1), 285–311. doi:10.25300/MISQ/2018/13853.

Mouakket, S., Sun, Y., 2019. Examining factors that influence information disclosure on social network sites from the perspective of network externalities. Ind. Manag. Data Syst. 119 (4), 774–791. doi:10.1108/IMDS-02-2018-0060.

Nam, T., 2019. Understanding the gap between perceived threats to and preparedness for cybersecurity. Technol. Soc. 58, 101122. doi:10.1016/j.techsoc.2019.03.005.

NCSC, N. C. S. C. (2021). *Annual Review 2021 Making the UK the safest place to live and work online*. https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2021.pdf.

NIST. (2022). *Getting Started with Cybersecurity Risk Management: ransomware*.

Paananen, H., Lapke, M., Siponen, M., 2020. State of the art in information security policy development. Comput. Secur. 88, 101608. doi:10.1016/J.COSE.2019.101608.

Pee, L.G., Woon, I.M.Y., Kankanhalli, A., 2008. Explaining non-work-related computing in the workplace: a comparison of alternative models. Inf. Manag. 45 (2), 120–130. doi:10.1016/j.im.2008.01.004.

Ping, R.A., 2004. On assuring valid measures for theoretical models using survey data. J. Bus. Res. 57 (2), 125–141. doi:10.1016/S0148-2963(01)00297-1.

Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of Method Bias in Social Science Research and Recommendations on How to Control It. Annu. Rev. Psychol. 63 (1), 539–569. doi:10.1146/annurev-psych-120710-100452.

Puhakainen, P., 2006. A design theory for information security awareness. [Faculty of Science, University of Oulu] http://jultika.oulu.fi/files/isbn9514281144.pdf.

Putri, F.F., Hovav, A., 2014. Employees' compliance with byod security policy: insights from reactance, organizational justice, and protection motivation theory. European conference on information systems (ECIS) 2014 proceedings http://aisel.aisnet.org/ecis2014/proceedings/track16/2/.

Quick, B.L., LaVoie, N.R., Reynolds-Tylus, T., Martinez-Gonzalez, A., Skurka, C., 2018. Examining mechanisms underlying fear-control in the extended parallel process model. Health Commun. 33 (4), 379–391. doi:10.1080/10410236.2016.1266738.

Rajab, M., Eydgahi, A., 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Comput. Secur. 80, 211–223. doi:10.1016/j.cose.2018.09.016.

Richter, N.F., Sinkovics, R.R., Ringle, C.M., Schlägel, C., 2016. A critical look at the use of SEM in international business research. Int. Mark. Rev. 33 (3), 376–404. doi:10.1108/IMR-04-2014-0148.

Rogers, R., ROGERS, R.W., Rogers, R., Rogers, R.W., 1983. Cognitive and physiological process in fear appeals and attitudes changer: a revised theory of protection motivation. Soc. Psychophysiol. 153–176. https://www.scienceopen.com/document?vid=a182a645-fc12-4d21-9e22-15c96a792275.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. J. Psychol. 91 (1), 93–114. doi:10.1080/00223980.1975.9915803.

Rogers, R.W., Prentice-Dunn, S., 1997. Protection motivation theory. In: Handbook of Health Behavior Research 1: Personal and Social Determinants. Plenum Press, pp. 113–132.

Rostami, E., Karlsson, F., Gao, S., 2020. Requirements for computerized tools to design information security policies. Comput. Secur. 99, 102063. doi:10.1016/J.COSE.2020.102063.

Silic, M., Barlow, J.B., Back, A., 2017. A new perspective on neutralization and deterrence: predicting shadow IT usage. Inf. Manag. 54 (8), 1023–1037. doi:10.1016/j.im.2017.02.007.

Silic, M., Lowry, P.B., 2020. Using design-science based gamification to improve organizational security training and compliance. J. Manag. Inf. Syst. 37 (1), 129–161. doi:10.1080/07421222.2019.1705512.

Siponen, M., Adam Mahmood, M., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inf. Manag. 51 (2), 217–224. doi:10.1016/j.im.2013.08.006.

Siponen, M., Vance, A., 2010a. Neutralization: new Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Q. 34 (3), 487. doi:10.2307/25750688.

Siponen, M., Vance, A., 2010b. Neutralization: new Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Q. 34 (3), 487. doi:10.2307/25750688.

Siponen, M., Vance, A., 2014. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. Eur. J. Inf. Syst. 23 (3), 289–305. doi:10.1057/ejis.2012.59.

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. 22 (1), 42–75. doi:10.1108/IMCS-08-2012-0045.

Sykes, G.M., Matza, D., 1957. Techniques of neutralization: a theory of delinquency. Am. Sociol. Rev. 22 (6), 664. doi:10.2307/2089195.

Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T., Klepacki, B., 2020. Information security assessment in public administration. Comput. Secur. 90, 101709. doi:10.1016/j.cose.2019.101709.

Thompson, N., McGill, T.J., Wang, X., 2017. Security begins at home": determinants of home computer and mobile device security behavior. Comput. Secur. 70, 376–391. doi:10.1016/j.cose.2017.07.003.

Triandis, H.C., 1980. Values, attitudes, and interpersonal behavior. In: Nebraska Symposium on Motivation. Nebraska Symposium on Motivation, 27, pp. 195–259.

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. Comput. Secur. 59, 138–150. doi:10.1016/j.cose.2016.02.009.

Tsohou, A., Karyda, M., Kokolakis, S., 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Comput. Secur. 52, 128–141. doi:10.1016/j.cose.2015.04.006.

Vance, A., Lowry, P.B., Eggett, D., 2013. Using accountability to reduce access policy violations in information systems. J. Manag. Inf. Syst. 29 (4), 263–290. doi:10.2753/MIS0742-1222290410.

Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. 49 (3–4), 190–198. doi:10.1016/j.im.2012.04.002.

Vance, A., Siponen, M.T., Straub, D.W., 2020. Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Inf. Manag. 57 (4), 103212. doi:10.1016/j.im.2019.103212.

van Teijlingen, E., Hundley, V., 2002. The importance of pilot studies. Nursing Standard (Royal College of Nursing (Great Britain) : 1987) 16 (40), 33–36. doi:10.7748/NS2002.06.16.40.33.C3214.

Venkatesh, Morris, Davis, Davis, 2003. User Acceptance of Information Technology: toward a Unified View. MIS Q. 27 (3), 425. doi:10.2307/30036540.

Verison. (2020). *2020 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/dbir/?CMP=OOH_SMB_OTH_22222_MC_20200501_NA_NM20200079_00001.

Verkijika, S.F., 2018. Understanding smartphone security behaviors: an extension of the protection motivation theory with anticipated regret. Comput. Secur. 77, 860–870. doi:10.1016/j.cose.2018.03.008.

Verplanken, B., Aarts, H., Knippenberg, A.V, 1997. Habit, information acquisition, and the process of making travel mode choices. Eur. J. Soc. Psychol. 27 (5), 539–560. doi:10.1002/(SICI)1099-0992(199709/10)27:5⟨539::AID-EJSP831⟩3.0.CO;2-A.

Verplanken, B., Aarts, H., Van Knippenberg, A., Moonen, A., 1998. Habit versus planned behaviour: a field experiment. Br. J. Soc. Psychol. 37 (1), 111–128. doi:10.1111/j.2044-8309.1998.tb01160.x.

Wall, J.D., Palvia, P., Lowry, P.B., 2013. Control-Related Motivations and Information Security Policy Compliance: the Role of Autonomy and Efficacy. J. Inf. Privacy Secur. 9 (4), 52–79. doi:10.1080/15536548.2013.10845690.

Wang, X., Wang, C., Yi, T., Li, W., 2022. Understanding the deterrence effect of punishment for marine information security policies non-compliance. J. Ocean Eng. Sci. doi:10.1016/J.JOES.2022.06.001.

Weidman, J., Grossklags, J., 2019. Assessing the current state of information security policies in academic organizations. Inf. Comput. Secur. 28 (3), 423–444. doi:10.1108/ICS-12-2018-0142.

West, R., 2008. The psychology of security. Commun. ACM 51 (4), 34–40. doi:10.1145/1330311.1330320.

Witte, K., 1992. Putting the fear back into fear appeals: the extended parallel process model. Commun. Monogr. 59 (4), 329–349. doi:10.1080/03637759209376276.

Witte, K., 1996. Fear as motivator, fear as inhibitor. In: Handbook of Communication and Emotion. Elsevier, pp. 423–450. doi:10.1016/b978-012057770-5/50018-7.

Witte, K., Allen, M., 2000. A meta-analysis of fear appeals: implications for effective public health campaigns. Health Educ. Behav. 27 (5), 591–615. doi:10.1177/109019810002700506.

Woon, I., Tan, G.W., Low, R.T., 2005. A Protection Motivation Theory Approach to Home Wireless Security. In: Proceedings of the International Conference on Information Systems, ICIS 2005.

Wu, Y.L., Li, E.Y., Chang, W.L., 2016. Nurturing user creative performance in social media networks: an integration of habit of use with social capital and information exchange theories. Internet Res. 26 (4), 869–900. doi:10.1108/IntR-10-2014-0239.

Xu, J., Wang, X., Yan, L., 2021. The moderating effect of abusive supervision on information security policy compliance: evidence from the hospitality industry. Comput. Secur. 111, 102455. doi:10.1016/J.COSE.2021.102455.

Yazdanmehr, A., Wang, J., Yang, Z., 2020. Peers matter: the moderating role of social influence on information security policy compliance. Inf. Syst. J. 30 (5), 791–844. doi:10.1111/isj.12271.

Yoon, J., Vonortas, N.S., Han, S.W., 2020. Do-It-Yourself laboratories and attitude toward use: the effects of self-efficacy and the perception of security and privacy. Technol. Forecast. Soc. Change 159, 120192. doi:10.1016/J.TECHFORE.2020.120192.

Youn, S., Kim, S., 2019. Understanding ad avoidance on Facebook: antecedents and outcomes of psychological reactance. Comput. Hum. Behav. 98, 232–244. doi:10.1016/j.chb.2019.04.025.

Zandt, F., 2021. The Industries Most Affected by Ransomware November. Statista https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/.

Zhang, H., Zhang, K.Z.K., Lee, M.K.O., Feng, F., 2015. Brand loyalty in enterprise microblogs: influence of community commitment, IT habit, and participation. Inf. Technol. People 28 (2), 304–326. doi:10.1108/ITP-03-2014-0047.

Mansour Naser Alraja received the PhD degree in management information systems (2010). He is currently senior lecturer of Information systems and business analytics with Newcastle business school at Northumbria University. Alraja acted as professor of management information systems (MIS) with the Department of MIS, College of Commerce and Business Administration, Dhofar University, Oman. His research interests include information technology adoption, data analytics, information security, e-commerce, and the IoT. Alraja published many papers in many reputable journals that are indexed in Web of Science and have an impact factor. He has also served as a reviewer for many well-reputed conferences, including AOM, AIB, and IEEE conferences, as well as acting as a reviewer for several reputable journals such the Journal of Small Business & Entrepreneurship, IEEE Access, and Sage open. Alraja is College's Chief Accreditation Officer for AACSB. Moreover, since 2018, he has been appointed as the Chair for the Department of MIS. Alraja was a principle investigator for many funded projects. Currently, he is leading and mentoring two funded research project. Moreover, out of his research work he has many accepted and under review papers in very good journals (ABS 4, ABS 3 and ABS 2). Currently, he is guest editor in the International Journal of Emergency Services (ABS 2).

Usman Javed Butt received Bachelor of Computer Science (Hons) degree in 2003, MSc. Degree in Computer Networks and Systems Security from University of Greenwich in 2010 and now doing Ph.D. in Cyber Security from Brunel University. He is certified Ethical Hacker, Certified CISMP and Certified ISO27001 Practitioner. He is also trained on GCHQ CyberFirst initiative. Along with the academic experience, he also possesses commercial experience and have worked in the role of Systems Administrator and Network Engineer. He is currently Associated Dean & Head of Department Computing with Northumbria University London and hold External Examiner position for UK HEI. He has also authored number of book chapters on Ransomware, Cyberwarfare and Smart Homes Security and current research interests includes contemporary issues in cyber security.

Maysam F. Abbod received the Ph.D. degree in control engineering from The University of Sheffield, U.K., in 1992. He is currently a Reader of Electronic Systems with the Department of Electronic and Computer Engineering, Brunel University London, U.K. He has authored over 50 papers in journals, nine chapters in edited books, and over 50 papers in refereed conferences. His-current research interests include intelligent systems for modelling and optimization. He is a member of the IET (U.K.), and a Chartered Engineer (U.K.). He is serving as an Associate Editor of the Engineering Application of Artificial Intelligence (Elsevier).