Asia Pacific Journal of Information Systems
Vol. 33 No. 4 (December 2023), 863-898

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2023.33.4.863

Investigate the Roles of Sanctions, Psychological Capital, and Organizational Security Resources Factors in Information Security Policy Violation

Ayman Hasan Asfoor[a,*], Hairoladenan kasim[b], Aliza Binti Abdul Latif[c], Fiza Binti Abdul Rahim[d]

[a] *Department of Information Technology, Faculty of Computer Science, Jubail Industrial College, Jubail Industrial, KSA*
[b] *Department of Informatics, Faculty of Computer and Information Technology, Tanga Nasional University, Selangor, Malaysia*
[c] *Department of Informatics, Faculty of Computer and Information Technology, Tanga Nasional University, Selangor, Malaysia*
[d] *Penyelaras Program, Fakulti Teknologi and Informatik Raza, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*

ABSTRACT

Previous studies have shown that insiders pose risks to the security of organisations' secret information. Information security policy (ISP) intentional violation can jeopardise organisations. For years, ISP violations persist despite organisations' best attempts to tackle the problem through security, education, training and awareness (SETA) programs and technology solutions. Stopping hacking attempts e.g., phishing relies on personnel's behaviour. Therefore, it is crucial to consider employee behaviour when designing strategies to protect sensitive data. In this case, organisations should also focus on improving employee behaviour on security and creating positive security perceptions. This paper investigates the role of psychological capital (PsyCap), punishment and organisational security resources in influencing employee behaviour and ultimately reducing ISP violations. The model of the proposed study has been modified to investigate the connection between self-efficacy, resilience, optimism, hope, perceived sanction severity, perceived sanction certainty, security response effectiveness, security competence and ISP violation. The sample of the study includes 364 bank employees in Jordan who participated in a survey using a self-administered questionnaire. The findings show that the proposed approach acquired an acceptable fit with the data and 17 of 25 hypotheses were confirmed to be correct. Furthermore, the variables self-efficacy, resilience, security response efficacy, and protection motivation directly influence ISP violations, while perceived sanction severity and optimism indirectly influence ISP violations through protection motivation. Additionally, hope, perceived sanction certainty, and security skills have no effect on ISP infractions that are statistically significant. Finally, self-efficacy, resiliency, optimism, hope, perceived severity of sanctions, perceived certainty of sanctions, perceived effectiveness of security responses, and security competence have a substantial influence on protection motivation.

Keywords: Violation of Information Security Policy, Psychological Capital, Organizational Punishment, Organizational Security Resource

*Corresponding Author. E-mail: ayman_asfoor@yahoo.com

Ⅰ. Introduction

Information security policy (ISP) violations lead to many negative consequences for organisations including data loss or theft, computer attacks and privacy breaches (Ponemon Institute, 2016; 2017; Young and Ernst, 2011). According to a recent survey conducted by Ponemon Institute, approximately nine out of ten bank employees suffered at least one data breach (Ponemon Institute, 2020). Researchers concluded that the weakest link in securing ISP in businesses is often the end users themselves (Kolkowska et al., 2017; Merhi and Ahluwalia, 2014; Moody et al., 2018; Safa and Von Solms, 2016). Strong ISP policies in organisations are nonetheless impeded by the actions of their employees. Nearly 56% of those who participated in an IT security practitioner survey said that workers' unwillingness to comply with ISP regulations is the most significant obstacle in adopting effective security tactics in firms (Ponemon Institute, 2016). Additionally, PWC's "Global State of IS Survey in 2018" indicated that staff activities remain the primary source of organisations' ISP (PwC, 2017).

Because of this, the emphasis of ISP research has been on examining employee behaviour in the setting of ISP regulations being followed (Bulgurcu et al., 2010; Hwang and Cha, 2018; Merhi and Midha, 2012). When insiders purposefully violate ISP, security breaches will escalate as insiders fall victim to phishing efforts (Jalali et al., 2020). In the case where organisations have tried various security training, awareness programs and technological solutions to tackle the situation (Dada et al., 2021), the ISP violations however still persist (Farshadkhah et al., 2021; Jalali et al., 2020). A total of 43% data breaches were triggered by employees breaking IT standards (Trends Report, 2021) and 33% of IT-related mishaps were caused by employees not following standards (PwC, 2017).

The adoption of ISP rules necessitates behavioural changes in how users interact with IT systems, thus producing triggers for resistance to such changes (Kolkowska and Dhillon, 2013; Krazit, 2016; Merhi and Ahluwalia, 2015). The two most important factors that are responsible for employees breaking ISP policies are psychological reactance, which is the desire of employees to restore freedom, and security compliance stress, which occurs when employees are required to fulfil security controls and standards in a manner that requires additional effort, time and expertise.

Therefore, it is essential to have knowledge of the factors that motivate employees to adhere to the ISP rules. As there have been very few studies on employee intention to break ISP regulations, this research fills a key gap in the literature. Liang et al. (2012) posited that organisational punishment is often employed in firms as a deterrence to guarantee that the organisational norms are followed to the fullest degree.

General deterrence theory (GDT) is used as the basis of the punishment concept which also relies on three elements i.e., harshness, certainty and speed of punishment (Aurigemma and Mattson, 2017a). Punishment is determined based on a considerable portion of the ISP material in which the employee's intention to comply with the ISP rules are explored and better understood. According to the research of Bulgurcu et al. (2010), D'Arcy et al. (2009) and Straub (1990), increasing the severity of the penalties for non-compliance with ISP can lead to higher level of ISP compliance, as it discourages employees from violating the policy. Therefore, further research is needed to clarify how exactly punishment affects employees' compliance intention, given that GDT yields

a wide range of behavioural outputs and contradictory results (D'Arcy and Herath, 2011; Herath and Rao, 2009; Hwang and Cha, 2018; Trang and Brendel, 2019).

Additionally, tangible resources such as SETA programs (D'Arcy et al., 2009), facilitating conditions (Ng and Rahim, 2005; Moody et al., 2018, resources availability (Herath and Rao, 2009), top management participation (Hu et al., 2012) and rewards (Bulgurcu et al., 2010) primarily focus on positively encouraging the employees to meet the security demand. Li et al. (2018) argued that intangible resources such as employee psychological capital (PsyCap) have always been disregarded despite their importance.

Next, the theory of psychological capital, according to Seligman and Csikszentmihalyi (2000), should focus not on frightening people but rather on empowering them and assisting them in adapting to the changes in their environment. Employees are motivated to meet the security criteria when they are encouraged to focus on their distinctive qualities such as character traits, virtues, and skills. PsyCap encourages workers to concentrate on these aspects of themselves in order to enrich and better their lives. Kimolo (2013) argued that an organisation's connection with its employees is significantly impacted by the degree to which the organisation empowers its workforce. Alternatively, Choi and Lee (2014) and Nolzen (2018) discovered that employees with a robust sense of autonomy are more likely to have a favourable attitude towards their organisations and take care of the properties belonging to the business.

Meanwhile, this research argues that considering the PsyCap's relevance in motivating an individual's response to changes and behaviour (Burns et al., 2017), protection-motivated behaviours among employees may efficiently be encouraged by PsyCap. This is one of the primary findings of this study. As a result, the findings of this research provide PsyCap that can be used to either enhance or replace the deterrence idea. Additionally, security compliance stress may result from the additional work, time and knowledge required to comply with security controls and regulations (Pham, 2019). Although employees may find security restrictions to be inconvenient, laborious and difficult to follow, the resources that an organisation makes available to facilitate employee security compliance can reduce the demand placed on IT and indicate the success of organisational security measures (Duong, 2022). Users are more likely to implement security precautions when they understand the purpose of the programme, see the significance and use of security precautions and have confidence in their ability to properly implement these safeguards. Users are more willing to work together with a cyber-security system if they believe an organisation is doing its bit to ensure the system's integrity (Pham, 2019).

Furthermore, when employees have a favourable impression towards an organisation, they are more likely to go above and beyond in their usual tasks to protect the safety of the organisation (Bélanger et al., 2017; Burns et al., 2018; Hsu et al., 2015; Wahda et al., 2020). In this sense, Hsu et al. (2015), MacKenzie et al. (1998), Wahda et al. (2020) and Xu and Guo (2017) stated that the motivation for in-role behaviour (i.e., obeying the instructions of the system) is different from the motivation for extra-role behaviour (i.e., organisation's citizenship behaviour) because of their belief and positive attitude towards the organisation. Consequently, the concept has become a practical application in research, in which the organisation's protective motivation lowers the ISP violation. This research analyses the organisation's protection motive as a mediator between the components of punishment, including psycho-

logical capital, organisational resources security and the desire to violate (resistance). In other words, the protection motive acts as a mediator in the relationship between ISP resistance and organisational sanctions, psychological capital, organisational security resources and organisational security resources.

Ⅱ. Literature Review

2.1. Information and Cyber Security

Cyber security protects networks, computers, programmes, and data against attack, damage, and unauthorised access. Ajie, 2019 Organisations struggle to secure customer, HR, business email, calendar, payment, accounting, and other data (Herath and Rao, 2009; Jakobsson, 2016; Mishra et al., 2022; Zweighaft, 2017). Information security protects confidential, secure, and available information and information systems against unauthorised access, use, disclosure, interruption, modification, or destruction.

Thus, information security seeks to identify and explain internal and external dangers that might damage, alter, or steal these resources (Kumar, 2022). Information security is often defined in terms of many different types of desired security, such as accessibility, integrity, and privacy. Most firms, at some point in the road, will adopt procedures to protect sensitive customer data better. Determining which courses of action are the most prudent and should be taken may be challenging. Standardised practises have developed over the last several decades to aid businesses in making the best judgements possible, even though they must adapt to ever-changing environments. Such processes are often included in the more widespread “plan-do-check-act” framework.

Therefore, information security aims to catalogue and define the many external and internal risks that businesses face, including those that aim to pilfer, tamper with, or destroy such assets (Kumar 2022). Potential attacks from the outside are the greatest challenge that businesses face. Therefore, the goal of cybersecurity is to theorise and explain the numerous online hazards that may be launched by an external person to the firm and unlocked, either purposely or mistakenly, by an inside person (Saxena et al., 2020). Based on the research of others (Akter et al., 2022; Siddiqi et al., 2022). The field of cybersecurity studies the technical and psychological components of cyberattacks; this is done to understand cyberattacks and develop a variety of human and technological responses to combat them.

2.2. Human Behaviours

The technology component ensures the confidentiality of an organisation’s data (Warrington, 2017). The current investigation revealed that human behaviour is the primary barrier (Khando et al., 2021; Yeo and Banfield, 2022), for instance, Alavizadeh et al. (2022) and Valasvuo (2022) concluded that firewalls and comprehensive monitoring systems are insufficient to ensure an organisation’s information security resources are safe. User behaviour is crucial to information security because it determines protection success (Khando et al., 2021; Saridakis et al., 2016). Users’ technical and physical security measures protect information assets and systems. Thus, understanding how user behaviour affects information asset security against vulnerabilities like cyberattacks is vital. User behaviour is a major risk to information security (Alohali et al., 2018). As the weakest link in the security chain, individuals often create problems (Jaakko, 2019; Sprissler et al., 2018).

Human variables are complex and intertwined with organisational culture, perception and personality.

Thus, information security is difficult to solve. This research examines direct and indirect human variables that impair an organisation's information security. Human factors e.g., ISP violation, human errors and talent deficit can create huge security breaches, thus different methods should address them (Evans et al., 2019; Ncubukezit, 2022). Therefore, understanding security behaviour is crucial because organisations may fail to resist insider threats if they misread or neglect purposeful and unintentional security behaviour (Saxena et al., 2020). It also assists organisations to choose and execute cybersecurity initiatives.

Individuals can intentionally breach an organisation's information security policy and deny its existence (D'Arcy and Lowry, 2019; Guo and Yuan, 2012; Koohang et al., 2020). Reactance is the violation intention. The intention to violate has a higher valence than the intention to conform (Lowry and Moody, 2015; Moody et al., 2018). In other words, the intention to violate indicates rejection and taking actions to violate the policies (Alotaibi, 2017; D'Arcy and Teh, 2019), while the weak intention to comply comes from a lack of awareness or perceptions of the uselessness of these policies (Al-Omari et al., 2012; Alotaibi, 2017; Pahnila et al., 2007). The intention to violate is founded in criminology as an offensive behaviour that risks an organisation's assets and may lead to punishment (Velazquez Lucia, 2020). In the next part, we will look at the various earlier studies that discussed ISP violations.

2.3. Related Work

The following <Table 1> summarizes various studies in ISP violation that include Theories used, Factors, Research Methods, Sample Size and Finding.

In the next part, four perspectives on ISP violations are discussed and considered; these ideas may be used to study techniques to enhance ISP compliance, which is an important area of research.

2.4. Theory of Planned Behaviour (TPB)

The TPB states three elements define a person's behavioural goals i.e., perceived behavioural control, subjective norm and attitude (Zhang et al., 2019) which may properly anticipate and explain human intention and behaviour in diverse situations such as embracing new technology (Johnson and Johnson, 2017). TPB may also predict safe online behaviour (Burns and Roberts, 2013). The field of ISP has adapted and modified TPB to comprehend employee intention on compliance and violation better (Pham et al., 2017; D'Arcy and Lowry, 2019). ISP compliance studies show a strong intention-behaviour correlation (Lebek et al., 2014; Ma, 2021). In this sense, "attitude" refers to a person's broad notion of whether or not they would comply with the ISP based on their own experiences, degree of faith in the ISP and cultural norms (Hina et al., 2019). The "perceived control behaviour" of employee confidence in their capacity to follow their employers' ISP has been shown to predict their actual compliance (Aurigemma and Mattson, 2017b). Finally, "subjective norms" is defined as peers' influence on ISP compliance that strongly predicts the desire to comply (Anye, 2019).

TPB's sufficiency and relevance to compliance and violation are questionable (Sommestad and Hallberg, 2013). TPB was established to describe how users accept technology depending on their connection with it (Venkatesh and Davis, 2000; Teo et al., 2016). In contrast, the desire to comply with regulations is based on the user's view of being deprived of

<Table 1> Various studies in ISP violation

Authors	Theories used	Factors	Research Method	Sample Size	Findings
(Xu et al., 2021)	Neutralization	Abusive supervision, organization directed IS misuse, Metaphor of the ledger, Tenure with supervisor	The quantitative research design used	203 responses	Demonstrated that when individuals felt abusive supervision, they were more likely to utilize the ledger metaphor as a neutralizing tactic to justify their participation in IS abuse.
(Gwebu et al., 2020)	Theory of Neutralization	Ethical work climate, beliefs	Quantitative investigation. PLS is used to test hypotheses.	393 employees from different organizations	Employee disobedience is significantly influenced by neutralization and beliefs.
(Vance et al., 2020)	Theory of Neutralization, Deterrence Theory	Power distance, masculinity, individualism, moral beliefs	Design of a scenario-based quantitative study. PLS was used to analyze the results.	From 48 nations, there are 615 employees.	Deterrence is not affected by national culture. ISP noncompliance intention is influenced by shame, neutralization, and moral beliefs of personnel from various cultures
(Bansal et al., 2020)	Deterrence theory and RCT	Punishment LaHood, Reward likelihood, Moral Beliefs, Control variables, Neutralization Scenarios	Design of a quantitative research	a total of 120 females and 101 males took part in the research	Computer abuse behaviour is caused by procedural and organizational unfairness; punishment certainty minimizes the effect of injustice and the desire to misuse ISP.
(Lankton et al., 2019)	PMT	IT vision conflict	The quantitative research approach employed, as well as the PLS utilized for findings and analysis	There were a total of 275 correct answers.	The perceived severity and attitude regarding ISP noncompliance behavior are influenced by IT vision conflict.
(Merhi and Ahluwalia, 2019)	TPB, GDT	Descriptive norms, moral norms	Design of quantitative research.PLS is used in model testing.	There are 139 employees from ten different companies.	Employee norms are shaped by deterrence variables, which impact behavioral resistance to ISP compliance
(Kajtazi et al., 2018)	Prospect Theory, RCT, self-justification Theory, Approach Avoidance Theory	Sunk cost, self-justification, and risk perception	Quantitative research methods including pre- and post-testing. For findings and analysis, SEM was employed.	A total of 500 people from various companies participated.	Impediments to task completion have a substantial impact on employees' noncompliance with ISP

<Table 1> Various studies in ISP violation (Cont.)

Authors	Theories used	Factors	Research Method	Sample Size	Findings
(Aurigemma and Mattson, 2017b))	TPB, PMT, GDT	Previous punishment experience	The quantitative research approach was used. SEM based on covariants is utilized for research model testing.	239 workers from the United States Department of Defense took part in the exercise.	The rational use of punishments results in attitude-dependent ISB. The attitude formed as a result of disciplinary threats is influenced by past punishment experience
(Lowry et al., 2015)	control theory, psychological reactance	Threat to freedom from new ISP, Importance of ISP freedom, Reactance proneness, Reactance to new ISP, Intent to comply with new ISP	Quantitative methods were used in this study.	320 experts from a wide range of industries	The paper's primary purpose was to put fairness theory to the test in the context of reactive computer usage at the workplace, which it accomplished successfully. The authors, on the other hand, considered certainty, severity, and timeliness as possible counter-explanations. They were inconsequential in the perspective of the situation.
(Warkentin et al., 2011)	Deterrence, Organizational justice, Neutralization	Perception of organization injustice, Technique of Neutralization, Behavior intention to perpetrate computer abuse	The quantitative research approach used	A total of five situations were chosen from a probable scenario pool of 64 possibilities.	Increase in employee interactions and, as a result, a reduction in computer abuse.

personal freedom owing to the policies or the organisations (Lowry and Moody, 2015b; Burns et al., 2018). Despite TPB being successful and applicable to other fields including dieting, drug usage, exercise and marketing, it has not been widely employed to influence or regulate security behaviour (Sommestad and Hallberg, 2013). Due to these discrepancies, researchers have to create and alter new theories to explain compliance (Burns et al., 2018; Lu, 2018). Thus, theories like the protection motivation model (PMT) (Rogers, 1975; Maddux and Rogers, 1983), general deterrence theory (GDT) (Goode et al., 2015), fear appeals theory (FAT) (Janis, 1967; Janis and Feshbach, 1953) and social cognitive theory (SCT) (Bandura, 1977) are used to extend and replace the main constructs.

2.4.1. Protection Motivation (PM)

The adoption of PMT is the first change that has been recognised to be made to the TPB (Ifinedo, 2012). Similarly, researchers proposed incorporating PMT into TPB (Sommestad et al., 2015). According to the PMT, an individual's primary motivation for ISP compliance is to safeguard the organisation's information assets because of the individual's positive perception towards organisations (Burns et al., 2018). When a person has a positive attitude towards organisation, he or she is willing to perform extra-role behaviour to protect the organisation, which leads

to a stronger intention to comply with policies than just avoiding punishment (Bélanger, 2017; Burns, 2018; Hsu et al., 2015; Wahda et al., 2020), based on that it has been replaced the concept of PM from PMT in instead of attitudes construct in TPB.

2.5. General Deterrence Theory (GDT)

Deterrence has been restricted to the crime-preventative effects of legal punishment. Cesare Beccaria's 1764 deterrence theory emphasises "fear" as the punishment for being detected. The perceived harshness of punishment and the advantages of breaching rules are considered (Ritzman and Kahle-Piasecki 2016), thus, *"detectability refers to the offender's capability and/or desire to make this calculation is the perceptual process by which would-be offenders evaluate risks and rewards prior to offending and deterrence"* (Jacobs, 2010, p.417).

Rational Choice Theory (RCT) addresses the costs and benefits of different outcomes while making decisions (Burns and Roszkowska, 2016; Lu, 2018). D'Arcy and Herath (2011) argued that this notion was derived from the ISP literature and is the most extensively used theory in this domain (D'Arcy and Lowry, 2019). This theory suggests that breaking the ISP provides users greater freedom, time-saving, and job efficiency (Chen et al., 2020; Pham, 2019). There is a cost to pay for following the ISP, for example, upgrading passwords every month may increase employees' burden, therefore some can save time and effort by not following these standards (Fitzgerald, 2020; Jeon and Hovav, 2015).

The psychological cost of defying the ISP depends on the severity and certainty of the penalty and is translated into threats and worries for those who do not comply (Bulgurcu et al., 2010; Herath and Rao, 2009). Since employees may not value password changes, the benefits may not be immediately apparent. Thus, ISP researchers used deterrence theory from criminology to boost ISP advantages. In other words, breaching the rules may cost (Chen et al., 2018; Lowry et al., 2015), Wortley and Sidebottom (2017). In other words, fear is used to construct *"persuasive messages aimed to terrify people by depicting the awful things that will happen to them if they do not do what the message suggests"* (Tannenbaum et al., 2018; Witte, 1992, p.329). Fear and penalties prevent ISP infractions, according to academics.

People who see a violation being punished have a higher perception of penalty severity and likelihood than those who have not (Aurigemma and Mattson, 2017a). Fear is transformed into severity and certainty for employees (Chen et al., 2018; Shahbaznezhad, 2020). That is to say, individual perceptions of the certainty and severity of repercussions are significant in forecasting employee compliance and non-compliance (Aurigemma and Mattson, 2014; Johnston et al., 2015; Merhi and Ahluwalia, 2014; Wang and Xu, 2021). The theory of deterrence has several weaknesses in it. Assumptions about individual differences in response to threats and sanctions might lead to unintended consequences. Employees may not react positively to punishment if they do not believe it is fair and lawful (Kuhalampi, 2017). This highlights the importance of the deterrence theory but also suggests that it should not be used in isolation. Differences in character and the ways in which punishment is perceived can also play a role in how employees respond to punishment. It is important to consider these factors when implementing deterrence mechanisms to ensure that they are effective in promoting compliance with ISP.

Due to the differences in ethics and reason, people often misjudge the ISP and its repercussions. As has

been pointed out before (Alshare et al., 2018; Boss et al., 2009; D'Arcy et al., 2009; Posey et al., 2011), an abundance of monitoring systems might be seen as an invasion of privacy and as a factor in deciding the password. D'Arcy et al. (2009), Merhi and Ahluwalia (2019), and Hirtenlehner and Schulz (2021) argued that moral convictions modulate the association between punishment and violation. However, the relationship between severity perception and compliance intention was shown to be modified by personal norm alignment but not certainty perception (Li et al., 2010).

Employees are often frustrated by the lack of communication between them and management. The employment of negative consequences has the potential to deter inappropriate actions. On the other side, encouraging positive interactions between management and employees might assist in lessening disruptive actions. Thus, Burns et al. (2018) found that in many businesses, the major motivator of following ISP is avoiding penalty rather than their overriding goal to preserve the security of the organisation's information assets. When workers know they are being watched and that deviation is always a possibility, they may be more likely to follow the rules. This short-sighted strategy requires a rigid monitoring apparatus that constantly monitors employees.

2.6. Psychological Capital (PsyCap)

Deterrence relies on fear and punishment, which might have unintended repercussions (Kuhalampi, 2017). One of the primary causes of this condition is concerned about changes in the rules (Xu et al., 2020). This study presents positive psychology as a supplement to the deterrence theory. Positive psychology literature focuses on empowering and allowing individuals to accomplish and deal with environmental changes (Seligman and Csikszentmihalyi, 2000). Some individuals struggle to grasp new regulations, rules, and policies. The changes in rules and regulations may stress them out (Tavakoli, 2010).

Employee empowerment largely determines organisational relationship (Kimolo, 2013). The more empowered employees feel, the more likely they are to have a good attitude towards their organisation and safeguard its assets (Choi and Lee, 2014; Nolzen, 2018). Positive psychology was introduced by Seligman and Csikszentmihalyi (2000) which focuses on people's assets such as qualities, values and abilities to make their lives more meaningful and productive. Burns et al. (2017) found that psychological capital (PsyCap) influences insider risk appraisal and coping evaluation. Avey et al. (2008) and Burns et al. (2017) stated that PsyCap is the key to countering dysfunctional attitudes and behaviour necessary for organisational transformation and impacting workplace outcomes since it develops employees' protective motivated behaviour. The PsyCap's IS security efficacy hinges on its employees' psychological skills. An organisation may develop PsyCap at the subconstruct or higher-order factor level for example by fostering a conducive organisational climate (Luthans et at., 2008).

2.7. Organizational Security Resources

Users may need different resources to meet security concerns. Organisational security resources are physical, social and organisational characteristics of the job that help achieve work goals by decreasing job-related costs and boosting personal progress. Perceptions of the organisational security response efficacy and security skills motivate personnel to take precautionary measures (Pham, 2019).

The resources and security measure an organ-

isation provides to aid end users in complying with regular and non-routine security chores will lessen compliance burnout and boost security engagement. In the context of information security, "security engagement" is the degree to which end users actively develop their security knowledge and skills and demonstrate ethical loyalty to the company (Pham et al., 2016).

Ⅲ. Research Model and Hypothesis Development

3.1. Related Variables and Assumptions on General Deterrence Theory (GDT)

The GDT theory uses two constructs i.e., perceived severity and certainty. Perceived severity is the perceived degree of physical, psychological, social and economic pain to the violation (Trang and Brendel, 2019). This perspective and ISP have a significant link (Boss et al., 2015; Lee and Larsen, 2009; Vance and Siponen, 2012; Warkentin et al., 2016). One possible explanation is that people are less likely to abuse an information system if they have a good opinion of its defensive capabilities (Choi et al., 2013; D'Arcy et al., 2009). D'Arcy et al. (2009) and Aurigemma and Mattson (2017a) stated that employees comply with ISP because they fear punishments and their severity while D'Arcy and Herath (2011) and Trang and Brendel (2019) found that the GDT is a better predictor of non-compliant ISP conduct than compliant ISP conduct.

When someone commits a crime, they may feel "certain" about the consequences they will face if they get caught. Assuming the person knows the high probability that a serious punishment will be imposed on them, for that person, the added cost of the crime will reduce the likelihood that they will commit it (Burns, 2021; Paternoster and Simpson, 1993). The employees' impression of the severity of the consequences of breaking the rules is a major element in whether or not they will break the rules (Chen et al., 2020; Pratt et al., 2006). Examples of such a system include technical monitoring (e.g., analysis of logs), administrative measures (e.g., regular on-site audits), and social control through peers; all of which have been shown in the academic literature to be effective in reducing deviant behaviour (Johnston et al., 2015; Kuhalampi, 2017). Individuals working for businesses could be concerned about the possibility of receiving sanction (severity or certainty) from their employers if they fail to carry out their regular obligations in a secured and risk-free manner (Posey et al., 2013). It has been demonstrated that the application of extrinsic considerations in the form of sanctions can deter criminals from engaging in acts of espionage and protect the company (Xu et al., 2019). As a result, it is predicted that:

H1a: Perceived Sanction Severity will be significantly negatively related to the Intention to Violate ISP

H1b: Perceived Sanction Severity will be significantly positively related to the Protection Motivation

H2a: Perceived Sanction Certainty will be significantly negatively related to the Intention to Violate ISP

H2b: Perceived Sanction Certainty will be significantly positively related to the Protection Motivation

3.2. Related Variables and Assumptions on Psychological Capital (PsyCap)

PsyCap is categorised into four dimensions i.e., self-efficacy, hope, optimism, and resilience. Self-efficacy expresses people's beliefs when doing (Plamenova Djourova, 2018) and goes beyond actual

skills to execute activities. High self-efficacy may positively and negatively affect motivation. Self-confident people are motivated and tend to choose tough assignments to improve their performance and drive themselves to overcome challenges. It is predicted that:

H3a: Self-Efficacy will be significantly negatively related to the Intention to Violate ISP

H3b: Self-Efficacy will be significantly positively related to the Protection Motivation

Next, resilience is the ability to rebound from misfortune or depression. It helps individuals see difficult circumstances positively. Kim et al. (2019), Burns et al. (2017), and Rabenu and Yaniv (2017) showed that resilience has a reactional component that impacts people's orientations to life challenges. It is predicted that:

H4a: Resilience will be significantly negatively related to the Intention to Violate ISP

H4b: Resilience will be significantly positively related to the Protection Motivation

Optimism means thinking most of the time favourably. Optimists beat pessimists in job satisfaction, job performance and work happiness (Nguyen and Ngo, 2020). Optimism boosts productivity by increasing constant involvement (Sahoo et al., 2015). Dora and Azim (2019) observed that the positively-oriented psychological development scenario, which includes optimism, is a complete resource for coping with challenges and crucial situations. These variables reduce workplace deviance by encouraging good conduct (Altahat and Atan, 2018). Four PsyCap factors positively correlate with hope, optimism, resilience and peaceful work behaviour (Sarkar and Garg, 2020). Moreover, optimists are ambitious, driven and happy. They foster organisational commitment by stating that people are responsible for their own happiness and believe that positive thinking bring more good things (Bhowmik and Sahai, 2018). Optimism at work improves job performance, productivity, happiness, fulfilment and a sense of responsibility (Avey et al., 2010; Burns et al., 2017; Malik, 2013; Paolillo et al., 2015).

H5a: Optimism will be significantly negatively related to the Intention to Violate ISP

H5b: Optimism will be significantly positively related to the Protection Motivation

Hope drives purpose (Boutilier, 2020). Dora and Azim (2019) found that hope, a subfactor of PsyCap, is crucial in minimising workplace deviance. Hope also distinguishes good psychological progress. Mindfulness practitioners are happier, more confident and less ruled by negative emotions. Emotionally stable employees are less likely to let negative moods distract them and are better able to handle impulsive intentions that may result from daily negative moods, which reduces the impact that daily negative moods may have on service sabotage and other misconduct (Altahat and Atan, 2018). Hope stabilises employees' emotions, reduces distractions and allows them to make spontaneous judgments (Nolzen, 2018). Four PsyCap traits, hope, optimism, resilience and peaceful work behaviour are positively correlated (Sarkar and Garg, 2020). It is predicted:

H6a: Hope will be a significant positively related To Violate ISP

H6b: Hope will be a significant positively related to Protection Motivation

3.3. Related Variables and Assumptions on Organizational Security Resources

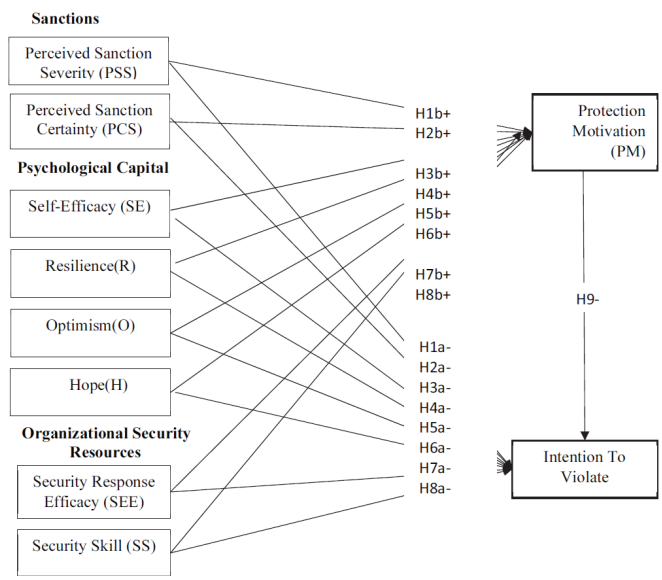
Security response efficacy assumes that adaptive reaction will be effective if an organisation is protected. Employees may feel that following business security policies will reduce security breaches. Research shows that employees' perceived efficacy in responding to security breaches affects their views about cybersecurity regulations and their inclinations to take cybersecurity measures (Li et al., 2022).

H7a: Security Response Efficacy will be significantly negatively related to the Intention to Violate ISP
H7b: Security Response Efficacy will be significantly positively related to the Protection Motivation

Insiders should be knowledgeable about technology and network prevention, as well as information and system management (ISM), to perform the protection step by identifying management and access control, setting data security protections consistent with the organisation's risk strategy and protecting organisational resources through maintenance and repair services (Senarak, 2021).

H8a: Security Skill will be significantly negatively related to the Intention to Violate ISP
H8b: Security Skill will be significantly positively related to the Protection Motivation

Protection motive refers to the behavioural intention of employees to protect their companies from security issues by complying with ISP (Moquin and Wakefield, 2016). Numerous studies based on TPB (Ajzen, 1991) have shown that motivation or behavioural intention strongly predicts actual behaviour in various contexts including in health (Ferrer et al., 2018), tourism (Wang et al., 2019), smartphone security (Verkijika, 2018), farming (Raza et al., 2019) and information security (Menard et al., 2018). In line with these results, this study proposes that em-



<Figure 1> Research Model.

ployees with high protective incentives are more likely to participate in the real action of ISP. Employees who are more dedicated to their organisations are more likely to follow security policies.

H9: Protection Motivation will be significantly negatively related to the Intention to Violate ISP

<Figure 1> shows the conceptual framework that underlies this investigation(Research Model).

Ⅳ. Research Methodology

4.1. Research Method and Data Collection

In this study, a survey was used as the research instrument to gather information and data. The survey questionnaire was based on measurement items from prior studies with some adjustments. A small-scale pilot study was conducted before the main survey, which was administered online to achieve a more equitable distribution of participants. Our studies utilized probability sampling techniques, including the simple random sample. The sample frame included employees from 10 different financial institutions in Jordan. Of the original 850 surveys, only 364 were processed, while 466 were returned and 102 were considered invalid.

4.2. Measurement

<Table 2> displays the items for each of the ten factors used in this study. The items were taken

<Table 2> Examining Results of Hypothesized Direct Effects of the Constructs in Structural Model

	Relationship	Std Beta	Std Deviation	t-value	p-value	95% LL-CI	95% UL-CI	f^2	VIF	Hypothesis Result
H1a$^-$	SE→IV_ISP	-.134*	.063	2.136	.033	-.260	-.008	.012	4.322	Supported
H2a$^-$	R→IV_ISP	-.090	.063	1.413	.158	-.210	.036	.006	4.276	Rejected
H3a$^-$	O→IV_ISP	-.100*	.047	2.137	.033	-.197	-.008	.009	3.346	Supported
H4a$^-$	H→IV_ISP	-.058	.075	0.777	.437	-.214	.077	.002	4.079	Rejected
H1b$^+$	SE→ PM	.112*	.047	2.407	.016	.024	.203	.015	4.260	Supported
H2b$^+$	R→ PM	.148**	.052	2.844	.005	.051	.255	.026	4.167	Supported
H3b$^+$	O→ PM	.096*	.038	2.542	.011	.022	.171	.014	3.300	Supported
H4b$^+$	H→ PM	.144**	.055	2.636	.009	.028	.245	.026	3.976	Supported
H5a$^-$	PSS→IV_ISP	-.075	.053	1.411	.159	-.182	.022	.005	3.391	Rejected
H6a$^-$	PSC→IV_ISP	.080	.061	1.304	.193	-.044	.203	.005	3.816	Rejected
H5b$^+$	PSS→ PM	.136**	.046	2.971	.003	.051	.234	.028	3.299	Supported
H6b$^+$	PSC→ PM	.102*	.046	2.223	.026	.009	.192	.014	3.765	Supported
H7a$^-$	SRE→IV_ISP	-.146*	.059	2.452	.014	-.258	-.020	.019	3.350	Supported
H8a$^-$	SS→IV_ISP	-.023	.063	0.369	.712	-.160	.088	.000	3.283	Rejected
H7b$^+$	SRE→ PM	.216***	.046	4.746	.000	.127	.298	.074	3.118	Supported
H8b$^+$	SS→ PM	.096*	.045	2.142	.032	.008	.187	.014	3.237	Supported
H9$^-$	PM→IV_ISP	-.361***	.083	4.356	.000	-.520	-.183	.078	4.956	Supported

Note: *p < 0.05, **p < 0.01, ***p < 0.001

directly from previously published publications using the same models or ideas. The modified instrument was also subjected to testing, validation and demonstration of its scales' internal consistency and reliability i.e., Cronbach's alpha and construct validity based on Alfons et al. (2022), A seven-point Likert scale was used to assign ratings to each topic, with 1 representing strong disagreement and 7 representing strong agreement.

4.3. Measurement Model Assessment

The level to which the observed variables are loaded onto their underlying concept is assessed by component analysis (Zhao et al., 2016). Cronbach's alpha and composite reliability were used to assess the model's internal consistency, convergent validity and discriminant accuracy. After completing the first three steps, the study moved on to the structural model analysis (hypotheses testing). The investigation determines whether or not there is a link between the variables observed and the latent components. The outer model or confirmatory factor analysis (CFA) was advised (Byrne, 2001) and used SmartPLS version 3.0.

The underlying latent variable is responsible for explaining the items' variance, which in turn demonstrates the items' reliability (Iacobucci, 2010), whereas the latent construct is responsible for illustrating the standardised outer loadings (absolute correlation), which must be more than 50% (Zhao et al., 2016). Cronbach's alpha was greater than the suggested value of 0.7, but the composite reliability was higher than the cut-off value of 0.70 (Cronbach, 1951; Nunnally and Bernstein, 1994). Every latent variable had an average variation extracted (AVE) value that was more than the suggested value of 0.5 (50%) which indicated that every construct could explain more than half of the variance associated with its measuring items on average (Fornell and Larcker, 1981).

<Appendix A> summarises the criteria for measuring how well a model fits the data. Results for discriminant validity are provided in <Appendix B>. The inter-correlations between the ten hypothesised latent constructs in the measurement model ranged between -0.781 and 0.823, which were below the threshold of 0.85 (Kline, 2005). Furthermore, as shown in <Appendix B>, the analysis indicated that the value of the off-diagonal elements was smaller than the value of the square root of AVE. Therefore, it confirms that each latent construct measurement was totally discriminating to each order (Fornell and Larcker, 1981; Hair et al., 2014) based on the Fornell-Larcker approach.

4.4. Data Analysis and Results

According to the findings of the study of the route coefficient, only 12 of the 17 hypotheses were significant. A p-value of less than 0.05 was required for statistical significance, and the expected sign orientations were present for all 12 hypotheses. However, the route coefficient values (β) varied from 0.081 to 0.332. There were found to be 12 significant direct connections (p-values less than 0.05 and t-values more than 1.96); in terms of the direct correlations that exist between the variables that influence the intention to violate, the findings showed that H1a (SE→IV_ISP, p = .033), H3a (O→IV_ISP, p = .033) and H7a (SRE→IV_ISP, p = .014), were statistically significant. Meanwhile, H2a (R→IV_ISP, p = .158), H4a (H→IV_ISP, p = .437), H5a (PSS→IV_ISP, p = .159), H6a (PSC→IV_ISP, p = .193) and H8a (SS→ IV_ISP, p = .712) were statistically insignificant. While the direct relationship between the determinants of PM indicated that H1b (SE→ PM, p =

.016), H2b (R→ PM, p = .005), H3b (O→ PM, p = .011) H4b (H→ PM, p = .009) H5b (PSS→ PM, p = 003), H6b (PSC→ PM, p = 026), H7b (SRE→ PM, p = .000), H8b (SS→ PM, p = .032) were statistically significant.

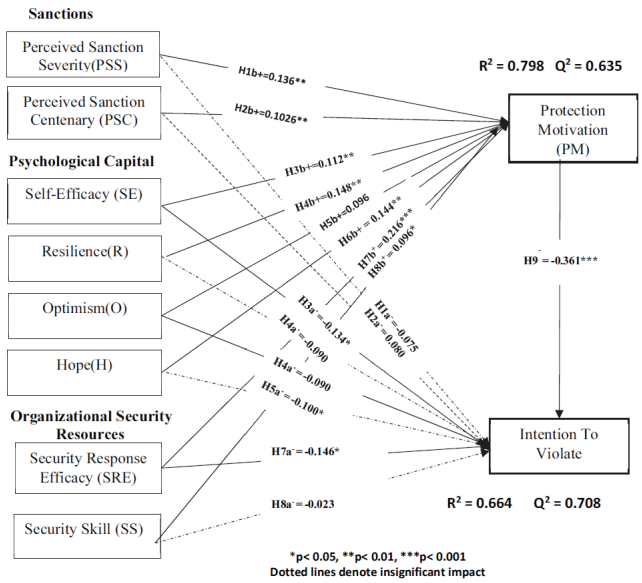
There was a substantial correlation between protection motivation and the intention to violate. The data supported the hypothesis which is the direct association between protection motivation and the intention to violate, H9 (PM (IV_ISP, p = .000) was statistically significant. The results are summed together in <Table 2> and <Figure 2>.

4.5. Path Coefficient Analyses

The path coefficient that Smart-PLS calculates is quite comparable to the standardised one calculated by multiple regression analysis. The bootstrapping method was used in order to estimate the t-statistics and the confidence intervals (Chin, 1998), given that PLS does not need distribution assumptions to be met. The use of path estimates or hypothetical connections was necessary in order to notice the important relationships included inside the inner route model. The regression coefficient (β) was used to explore each hypothetical route in the framework. In order to determine whether or not the assumptions of the structural model should be accepted (Alfons et al., 2022; Hayes, 2009), the value was put to the test using the PLS bootstrap procedure. The value of the path coefficient must be at least 0.1 for the model to consider a particular impact caused by the interactions between the variables (Wetzels et al., 2009)

4.6. Mediation Effect of Protection Motivation (Indirect)

Protective motivation has a significant and long-lasting effect on employee attitudes and actions, contributing to reducing ISP violations. For instance, employees might comply with the requirement of



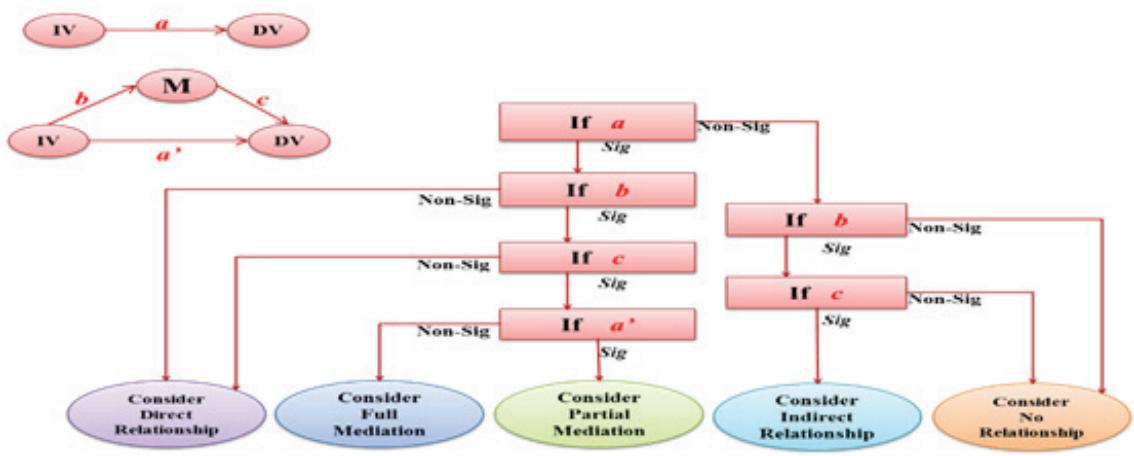
<Figure 2> Results of Structural Model Testing

the organisation's policy to not download any material from an email that seems suspicious as a kind of protective motivation. The mediation analysis was used to determine the mediation effects of Protection Motivation (PM) as a mediating variable on the effects of Self-Efficacy (SE), Resilience (R), Optimism (O), Hope (H), Perceived Sanction Severity (PSS), Perceived Sanction Certainty (PSC), Security Response Efficacy (SRE) and Security Skill (SS) as independent variables on the Intention to Violate ISP (IV_ISP) as dependent variable (i.e., H1c, H2c, H3c, H4c, H5c, H6c, H7c, H8a, H8b, H9). The indirect effects of the independent factors on the dependent variable via the mediating variable were also explored. Mediation statistics are correlational.

Mathieu and Taylor (2006) proposed a decision tree framework to investigate the covariance connections between an independent variable (IV), a mediating variable (M), and a dependent variable (DV). <Figure 3> illustrates this concept (Garver and Mentzer, 1999). In order to establish the mediation effect and its degree, the regression coefficients between IV, M and DV were analysed. The results indicated that Protection Motivation (PM) fully mediates the relationship between Resilience (R), Perceived Sanctions Severity (PSS) and Intention to Violate ISP (IV_ISP) [(H2c (R→PM→IV_ISP) H5c (PSS→PM→IV_ ISP)]. Protection Motivation (PM) also partially mediates the relationship between Self-Efficacy (SE), Optimism (O), Security Response Efficacy (SRE) and Intention to Violate ISP (IV_ISP)[H1c (SE→PM→IV_ISP), H3c (O→PM→IV_ISP) and H7c (SER→PM→IV_ISP)], were the remaining two hypotheses i.e., H4c (H→PM→IV_ISP) and H8c (SS→PM→IV_ISP) were statistically insignificant as shown in <Table 3>.

Ⅴ. Discussion

Several studies have demonstrated the significance of considering behavioural elements while tackling the issues and problems with ISP compliance in the workplace. Companies create ISP policies to direct and evaluate employee conduct to mitigate the damage that could result from ISP breaches occurring in the workplace. This study has examined the concept of opposition to ISP policy and its significance



<Figure 3> Decision tree for Evidence Supporting Different Intervening Effects (Source: Mathieu and Taylor, 2006)

<Table 3> Results of Examining Mediation Effect Hypotheses in Structural Model

	Independent Variable							
	Self-Efficacy (SE)	Resilience (R)	Optimism (O)	Hope (H)	Perceived Sanction Severity (PSS)	Perceived Sanction Certainty (PSC)	Security Response Efficacy (SRE)	Security Skill (SS)
Total Effect of IV on DV without M (path a)	-0.175**	-0.143*	-0.134**	-0.110	-0.125*	0.043	-0.224***	-0.058
Direct Effect of IV on DV with M (path a')	-0.134*	-0.090	-0.100*	-0.058	-0.075	0.080	-0.146*	-0.023
Indirect Effect of IV on DV through M (path bc)	-0.040*	-0.053*	-0.035*	-0.052*	-0.049*	-0.037*	-0.078**	-0.035*
Effect of IV on M (path b)	0.112*	0.148**	0.096*	0.144**	0.136**	0.102*	0.216***	0.096*
Effect of M on DV (path c)	-0.361***	-0.361***	-0.361***	-.361***	-0.361***	-0.361***	-0.361***	-0.361***
Mediation Type	**Partial**	**Full**	**Partial**	**N/A**	**Full**	**N/A**	**Partial**	**N/A**
Hypothesis Result	H1c	H2c	H3c	H4c	H5c	H6c	H7c	H8c

in ensuring sufficient compliance with ISP regulations. According to the research on resistance, factors that need people to alter their behaviour are a common source of this phenomenon. It is possible for the circumstances set by organisations for employees to comply with ISP policies to operate as stimulants that cause employees to act in a way that goes against the original intent.

This study proposes that the opposition is an underappreciated yet important aspect of ISP compliance studies. It also investigates the factors contributing to employee violation (resistance) of ISP regulations, including employees' psychological capital, organisational punishment, organisational security resources and protection motivation. PLS-SEM was used to test and validate a total of twenty-five (25) hypotheses that were generated. A total of 364 valid responses were obtained from employees working at ten different banks in Amman, Jordan, indicating that 17 of the 25 hypotheses were verified, while the other eight were invalid. It was found that ISP violations are affected directly by factors i.e., Self-Efficacy, Resilience, Security Response Efficacy, and Protection Motivation. Optimism and Perceived Sanction Severity, on the other hand, influence ISP violations indirectly by acting on Protection Motivation. In addition, Hope, Perceived Sanction Certainty and Security skills do not significantly impact ISP infractions. In addition, the research found that self-efficacy, resilience, optimism, hope, perceived severity of penalties, perceived certainty of sanctions, perceived effectiveness of security responses and security competence have substantial influences on protection motivation.

5.1. Theoretical Contribution

In sociological literature, certain personalities act differently and break regulations when presented with new freedom-limiting laws. This study used psychological reactance theory to understand employee's policy intention and attitude. In this study, the TPB, GDT, PsyCap and organisational security resources were integrated, which represents the study's most significant contribution. This study also proposes a comprehensive and interrelated conceptualisation

of security behavioural elements to improve personality characteristics in sociological literature to reduce ISP breaches. Thus, the model has the sufficient predictive capacity and predictive significance to explain the ISP violation protection organisation and its results. The first major improvement is a shift from the "Attitude" idea of TPB to the "PM" concept of PMT. This research was conducted in Jordan's organisational context, providing actual evidence of the factors that reduce ISP infractions in developing countries. This study addresses the absence of research on ISP infractions in developing country organisations. Given that the research model was highly influenced by literature from industrialised nations, the results demonstrated that certain characteristics are not vital to the financial organisation in Jordan. Furthermore, no studies have included protection motive as a mediator between psychological capital, punishment as deterrent, organisational security resources, and the intention to violate.

5.2. Practical Implications

From the perspective of self-efficacy, organisations should provide security skills training and knowledge-sharing activities for their employees to increase self-efficacy and their ability to deal with potential dangers, such as training employees on how to properly manage sensitive data and specialist training on the steps, tools and methods needed to reduce these risks and mitigate their effects. Employee training and chances to boost self-efficacy may enhance information security management. This will boost employee confidence in security-related talents. The important outcomes suggest businesses to develop an optimistic atmosphere in information security management, which increases employees' trust in their abilities to combat security-related challenges. Training and optimism boost employee optimism, which aids information security. Businesses can promote optimism around information security management to enhance employee trust in the organisations' ability to identify and resolve security issues. Training on security tactics and other information sharing will boost employee's security incident response confidence.

Organizations should foster resilience by giving employees many ways to achieve their goals. Participants are also asked to list their own assets and difficulties to help them build resilience. Dissatisfaction management training boosts information security employee resilience. Maintaining employees' resiliency is also important. The results of the perceived severity sanction have a significant with major effect on employees. According to the findings, organisations must make efforts to increase the harshness of penalties to enhance employee's adherence to information security regulations. Organisation's management must develop fear-appeal scenarios that tend to focus on the severity of consequences security measures such as creating a cautionary statement that includes management's intention and willingness to expose employees to new security technologies and encourage them to learn how to protect organisational IT assets because security response efficacy affects security behaviour. When management and skills development incentives are available, it is easier to follow the information system's security rules. Company leaders must make sure employees understand the risks of ISP violations.

VI. Limitations and Future Research

Despite its substantial contributions, it is necessary

to highlight the constraints imposed by this work. These limitations also provide opportunities for further research. To begin, the model offered in this study probably requires some alterations; nonetheless, considering the culture will surely result in the extension of the researcher's knowledge and will increase the comprehension of the factors that contribute to the resistivity of the ISP. Power distance is an example of one of the cultural elements at play here i.e., the variables that may cause individuals to react in various ways to government initiatives on ISP.

As a result, the potential moderating effect of power distance on the hypotheses discussed in this article may be the subject of an investigation in subsequent research. Second, researchers have emphasised keeping the study model as simple and practical as possible. Finally, what is contained in the ISP's rules might be the reason employees resist the ISP's regulations. On the other hand, this study aims to analyse the role of social norms in dealing with resistance from employees against ISP regulations. It is strongly recommended for more research to be carried out that analyse many parts of ISP guidelines and how these various aspects affect employee resistance.

<References>

[1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T.

[2] Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., and Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research. https://doi.org/10.1007/s10479-022-04844-8.

[3] Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., Welch, I., Camtepe, S. A., and Kim, D. D. (2022). A Survey on Cyber Situation-Awareness Systems: Framework, Techniques, and Insights. *ACM Computing Surveys, 55*(5), 1-35. https://doi.org/10.1145/3530809.

[4] Aldawood, H., and Skinner, G. (2020). Evaluating contemporary digital awareness programs for future application within the cyber security social engineering domain. *International Journal of Computer Applications*, *177*(31), 57-61. https://doi.org/10.5120/ijca2020919793

[5] Alfons, A., Ateş, N. Y., and Groenen, P. J. F. (2022). A robust bootstrap test for mediation analysis. *Organizational Research Methods*, *25*(3), 591-617. https://doi.org/10.1177/1094428121999096

[6] Alohali, M., Clarke, N., Li, F., and Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, *26*(3), 306-326. https://doi.org/10.1108/ICS-03-2018-0037

[7] Al-Omari, A., El-Gayar, O., and Deokar, A. (2012). Information security policy compliance: The role of information security awareness. *18th Americas Conference on Information Systems 2012, AMCIS 2012*, *2*(January), 1633-1640.

[8] Alotaibi, M. (2017). A Model for Monitoring End-User Security Policy Compliance. Plymouth University.

[9] Alshare, K., Lane, P. L., and Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information and Computer Security*, *26*(1), 91-108. https://doi.org/10.1108/ICS-09-2016-0073

[10] Altahat, S. M., and Atan, T. (2018). Role of healthy work environments in sustainability of goal achievement; ethical leadership, intention to

sabotage, and psychological capital in Jordanian universities. *Sustainability (Switzerland), 10*(10). https://doi.org/10.3390/su10103559.

[11] Anye, E. (2019). Factors affecting employee intentions to comply with password policies.

[12] Aurigemma, S., and Mattson, T. (2014). Do it OR ELSE! exploring the effectiveness of deterrence on employee compliance with information security policies. In *20th Americas Conference on Information Systems*, *AMCIS 2014* (pp. 1-12).

[13] Aurigemma, S., and Mattson, T. (2017a). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security*, *25*(4), 421-436. https://doi.org/10.1108/ICS-11-2016-0089

[14] Aurigemma, S., and Mattson, T. (2017b). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers and Security*, *66*, 218-234. https://doi.org/10.1016/j.cose.2017.02.006

[15] Avey, J. B., Luthans, F., Smith, R. M., and Palmer, N. F. (2010). Impact of positive psychological capital on employee well-being over time. *Journal of Occupational Health Psychology, 15*, 17-28.

[16] Avey, J. B., Wernsing, T. S., and Luthans, F. (2008). Can positive employees help positive organizational change? Impact of psychological capital and emotions on relevant attitudes and behaviors. *The journal of applied behavioral science*, 44(1), 48-70.

[17] Bandura, D. (1977). Control Document Cont rolled Documt. November 1997.

[18] Bansal, G., Muzatko, S., and Shin, S. I. (2020). Information system security policy noncompliance: The role of situation-specific ethical orientation. *Information Technology and People*, *30*(1), 1350-1917. https://doi.org/10.1108/ITP-03-2019-0109

[19] Beccaria. (1963). On crimes and punishments / trans. with an introduction, by Henry Paolucci. In Indianapolis, IN: Bobbs-Merrill. (Original work published 1764).

[20] Bélanger, F., Collignon, S., Enget, K., and Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management*, *54*(7), 887-901. https://doi.org/10.1016/j.im.2017.01.003

[21] Bennett, R. J., and Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology*, *85*(3), 349-360. https://doi.org/10.1037/0021-9010.85.3.349

[22] Bhaharin, S. H., Mokhtar, U. A., Sulaiman, R., and Yusof, M. M. (2019). Issues and trends in information security policy compliance. *International Conference on Research and Innovation in Information Systems*, *ICRIIS*, *December-2*. https://doi.org/10.1109/ICRIIS48246.2019.9073645

[23] Bhowmik, D., and Sahai, A. (2018). Optimism Promotes Organizational Commitment. *The International Journal of Indian Psychology, 6*(3), 35-50. https://doi.org/10.25215/0603.044.

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

[25] Bougaardt, G., and Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *The Electronic Journal Information Systems Evaluation*, *14*(2), 167-178.

[26] Boulhna, O. (2020). Applying psychological reactance theory to intercultural communication in the workplace: Dealing with technological change and tolerance for ambiguity. *ProQuest Dissertations and Theses*, *138*. Retrieved from https://search.proquest.com/dissertations-theses/applying-psychological-reactance-theory/docview/2457967884/se-2?accountid=49069

[27] Boutilier, R. (2020). Personality differences in hope and optimism on consideration of future consequences and goal motivation. *PsyArXiv Preprints*, *2*(September), 1-20. https://doi.org/10.

13140/RG.2.2.30907.03365

[28] Bradley, K. T., and Westlund, N. K. (2017). Risk perceptions and health behavior Rebecca. *J Neruosci Res*, *95*(6), 1336-1356. https://doi.org/10.1016/j.copsyc.2015.03.012.Risk

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

[30] Burns, A. J. (2021). Protecting organizational information assets: Exploring the influence of regulatory focus on rational choices. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, (pp. 5228-5237). https://doi.org/10.24251/hicss.2021.637

[31] Burns, A. J., Johnson, M. E., and Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24-39. https://doi.org/10.1080/10919392.2019.1552745

[32] Burns, A. J., Posey, C., Roberts, T. L., and Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. https://doi.org/10.1016/j.chb.2016.11.018

[33] Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2018). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. *Decision Sciences, 49*(6), 1187-1228. https://doi.org/10.1111/deci.12304.

[34] Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. *Decision Sciences*, *49*(6), 1187-1228. https://doi.org/10.1111/deci.12304

[35] Burns, S., and Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48-64. https://doi.org/10.1057/cpcs.2012.13

[36] Burns, T., and Roszkowska, E. (2016). Rational choice theory: Toward a psychological, social, and material contextualization of human choice behavior. *Theoretical Economics Letters*, *6*(02), 195-207. https://doi.org/10.4236/tel.2016.62022

[37] Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. *International Journal of Testing*, *1*(1), 55-86. https://doi.org/10.1207/s15327574ijt0101_4

[38] Çavuş, M., and Gökçen, A. (2015). Psychological Capital: Definition, Components and Effects. *British Journal of Education, Society and Behavioural Science*, *5*(3), 244-255. https://doi.org/10.9734/bjesbs/2015/12574

[39] Chen, L., Zhen, J., Dong, K., and Xie, Z. (2020). Effects of sanction on the mentality of information security policy compliance. *Revista Argentina de Clinica Psicologica*, *29*(1), 39-49. https://doi.org/10.24205/03276716.2020.6

[40] Chen, X., Wu, D., Chen, L., and Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information and Management*, *55*(8), 1049-1060. https://doi.org/10.1016/j.im.2018.05.011

[41] Chin, W. W. (1998). The partial least squares approach to structural equation modelling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research*, *295*(2), 295-336.

[42] Choi, M., Levy, Y., and Anat, H. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2013*, *December* (pp.

1-19). Retrieved from https://www.researchgate.net/publication/318710121%0Ahttps://nsuworks.nova.edu/gscis_facpres/98

[43] Choi, Y., and Lee, D. (2014). Psychological capital, Big Five traits, and employee outcomes. *Journal of Managerial Psychology*, *29*(2), 122-140. https://doi.org/10.1108/JMP-06-2012-0193

[44] Clubb, A. C., and Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, *28*(3), 336-355. https://doi.org/10.1080/1478601X.2015.1050590

[45] Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297-334.

[46] Cross, C., and Kelly, M. (2016). The problem of 'white noise': Examining current prevention approaches to online fraud. *Journal of Financial Crime, 23*(4), 806-818. https://doi.org/10.1108/JFC-12-2015-0069

[47] D'Arcy, J., and Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658. https://doi.org/10.1057/ejis.2011.23

[48] D'Arcy, J., and Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information and Management, 56*(7). https://doi.org/10.1016/j.im.2019.02.006.

[49] D'Arcy, J., and Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43-69. https://doi.org/10.1111/isj.12173

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

[51] Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and Security*, *20*(2), 165-172. https://doi.org/10.1016/S0167-4048(01)00209-7

[52] Dora, M., and Azim, A. (2019). Organizational Justice and Workplace Deviance Behavior: Psychological Capital as Mediator. *American International Journal of Humanities and Social Science, 5*(2), 2415-1424. www.cgrd.org.

[53] Duong, B. (2022). Security counterproductive behaviors employees' security counterproductive. Louisiana Tech University.

[54] Evans, M., He, Y., Maglaras, L., and Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers and Security*, *80*(May 2018), 74-89. https://doi.org/10.1016/j.cose.2018.09.002

[55] Farshadkhah, S., Van Slyke, C., and Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers and Security*, *100*, 102082. https://doi.org/10.1016/j.cose.2020.102082

[56] Ferrer, R. A., Klein, W. M. P., Avishai, A., Jones, K., Villegas, M., and Sheeran, P. (2018). When does risk perception predict protection motivation for health threats? A person-by-situation analysis. *PLoS ONE, 13*(3), 1-15. https://doi.org/10.1371/journal.pone.0191994.

[57] Fitzgerald, K. (2020). Walden University.

[58] Fornell, C., and Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research.*, *18*(1), 39-50.

[59] Frank, M., and Kohn, V. (2021). How to mitigate security-related stress: The role of psychological capital. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-January* (pp. 4538-4547). https://doi.org/10.24251/hicss.2021.550

[60] Garver, M.S and Mentzer, J.T (1999). Logistics research methods: employing structural equation modeling to test for construct validity. *Journal of*

business logistics, 20(1), 33.

[61] Ghazvini, A., and Shukur, Z. (2016). Awareness training transfer and information security content development for healthcare industry. *International Journal of Advanced Computer Science and Applications*, *7*(5), 361-370. https://doi.org/10.14569/ijacsa.2016.070549

[62] Goode, S., Lin, C., Tsai, J. C., and Jiang, J. J. (2015). Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. *Decision Support Systems*, *70*, 73-85. https://doi.org/10.1016/j.dss.2014.12.005

[63] Guo, K. H., and Yuan, Y. (2012). Information & Management The effects of multilevel sanctions on information security violations : A mediating model. *Information & Management, 49*(6), 320-326. https://doi.org/10.1016/j.im.2012.08.001.

[64] Gurung, A., Luo, X., and Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management and Computer Security*, *17*(3), 276-289. https://doi.org/10.1108/09685220910978112

[65] Gwebu, K. L., Wang, J., and Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, *30*(2), 220-269. https://doi.org/10.1111/isj.12257

[66] Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *June*, e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[67] Hair, J. J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. (2014). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks, california: SAGE Publications. http://fortune.com/2016/06/20/employees-computer-security/

[68] Hanus, B., and Wu, Y. "Andy." (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

[69] Hayes, A. F. (2009). Beyond Baron and Kenny: Statistical mediation analysis in the new millennium. *Communication Monographs*, *76*(4), 408-420. https://doi.org/10.1080/03637750903310360

[70] Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

[71] Higgins, G. E., and Lauterbach, C. (2004). Control balance theory and exploitation: an examination of contingencies. *Criminal Justice Studies*, *17*(3), 291-310. https://doi.org/10.1080/1478601042000281123

[72] Hina, S., Panneer Selvam, D. D. D., and Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security*, *87*, 101594. https://doi.org/10.1016/j.cose.2019.101594

[73] Hirtenlehner, H., and Schulz, S. (2021). Deterrence and the moral context: Is the impact of perceived sanction risk dependent on best friends' moral beliefs? *Criminal Justice Review*, *46*(1), 53-79. https://doi.org/10.1177/0734016820949641

[74] Höne, K., and Eloff, J. H. P. (2002). Information security policy: What do international information security standards say? *Computers and Security*, *21*(5), 402-409. https://doi.org/10.1016/S0167-4048(02)00504-7

[75] Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81. https://doi.org/10.1145/2063176.2063197

[76] Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300. https://doi.org/10.1287/isre.2015.0569

[77] Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing Employee Compliance with Information

Security Policies : The Critical Role of Top Management and Organizational Culture. *Decis. Sci, 43*, 615-660.

[78] Hwang, I., and Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293. https://doi.org/10.1016/j.chb.2017.12.022

[79] Hwang, I., Kim, K. T., and Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Inf. Rev*, *41*(1), 1-18.

[80] Iacobucci, D. (2010). Structural equations modeling: Fit Indices, sample size, and advanced topics. *Journal of Consumer Psychology*, *20*(1), 90-98. https://doi.org/10.1016/j.jcps.2009.09.003

[81] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

[82] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

[83] Inuwa, I., and Ononiwu, C. (2020). Motivations and prevention of malicious and criminal misuse of information systems in organizations: A systematic review. In *Proceedings of the 24th Pacific Asia Conference on Information Systems: Information Systems (IS) for the Future*, *PACIS 2020*.

[84] Jaakko, J. (2019). Is Human The Weakest Link In Information Security: A Systematic Literature Review. In Information security, Master's thesis (Vol. 204, Issue 1). http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=28111529&site=ehost-live.

[85] Jacobs, B. A. (2010). Deterrence and deterrability. *Criminology: An Interdisciplinary Journal, 48*(2), 417-441.

[86] Jakobsson, M. (2016). Understanding social engineering based scams. In springer.com (Vol. 49, Issue 0). https://doi.org/10.1007/978-1-4939-6457-4

[87] Jalali, M. S., Bruckes, M., Westmattelmann, D., and Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, *22*(1), 1-16. https://doi.org/10.2196/16775

[88] Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in experimental social psychology, 3*, 166-224.

[89] Janis, I. L., and Feshbach, S. (1953). Effects of fear-arousing communications. *The Journal of Abnormal and Social Psychology, 48*(1), 78-92. https://doi.org/10.1037/h0060732

[90] Jansen, J., and van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human Computer Studies*, *123*(January 2018), 40-55. https://doi.org/10.1016/j.ijhcs.2018.10.004

[91] Jeon, S., and Hovav, A. (2015). Empowerment or control: Reconsidering employee security policy compliance in terms of authorization. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2015-March* (pp. 3473-3482). https://doi.org/10.1109/HICSS.2015.418

[92] John, F. R. (2021). Influence of Psychological Capital on Employee Engagement and Explored the Mediating Role of Organizational Commitment. *European Journal of Molecular & Clinical Medicine*, 8(3), 3222-3231.

[93] Johnson, D. P., and Johnson, D. (2017). How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention. *Walden Dissertations and Doctoral Studies,* 4454.

[94] Johnston, A. C., Warkentin, M., and Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly: Management Information Systems*, *39*(1), 113-134.

https://doi.org/10.25300/MISQ/2015/39.1.06

[95] Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251. https://doi.org/10.1057/ejis.2015.15

[96] Junglas, I. A., Johnson, N. A., and Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387-402. https://doi.org/10.1057/ejis.2008.29

[97] Kajtazi, M., Cavusoglu, H., Benbasat, I., and Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information and Computer Security*, *26*(2), 39-57. https://doi.org/10.1108/ICS-09-2017-0066

[98] Khando, K., Gao, S., Islam, S. M., and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267.

[99] Kim, B., Lee, D. Y., and Kim, B. (2020). Deterrent effects of punishment and training on insider security threats: A field experiment on phishing attacks. *Behaviour and Information Technology*, *39*(11), 1156-1175. https://doi.org/10.1080/0144929X.2019.1653992

[100] Kim, M., Kim, A. C. H., Newman, J. I., Ferris, G. R., and Perrewé, P. L. (2019). The antecedents and consequences of positive organizational behavior: The role of psychological capital for promoting employee well-being in sport or ganizations. *Sport Management Review*, *22*(1), 108-125. https://doi.org/10.1016/j.smr.2018.04.003

[101] Kimolo, K. (2013). The relationship between employee empowerment practices and employee perfromance in regional development authorities in Kenya. In *Kimanzi Kimolo a Research Project Submitted in Partial Fulfillment of the Requirement for Degree of Masters of Business Admini* (Issue October).

[102] Kline, R. B. (2005). Principles and practice of structural equation modeling. New York, USA: The Guilford Press. https://doi.org/10.1038/156278a0.

[103] Kolkowska, E., and Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers and Security, 33*, 3-11. https://doi.org/10.1016/j.cose.2012.07.001

[104] Kolkowska, E., Karlsson, F., and Hedström, K. (2017). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information and Computer Security*, *26*(2), 39-57. https://doi.org/10.1108/ICS-09-2017-0066

[105] Koohang, A., Nord, J. H., Sandoval, Z. V., and Paliszkiewicz, J. (2020). Reliability, validity, and strength of a unified model for information security policy compliance. *Journal of Computer Information Systems*, *61*(2), 99-107. https://doi.org/10.1080/08874417.2020.1779151

[106] Krazit, T. (2016). Employees are the weakest link in computer security.

[107] Kuhalampi, M. (2017). Impact of Deterrence Theory Methods on Employees' Informati on Security Behavior. *PhD Thesis.*

[108] Kulyk, O., and Volkamer, M. (2018). Usability is not enough: Lessons learned from "human factors in security" research for verifiability. In *Third International Joint Conference on Electronic Voting (E-Vote-ID 2018)* (pp. 66-79).

[109] Kumar. (2022). Cyber Security Issues and Challenges - A Review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8*(11), 269-273. https://doi.org/10.32628/cseit228379

[110] Lankton, N. K., Stivason, C., and Gurung, A. (2019). Information protection behaviors: morality and organizational criticality. *Information and Computer Security*, *27*(3), 468-488. https://doi.org/10.1108/ICS-07-2018-0092

[111] Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085

[112] Li, Y., Zhang, N., and Pan, T. (2018). Understanding the roles of challenge security demands, psychological resources in information security policy noncompliance. *Proceedings of the 22nd Pacific Asia Conference on Information Systems - Opportunities and Challenges for the Digitized Society: Are We Ready?*, *PACIS 2018*.

[113] Liang, H., Xue, Y., and Wu, L. (2012). Ensuring employees' IT compliance: Carrot or stick? *Information System Resrach, June 24*(2), 201-497. https://doi.org/10.1287/isre.1120.0427

[114] Liu, C., Wang, N., and Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, *54*(28), 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

[115] Lowry, P. B., and Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433-463. https://doi.org/10.1111/isj.12043

[116] Lowry, P. B., Moody, G. D., and Chatterjee, S. (2017). Using the control balance theory to explain online social media deviance. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2017-Janua* (pp. 2253-2262). https://doi.org/10.24251/hicss.2017.272

[117] Lowry, P. B., Posey, C., Bennett, R. (Becky) J., and Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193-273. https://doi.org/10.1111/isj.12063

[118] Lu, Y. (2018). Cybersecurity Research: A Review of Current Research Topics. *Journal of Industrial Integration and Management, 03*(04), 1850014. https://doi.org/10.1142/s2424862218500148.

[119] Luo, X. R., and Zhdanov, D. (2016). Special issue introduction: A comprehensive perspective on information systems security — technical advances and behavioral issues. *Decision Support Systems*, *92*, 1-2. https://doi.org/10.1016/j.dss.2016.10.003

[120] Ma, X. (2021). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing and Management*, *59*(1), 1-14. https://doi.org/10.1016/j.ipm.2021.102744

[121] MacKenzie, S. B., Podsakoff, P. M., and Ahearne, M. (1998). Some possible antecedents and consequences of in-role and extra-role salesperson performance. *Journal of Marketing*, *62*(3), 87-98. https://doi.org/10.2307/1251745

[122] Maddux, J.E., and Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

[123] Malik, A. (2013). Efficacy, hope, optimism and resilience at workplace—positive organizational behavior. *International Journal of Scientific and Research Publications, 3*(10), 1-4.

[124] Marlina, L., Setyoningrum, N. G., Mulyani, Y. S., Permana, T. E., and Sumarni, R. (2021). Improving employees working discipline with punishment, reward, and implementation of standard operational procedures 1Lina. *Perwira International Journal of Economics and Business, 1*(1).

[125] Mathieu, J., and Taylor, S. (2006). Clarifying conditions and decision points for mediational type

inferences in Organizational Behavior. *Journal of Organizational Behavior, 27*, 1031-1056. https://doi.org/10.1002/job.406.

[126] Menard, P., Warkentin, M., and Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security*, *75*, 147-166. https://doi.org/10.1016/j.cose.2018.01.020

[127] Merhi, M. I., and Ahluwalia, P. (2014). The role of punishment and task dissonance in information security policies compliance. In *20th Americas Conference on Information Systems, AMCIS 2014, Straub 1990* (pp. 1-10).

[128] Merhi, M. I., and Ahluwalia, P. (2015). Top management can lower resistance toward information security compliance. In *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015, December 2015*.

[129] Merhi, M. I., and Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37-46. https://doi.org/10.1016/j.chb.2018.10.031

[130] Merhi, M. I., and Midha, V. (2012). The impact of training and social norms on information security compliance: A pilot study. *International Conference on Information Systems (ICIS)* (pp. 4183-4193).

[131] Mishra, A., Alzoubi, Y. I., Gill, A. Q., and Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors, 22*(2), 1-35. https://doi.org/10.3390/s22020538

[132] Moody, G. D., Siponen, M., and Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1), 285-311. https://doi.org/10.25300/MISQ/2018/138532018R.

[133] Moody, G., Siponen, M., and Pahnila, S. (2018). Toward a unified model of information security policy compliance. *Mis Quarterly*, *42*, 285-302. https://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=056bcc95-624f-437e-a25e-2f1b41f0bedf%40sdc-v-sessmgr03

[134] Moquin, R., and Wakefield, R. L. (2016). The roles of awareness, sanctions, and ethics in software compliance. *Journal of Computer Information Systems, 56*(3), 261-270. https://doi.org/10.1080/08874417.2016.1153922.

[135] Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139. https://doi.org/10.1057/ejis.2009.10

[136] Ncubukezit, T. (2022). Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. *International Conference on Cyber Warfare and Security, 17*(1), 395-403. https://doi.org/10.34190/iccws.17.1.51.

[137] Ng, B. Y., and Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security. 9th Pacific Asia Conference on Information Systems: I.T. and Value Creation, PACIS 2005, 234-247.

[138] Nguyen, H. M., and Ngo, T. T. (2020). Psychological Capital, Organizational Commitment and Job Performance : A Case in Vietnam. *The Journal of Asian Finance, Economics and Busines, 7*(5), 269-278. https://doi.org/10.13106/jafeb.2020.vol7.no5.269.

[139] Nolzen, N. (2018). The concept of psychological capital: A comprehensive review. *Management Review Quarterly*, *68*(3), 237-277. https://doi.org/10.1007/s11301-018-0138-6

[140] Nunnally, J., and Bernstein, I. (1994). Book Review: Psychometric theory. *Journal of Psychoeducational Assessment*, 275-280.

[141] Pahnila, S., Siponen, M., and Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. PACIS 2007 Proceedings.

[142] Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal*

of Computer Information Systems, *59*(3), 211-217. https://doi.org/10.1080/08874417.2019.1571459

[143] Paolillo, A., Platania, S., Magnano, P., and Ramaci, T. (2015). Organizational Justice, Optimism and Commitment to Change. *Procedia - Social and Behavioral Sciences*, *191*, 1697-1701. https://doi.org/10.1016/j.sbspro.2015.04.479.

[144] Paternoster, R., and Simpson, S. (1993). A Rational Choice Theory of Corporate Crime. In R. V. Clarke, & M. Felson (Eds.), Routine Activities and Rational Choice Theory (pp. 37-51). NJ: New Brunswick Transaction.

[145] Pham, H. C. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*, *46*, 96-107. https://doi.org/10.1016/j.jisa.2019.03.012

[146] Pham, H. C., Brennan, L., and Richardson, J. (2017). Review of behavioural theories in security compliance and research challenges. In *Proceedings of the Informing Science and Information Technology Education Conference* (pp. 65-76).

[147] Pham, H. C., El-Den, J., and Richardson, J. (2016). Stress-based security compliance model - An exploratory study. *Information and Computer Security*, *24*(4), 326-347. https://doi.org/10.1108/ICS-10-2014-0067

[148] Plamenova Djourova, N. (2018). Psychological capital: Underlying mechanisms, antecedents, and outcomes in the workplace. *Doctoral thesis*.

[149] Ponemon Institute. (2016). Sixth annual benchmark study on privacy & security of healthcare data. *Ponemon Institute*, 1-52.

[150] Ponemon Institute. (2017). 2016 Cost of cyber crime study and the risk of business innovation. *Ponemon Institute,* 1-36.

[151] Ponemon Institute. (2020). 2020 Cost of Insider Threats. Retrieved from https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

[152] Posey, C., Bennett, B., and Roberts, T. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, *10*(1), 21-45.

[153] Posey, C., Roberts, T. L., and Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214. https://doi.org/10.1080/07421222.2015.1138374

[154] Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly: Management Information Systems*, *37*(4), 1189-1210. https://doi.org/10.25300/MISQ/2013/37.4.09

[155] Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., and Madensen, T. D. (2006). The Empirical Status of Deterrence Theory: A Meta-Analysis. Taking Stock: The Status of Criminological Theory: Advances in Criminological Theory: Volume 15, 15(January), 367-396. https://doi.org/10.4324/9781315130620-14.

[156] PwC. (2017). UK organisations still failing to prepare effectively for cyber attacks. *UK Organisations Still Failing to Prepare Effectively for Cyber Attacks.* PWC: Cambridge, UK.

[157] Rabenu, E., and Yaniv, E. (2017). Psychological resources and strategies to cope with stress at work. International *Journal of Psychological Research*, *10*(2), 8-15. https://doi.org/10.21500/20112084.2698

[158] Raza, M. H., Abid, M., Yan, T., Ali Naqvi, S. A., Akhtar, S., and Faisal, M. (2019). Understanding farmers' intentions to adopt sustainable crop residue management practices: A structural equation modeling approach. In Journal of Cleaner

Production (Vol. 227). Elsevier B.V. https://doi.org/10.1016/j.jclepro.2019.04.244.

[159] Ritzman, M., and Kahle-Piasecki, L. (2016). What works: a systems approach to employee performance in strengthening information security. *Performance Improvement*, *55*(8), 17-22. https://doi.org/10.1002/pfi.21614

[160] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

[161] Safa, N. S., and Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451. https://doi.org/10.1016/j.chb.2015.12.037

[162] Safa, N. S., Solms, R. Von, and Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud and Security*, *2016*(2), 15-18. https://doi.org/10.1016/S1361-3723(16)30017-3

[163] Sahoo, B. C., Sia, S. K., Sahu, N., and Appu, A. V. (2015). Psychological Capital and Work Attitudes: A Conceptual Analysis. *Journal of Organization and Human Behaviour, 4*(2and3), 10-21. https://doi.org/10.21863/johb/2015.4.2and3.008.

[164] SANS. (2014). Information Security Policy Templates. Retrieved from http://www.sans.org/security-resources/policies/general

[165] Saridakis, G., Benson, V., Ezingeard, J. N., and Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330. https://doi.org/10.1016/j.techfore.2015.08.012

[166] Sarkar, A., and Garg, N. (2020). "Peaceful workplace" only a myth?: Examining the mediating role of psychological capital on spirituality and nonviolence behaviour at the workplace. *International Journal of Conflict Management, 31*(5), 709-728. https://doi.org/10.1108/IJCMA-11-2019-0217.

[167] Sawyer, B. D., Finomore, V. S., Funke, G. J., Matthews, G., Mancuso, V., Funke, M., Warm, J. S., and Hancock, P. A. (2016). Report date (dd-mm-yy) 2. report type 3. dates covered (from-to) cyber vigilance: The human factor 5a. contract number. 298(0704).

[168] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., and Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics (Switzerland)*, *9*(9), 1-29. https://doi.org/10.3390/electronics9091460

[169] Seligman, M. E., and Csikszentmihalyi, M. (2000). Positive psychology. An introduction. *The American Psychologist*, *55*(1), 5-14. https://doi.org/10.1037/0003-066X.55.1.5

[170] Senarak, C. (2021). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *Asian Journal of Shipping and Logistics, 37*(4), 345-360. https://doi.org/10.1016/j.ajsl.2021.10.002

[171] Shahbaznezhad, H., Kolini, F., and Rashidirad, M. (2020). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, 1-12. https://doi.org/10.1080/08874417.2020.1812134

[172] Siddiqi, M. A., Pak, W., and Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences (Switzerland), 12*(12). https://doi.org/10.3390/app12126042

[173] Siponen, M., Adam Mahmood, M., and Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

[174] Siponen, M., Soliman, W., and Vance, A. (2022). Common misunderstandings of deterrence

theory in information systems research and future research directions. *Data Base for Advances in Information Systems*, *53*(1), 25-60. https://doi.org/10.1145/3514097.3514101

[175] Sommestad, T., and Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. *IFIP Advances in Information and Communication Technology*, *405*, 257-271. https://doi.org/10.1007/978-3-642-39218-4_20

[176] Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42-75. https://doi.org/10.1108/IMCS-08-2012-0045

[177] Sommestad, T., Karlzén, H., and Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*. https://doi.org/10.1108/ICS-04-2014-0025

[178] Sprissler, E., Yan, Z., Robertson, T., Bordoff, S., Chen, Q., Yan, R., and Park, S. Y. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382. https://doi.org/10.1016/j.chb.2018.02.019.

[179] Stahl, B. C., Doherty, N. F., and Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal*, *22*(1), 77-94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

[180] Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

[181] Straub, D. W., and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly: Management Information Systems*, *22*(4), 441-464. https://doi.org/10.2307/249551

[182] Straub, D., and Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems*, *13*. https://doi.org/10.17705/1cais.01324

[183] Talib, Y. Y. A., and Dhillon, G. (2015). Employee ISP compliance intentions: An empirical test of empowerment. In *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015,* December 2015.

[184] Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., and Jacobs, S. (2018). Appealing to fear: A meta-analysis of fear appeal effectiveness and. *Psychol Bull.*, *141*(6), 1178-1204. https://doi.org/10.1037/a0039729. Appealing

[185] Tavakoli, M. (2010). A positive approach to stress, resistance, and organizational change. *Procedia - Social and Behavioral Sciences*, *5*, 1794-1798. https://doi.org/10.1016/j.sbspro.2010.07.366

[186] Teo, T., Zhou, M., and Noyes, J. (2016). Teachers and technology: Development of an extended theory of planned behavior. *Educational Technology Research and Development*, *64*(6), 1033-1052. https://doi.org/10.1007/s11423-016-9446-5

[187] Tittle, C. R. (1995). *Control Balance: Toward a General Theory of Deviance.* New York: ImprintRoutledge.

[188] Trang, S., and Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, *21*(6), 1265-1284. https://doi.org/10.1007/s10796-019-09956-4

[189] Tsohou, A., and Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People, 31*(5), 1047-1068.

[190] Valasvuo, S. (2022). Cybersecurity development

and business continuity plan for car dealership.

[191] Vance, A., and Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41. https://doi.org/10.4018/joeuc.2012010102.

[192] Vance, A., Fellow, S., and Siponen, M. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Science of the Total Environment*, 136126. https://doi.org/10.1016/j.scitotenv.2019.136126

[193] Velazquez, Lucia. (2020). Examining Information Security Policy Violations, Rationalization of Deviant Behaviors, and Preventive Strategies Dissertation Manuscript Submitted to Northcentral University School of Business in Partial Fulfillment of the Requirements for the Degree o (Issue July).

[194] Venkatesh, V., and Davis, F. D. (2000). Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, *46*(2), 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926

[195] Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security, 77*, 860-870. https://doi.org/10.1016/j.cose.2018.03.008.

[196] Wahda, Mursalim, Fauziah, and Asty. (2020). Extra-role behavior improvement model: Organizational learning culture, organizational trust, and organizational justice approach. *International Journal of Engineering Business Management*, *12*, 1-12. https://doi.org/10.1177/1847979020963774

[197] Wang, J., Li, Y., and Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396. https://doi.org/10.1287/isre.2016.0680

[198] Wang, J., Liu-Lastres, B., Ritchie, B. W., and Mills, D. J. (2019). Travellers' self-protections against health risks: An application of the full protection motivation theory. Annals of Tourism Research.

[199] Wang, X., and Xu, J. (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tourism Management, 84*. https://doi.org/10.1016/j.tourman.2021.104282

[200] Warkentin, M., Willison, R., Johnston, A. C., Warkentin, M., Willison, R., and Johnston, A. C. (2011). The role of perceptions of organizational injustice and techniques of neutralization in forming computer abuse intentions. In *Proceedings of the Seventeenth Americas Conference on Information Systems*, Detroit, Michigan.

[201] Warrington, C. (2017). A study of personality traits to explain employees' information security behavior among generational cohorts. *Journal of Organizational Psychology, 22*(3). https://doi.org/10.33423/jop.v22i3.5647

[202] Wetzels, M., Odekerken-Schröder, G., and Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly: Management Information Systems*, *33*(1), 177-196. https://doi.org/10.2307/20650284

[203] Williams, E. J., Hinds, J., and Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, *120*, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004

[204] Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

[205] Woon, I., Tan, G. W., and Low. (2005). A protection motivation theory approach to home wireless security. In *International Conference on Information Systems (ICIS)*. Retrieved from http://aisel.aisnet.org/icis2005

[206] Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: *A threat control*

model and empirical test. Computers in Human Behavior, 24(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005

[207] Wortley, R., and Sidebottom, A. (2017). Deterrence and rational choice theory. *The Encyclopedia of Juvenile Delinquency and Justice*, 1-6. https://doi.org/10.1002/9781118524275.ejdj0131

[208] Xu, F., Hsu, C., Luo, X., and Warkentin, M. (2021). Reactions to abusive supervision: Neutralization and IS misuse. *Journal of Computer Information Systems*, 1-10. https://doi.org/10.1080/08874417.2021.1887776 November, 36.

[209] Xu, J., Qureshi, A. R., Mohamed, Y., Dabagh, A., Kin, C. L., and Khan, R. (2021). Effective virtual interventions to enhance psychological capital: A mixed-methods systematic review. https://doi.org/10.31234/osf.io/dpjuy

[210] Xu, Z., and Guo, K. (2017). Organizational Citizenship Behavior regarding Information Security (OCB-S): Leadership Approach Perspective organizational citizenship behavior regarding security (OCB-S): leadership approach perspective. Journal of Computer Information Systems.

[211] Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?, *Computers in Human Behavior, 84,* 375-382. https://doi.org/10.1016/j.chb.2018.02.019

[212] Yazdanmehr, A., and Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36-46. https://doi.org/10.1016/j.dss.2016.09.009

[213] Yeo, L. H., and Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspectives in Health Information Management, 19(Spring).

[214] Young, and Ernst. (2011). Into the cloud, out of the fog; Global Information Security Survey. Into the Cloud, out of the Fog: Global Information Security Survey. Retrieved from https://www.Techzim.Co.Zw/Wp-Content/Uploads/Ey-Global-formationsecurity-Survey-Zimbabwe-Report-6-December-2011.Pdf

[215] Zhang, X., Liu, S., Wang, L., Zhang, Y., and Wang, J. (2019). Mobile health service adoption in China: Integration of theory of planned behavior, protection motivation theory and personal health differences. *Online Information Review*, *44*(1), 1-23. https://doi.org/10.1108/OIR-11-2016-0339

[216] Zhao, L., Yin, J., and Song, Y. (2016). An exploration of rumor combating behavior on social media in the context of social crises. *Computers in Human Behavior*, *58*, 25-36. https://doi.org/10.1016/j.chb.2015.11.054

[217] Zhen, J., Xie, Z., Dong, K., and Chen, L. (2021). Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour and Information Technology*, 41, 2342-2354. https://doi.org/10.1080/0144929X.2021.1921029

<Appendix A> Convergent Validity and Reliability for Measurements

Construct	Item / 1st Order Construct	Factor Loading	Average Variance Extracted (AVE)[a]	Composite Reliability (CR)[b]	Internal Reliability Cronbach Alpha
Protection Motivation (PM)	PM1	0.909	0.833	0.952	0.933
	PM2	0.908			
	PM3	0.906			
	PM4	0.927			
Intention to Violate ISP (IV_ISP)	IV_ISP1	0.943	0.883	0.968	0.956
	IV_ISP2	0.936			
	IV_ISP3	0.939			
	IV_ISP4	0.941			
Self-Efficacy (SE)	SE1	0.935	0.859	0.968	0.959
	SE2	0.926			
	SE3	0.919			
	SE4	0.935			
	SE5	0.921			
Resilience (R)	R1	0.930	0.869	0.964	0.950
	R2	0.922			
	R3	0.945			
	R4	0.931			
Optimism (O)	O1	0.918	0.851	0.958	0.942
	O2	0.926			
	O3	0.929			
	O4	0.918			
Hope (H)	H1	0.915	0.860	0.968	0.959
	H2	0.933			
	H3	0.930			
	H4	0.929			
	H5	0.927			
	H6	0.362[c]			
Perceived Sanction Severity (PSS)	PSS1	0.941	0.887	0.969	0.957
	PSS2	0.945			
	PSS3	0.944			
	PSS4	0.937			

<Appendix A> Convergent Validity and Reliability for Measurements (Cont.)

Construct	Item / 1st Order Construct	Factor Loading	Average Variance Extracted (AVE)[a]	Composite Reliability (CR)[b]	Internal Reliability Cronbach Alpha
Perceived Sanction Certainty (PSC)	PSC1	0.951	0.896	0.972	0.961
	PSC2	0.946			
	PSC3	0.946			
	PSC4	0.941			
Security Response Efficacy (SRE)	SRE1	0.939	0.890	0.970	0.959
	SRE2	0.941			
	SRE3	0.955			
	SRE4	0.939			
Security Skill (SS)	SS1	0.950	0.898	0.972	0.962
	SS2	0.946			
	SS3	0.952			
	SS4	0.943			

<Appendix B> Discriminant Validity

	H	IV_ISP	O	PM	PSC	PSS	R	SE	SRE
H	**0.927**								
IV_ISP	-0.699	**0.940**							
O	0.775	-0.693	**0.923**						
PM	0.780	-0.781	0.755	**0.912**					
PSC	0.655	-0.607	0.632	0.740	**0.946**				
PSS	0.607	-0.601	0.600	0.711	0.823	**0.942**			
R	0.811	-0.709	0.752	0.782	0.650	0.588	**0.932**		
SE	0.792	-0.722	0.782	0.784	0.665	0.636	0.819	**0.927**	
SRE	0.640	-0.684	0.641	0.766	0.639	0.600	0.670	0.656	**0.944**
SS	0.676	-0.656	0.658	0.747	0.642	0.604	0.643	0.682	0.789

Note: Diagonals represent the square root of the average variance extracted while the other entries represent the correlations; H = Hope; IV_ISP = Intention to Violate ISP; O = Optimism; PM = Protection Motivation; PSC = Perceived Sanction Certainty; PSS = Perceived Sanction Severity; R = Resilience; SE = Self-Efficacy; SRE = Security Response Efficacy; SS = Security Skill;

◆ About the Authors ◆

Ayman Hasan Asfoor

Ayman Hasan Asfoor is now pursuing a Doctor of Philosophy degree in computers and informatics at Universiti Tenaga Nasional-Malysia. He has already accomplished Master of Computer Science degrees at Capella University in the United States of America in 2004 and Al-Madinah International University in Malaysia in 2016. Additionally, he holds a Bachelor of Computer Science degree from Brock University in Canada in 2003. Since 2007, he has been appointed to the position of lecturer, and he is presently serving as a senior lecturer at Jubail Industrial College in Saudi Arabia. His areas of interest in the field of research include informatics, networking, and cybersecurity. his email is ayman asfoor@yahoo.com

HAIROLADENAN KASIM

HAIROLADENAN KASIM holds Doctor of Philosophy, Universiti Teknologi Mara, 2015; master's in information technology, University Technology Mara, 2007; and Bachelor Information Technology, Universiti Utara Malaysia, 1998. He is currently working as a lecturer at Universiti Tenaga Nasional (UNITEN). He can be contacted at email: hairol@uniten.edu.my.

Aliza Abdul Latif

Aliza Abdul Latif currently works at the Department of Information Systems, Universiti Tenaga Nasional (UNITEN). Aliza does research in Data Analytics, Information Management (Business Informatics) relating to Disaster Management. Her current project is Detecting Depression Using Data Analytics.

Fiza Abdul Rahim

Fiza Abdul Rahim holds Doctor of Philosophy, Universiti Teknologi Malaysia, 2016; Master of Computer Science (Information Security), Universiti Teknologi Malaysia, 2009; and Bachelor of Computer Science, Management and Science University (MSU), 2005. She has been a lecturer since 2012 and is currently a senior lecturer at Universiti Teknologi Malaysia. Her research interests include information privacy, cybersecurity, digital forensics, and informatics. She can be contacted at email: fiza.abdulrahim@utm.my.

Submitted: January 28, 2023; 1st Revision: May 11, 2023; 2nd Revision: August 13, 2023;
Accepted: August 16, 2023