Information & Computer Security

807

Beyond the direct impact of sanctions and subjective norms in cybersecurity

Sunitha Prabhu
School of Management and Marketing, Curtin University, Perth, Australia

David Kocsis
College of Business, University of Colorado Colorado Springs, Colorado Springs, Colorado, USA, and

Tek Yew Lew
School of Management and Marketing, Curtin University, Perth, Australia

Received 23 April 2025
Revised 20 May 2025
Accepted 23 May 2025

Abstract

Purpose – Cybersecurity literature has traditionally examined sanctions and subjective norms as separate drivers of security intentions. This may lead to an incomplete understanding of their interaction and explain some inconsistencies in prior research. This paper aims to investigate how the motivation for social approval and punishment avoidance interplay to shape insider cybersecurity intentions, specifically, examining whether subjective norms moderate the effect of sanctions.

Design/methodology/approach – An online survey with 120 employees focused on password reuse. Data were analysed using SPSS and AMOS, employing moderation analysis to test the interaction between formal sanctions and subjective norms.

Findings – Results reveal a dual role of subjective norms: a direct impact on intentions and a significant moderating effect on sanctions, potentially amplifying or diminishing their effectiveness depending on certain social conditions. This interaction offers a richer, more integrated understanding of insider behavioural motivation.

Practical implications – Organisations aiming for sustained cybersecurity compliance should prioritise cultivating strong social norms. Doing so may reduce reliance on punitive sanctions while achieving high levels of compliance.

Originality/value – While the theory of planned behaviour (TPB) and deterrence theory (DT) have been frequently used in cybersecurity literature, this study uniquely proposes that subjective norms, a key construct in TPB, may serve as a boundary condition for the effectiveness of formal sanctions, a central element of DT. Demonstrating this moderating effect, the study offers a novel perspective on integrating social and formal

The authors gratefully acknowledge Michael Elrick, Retd. Chief Security Officer at Wintec, New Zealand, for his valuable contribution and practical insights that informed the development of this manuscript. Authors also acknowledge Peter Dell, Curtin University, Australia, for his guidance during the development of this manuscript.

Information & Computer Security
Vol. 33 No. 5, 2025
pp. 807-825
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-04-2025-0148

control mechanisms, potentially clarifying inconsistent findings in existing literature. Subjective norms thus not only shape security intentions but also moderate the impact of sanctions.

Keywords Information security, Password reuse, Social influence, Subjective norms, Sanctions, Intention, Sanction effectiveness, Theory of planned behaviour, Deterrence theory

Paper type Research paper

1. Introduction

When employees interact with information systems (IS), security is rarely their primary concern (Prabhu and Thompson, 2022). Yet, secure practices are critical, as lapses can lead to serious consequences such as data breaches, malware infection and reputational damage (Aigbefo *et al.*, 2022). 82% of security breaches involve a human element, with non-malicious employee actions being seven times more likely to cause breaches than malicious actions (DBIR, 2024). Thus, effectively managing non-malicious employees' cybersecurity behaviours is vital for organisational cybersecurity.

To reduce employee-induced cybersecurity breaches, organisations commonly implement disciplinary controls, often in the form of sanctions. Sanctions can be both formal (i.e. imposed through official policies) or informal (operating through social influences and peer pressure) (Straub, 1990). In this context, Ajzen (1991) highlights the role of subjective norms, which reflect the perceived expectations from important others, such as peers and supervisors, in guiding individual behaviour. While the effectiveness of sanctions has yielded mixed results (see Section 2.1), research increasingly supports the importance of social influence in shaping compliance (Aigbefo *et al.*, 2022; Jaeger *et al.*, 2021; Johnston *et al.*, 2015). Notably, both sanctions and subjective norms operate through social mechanisms; sanctions rely on the threat of consequences, while subjective norms draw on the anticipation of social approval or disapproval.

Because both appeal to social influence, this overlap raises a critical question: Can subjective norms shape the effectiveness of sanctions, and vice versa? For example, when formal rules align with group norms, sanctions may carry greater weight through the imposed penalty and the added pressure of social disapproval. Supporting this, Wenzel (2004) found that in the context of tax compliance, social norms enhanced deterrence by introducing reputational consequences. Yet, this dynamic remains underexplored in organisational IS settings, particularly how perceived peer expectations might condition employee responses to formal sanctions. Insights on this interplay are essential for strengthening cybersecurity compliance through social alignment and enforcement.

While prior studies have examined subjective norms alongside sanctions (see Section 2.3), the nature of their relationship remains theoretically underdeveloped. It is still unclear whether subjective norms mediate, moderate, or merely independently influence security intentions. Specifically, the potential moderating role, where social expectations amplify or dampen the influence of sanctions, has not been empirically tested. To address this gap, the present study investigates whether subjective norms moderate the impact of sanctions on employees' cybersecurity intentions. Exploring this relationship offers an opportunity to integrate deterrence theory (DT) and the theory of planned behaviour (TPB), enhancing our understanding of how formal and informal forces jointly interact to shape cybersecurity intentions. The research question (RQ) is:

RQ. How do subjective norms and sanctions interact to influence employees' cybersecurity intentions?

This study contributes to cybersecurity literature by empirically testing the moderating role of subjective norms, suggesting that variations in subjective norms may explain some of the

inconsistencies in sanction effectiveness, offering a fresh perspective through which to evaluate deterrence, and offering practical insights for fostering a security-conscious culture.

The paper is structured as follows: Section 2 covers the theoretical background, followed by hypotheses in Section 3. Section 4 outlines the methodology, while Section 5 tests measurement items and hypotheses on password reuse, presenting the results and moderation analysis. Section 6 discusses the findings, contributions and limitations of the study. Finally, Section 7 concludes the study.

2. Theoretical background

This section outlines the key constructs underpinning the study, sanctions and subjective norms. It provides the foundation for understanding their direct roles and their potential interaction in influencing employees' cybersecurity compliance.

2.1 Sanctions

Deterrence theory posits that individuals are less likely to engage in undesirable behaviour, such as violating security protocols, when they perceive a high likelihood of detection and severe consequences (Straub, 1990). Sanctions, which encompass penalties or consequences imposed for rule violations, function as deterrents by leveraging individuals' drive to avoid punishments and maintain social acceptance (Merhi and Ahluwalia, 2019; Jaeger *et al.*, 2021; Straub, 1990; Merhi and Ahluwalia, 2024). These sanctions can be formal, such as fines or job termination, or informal, such as social disapproval or reputational harm (Straub, 1990). Sanctions have two key dimensions: *certainty* (the perceived likelihood of being caught) and *severity* (the perceived harshness of the punishment). Importantly, sanction effectiveness depends not only on their existence but on how individuals perceive them (Vance *et al.*, 2020).

The literature shows variation in defining sanction certainty. Straub (1990) originally described deterrent certainty as "*the risk of punishment*", while a subsequent study by Straub and Welke (1998) defined it as "*certainty of getting caught*" on p.5 and "*certainty of punishment*" on p.6. Subsequent studies diverge in their interpretations, while some define sanction certainty as detection certainty, referring to the likelihood of detecting deviant behaviour (Herath and Rao, 2009a, 2009b; Foth, 2016; Rajab and Eydgahi, 2019; Hooper and Blunt, 2020; Cheng *et al.*, 2013; Safa *et al.*, 2019; Johnston *et al.*, 2015). Others equate it to punishment certainty, indicating the probability of facing consequences for deviant behaviour (D'Arcy *et al.*, 2009; Johnston *et al.*, 2016; Brown, 2017; Moody *et al.*, 2018). Kuo *et al.* (2017) argue that detection certainty and punishment certainty should be treated as separate constructs. Merhi and Ahluwalia (2019) suggest that organisations prioritise detection through security measures like firewalls and monitoring systems, making detection certainty a stronger deterrent than punishment certainty (Merhi and Ahluwalia, 2019). In line with this perspective, this study interprets sanction certainty as the perceived likelihood that deviant behaviour will be detected.

While sanctions are often assumed to deter employees from engaging in security violations, empirical findings are inconsistent. Studies examining sanction certainty report conflicting results, while Herath and Rao (2009b), Foth (2016), Kuo *et al.* (2017) find significant deterrent effects, others, including Cheng *et al.* (2013), Johnston *et al.* (2015), Rajab and Eydgahi (2019), and Hooper and Blunt (2020) reported no significant influence. Similarly, research on sanction severity is inconclusive; whereas Johnston *et al.* (2016), Cheng *et al.* (2013) and D'Arcy *et al.* (2009) identify a deterrent effect, studies by Hooper and Blunt (2020), Moody *et al.* (2018), Johnston *et al.* (2015) and Hu *et al.* (2011) contradict these findings. Moreover, overly severe sanctions can backfire, leading to unintended consequences such as resentment, resistance or reduced intrinsic motivation (Herath and Rao, 2009a). This raises concerns about the optimal balance between deterrence and employee engagement in cybersecurity policies.

Beyond formal sanctions, informal sanctions, such as reputational consequences, have gained attention in cybersecurity research. Johnston *et al.* (2015) and Kuo *et al.* (2017) report that informal sanctions significantly influence cybersecurity intentions, whereas Moody *et al.* (2018) and Brown (2017) find no such effect. Interestingly, Johnston *et al.* (2015) observe that informal sanctions influence cybersecurity intentions even when formal sanctions do not, highlighting the need to explore the importance of social factors in compliance decisions. Given that sanctions are often implemented within social contexts, understanding their interaction with subjective norms is crucial for developing more effective cybersecurity interventions.

2.2 Subjective norms

Subjective norms refer to the perceived social pressure from relevant individuals regarding whether one should or should not engage in a particular behaviour and the individual's motivation to comply (Fishbein and Ajzen, 1975). This concept is central to various decision-making theories, including the Theory of Reasoned Action, Theory of Planned Behaviour, and the Social Identity Theory (Ajzen, 1985; Ajzen and Fishbein, 1970; Turner and Oakes, 1986). These theories suggest that individuals often align their behaviours with the expectations of their social and professional groups. Within an organisational context, the pressure to conform to the expectations of colleagues and managers can strengthen adherence to compliant behaviours (Johnston *et al.*, 2015; Hu *et al.*, 2011; Jaeger *et al.*, 2021; Herath and Rao, 2009a). For example, employees who perceive that their peers and supervisors value adherence to security protocols are more likely to comply to maintain their professional reputation and avoid social disapproval.

Although subjective norms and informal sanctions both involve social influence, they are distinct in their mechanisms. Subjective norms refer to an individual's perception of social expectations – the belief that relevant others expect them to behave in a certain way, influencing behaviour through anticipated approval or disapproval (Ajzen, 1985; Ajzen and Fishbein, 1970; Turner and Oakes, 1986). In contrast, informal sanctions are the actual social consequences that occur after a behaviour is performed, such as criticism or loss of reputation (Anderson *et al.*, 1977). For example, an employee might report phishing emails because they believe their manager would approve of it (no actual consequences yet, just perceived expectation – subjective norms) or because failing to do so could lead to colleagues blaming them if a breach occurs (real consequences – informal sanction). While both mechanisms drive compliance, subjective norms operate through perceived social pressure, whereas informal sanctions rely on real social feedback following one's actions.

Individuals regularly interact with their peers within an organisation, and their drive to be liked by these peers can significantly influence their behaviour (Johnston *et al.*, 2015). Norms can manifest through explicit reinforcement (e.g. managerial directives) and implicit cues (e.g. peer behaviours). Individuals rely on these social cues to guide their behaviour in security-related decisions (Vafaei-Zadeh *et al.*, 2019). When employees observe widespread security-conscious behaviour within their organisation, they are likely to adopt similar practices to meet the implicitly shared expectations. Conversely, a workplace culture that downplays security risks can normalise negligence, fostering poor security behaviours (Grimes and Marquardson, 2019). Research on subjective norms shows that the perception of approval from influential others is a powerful predictor of one's intention, e.g. Jaeger *et al.* (2021), Safa *et al.* (2019), and Kuo *et al.* (2017).

2.3 The interaction between subjective norms and sanctions

DT and TPB suggest that sanctions and subjective norms play crucial roles in shaping security behaviour. Sanctions primarily act as deterrents, while subjective norms encourage social conformity (Aigbefo *et al.*, 2022; Merhi and Ahluwalia, 2019, 2024). When aligned,

these factors can promote desired behaviours. For example, individuals who believe that others expect them to comply may respond more strongly to sanctions due to added social pressure. Moreover, when formal policies and social expectations align to discourage risky behaviours, like sharing passwords, individuals are more likely to comply.

Prior studies acknowledge the importance of considering subjective norms alongside sanctions. For instance, Herath and Rao (2009a) identify both as forms of extrinsic motivation, while Li *et al.* (2010) view them as perceived risks, and Johnston *et al.* (2015) classify them as formal and informal controls. Most research has examined their direct effects in parallel, e.g. Safa *et al.* (2019); Rajab and Eydgahi (2019); Moody *et al.* (2018); Foth (2016). Vance *et al.* (2020) suggest that sanctions and norms are closely intertwined. Merhi and Ahluwalia (2019, 2024) propose a sequential relationship, suggesting that subjective norms mediate the influence of sanctions by shaping perceptions of acceptable behaviour when sanctions are well-communicated. When working in tandem, these factors can create a robust compliance framework.

Despite emerging patterns in the literature indicating that these factors may interact, they remain empirically untested. This study proposes an interaction between subjective norms and sanctions, grounded in several indicators, including (1) patterns indicating interactions between these factors, (2) inconsistent empirical findings on sanctions and (3) the inferred but untested interaction between subjective norms and sanctions. These numbered issues are elaborated below.

First, several studies have examined the role of subjective norms and sanctions in shaping cybersecurity intentions. Table 1 summarises findings from IS research on these factors. When subjective norms have a substantial and significant impact on intentions ($\beta > 0.150$ and p-value < 0.05), sanctions [as a unified construct] and sanction certainty also tend to have significant impacts. In studies where subjective norms had a high β value, sanctions also exhibited a high β value. Conversely, when subjective norms lack significance ($\beta < 0.150$ or p-value ≥ 0.05), sanctions and sanction certainty also tend to be insignificant, except in the cases of Rajab and Eydgahi (2019) and Li *et al.* (2010). However, there is no clear pattern regarding subjective norms and the effects of sanction severity.

Table 1. Prior findings on subjective norms and sanctions impacting cybersecurity intentions

	Subjective norms		Sanction certainty		Sanction severity		Sanctions	
Source	β	p-value	β	p-value	β	p-value	β	p-value
Jaeger *et al.* (2021)	0.060	ns	0.070	ns	−0.040	ns		
Vance *et al.* (2020)	0.070	ns					0.010	ns
Rajab and Eydgahi (2019)	0.033	ns	−0.320	<0.010	−0.062	ns		
Safa *et al.* (2019) *	0.729	<0.001	0.722	<0.010	0.789	<0.010		
Kuo *et al.* (2017)	−0.410	<0.001	−0.220	<0.001	0.000	ns		
Foth (2016)	0.249	<0.001	0.194	<0.001	0.014	ns		
Cheng *et al.* (2013)∼	−0.139	<0.05	0.027	ns	−0.311	<0.001		
D'Arcy and Devaraj (2012)	−0.240	<0.001					−0.170	<0.001
Siponen and Vance (2010)	0.450	<0.001					0.090	<0.001
Li *et al.* (2010)	−0.090	ns	0.240	<0.001	−0.120	ns		
Herath and Rao (2009b)	0.313	<0.001	0.155	<0.001	−0.139	<0.001		
Liao *et al.* (2009) *∼	0.127	<0.05	0.026	ns	0.109	ns		

Note(s): ** DVattitude, ∼ low support ($p < 0.05$ but $\beta < 0.15$), ns ($p \geq 0.05$ or β in the wrong direction)*
Source(s): Authors' own work

Notably, sanctions appear to be more effective in environments with strong subjective norms, as norms can amplify the perceived legitimacy and fairness of sanctions. Conversely, sanctions appear to have a diminished effect with weak or contradictory norms, which may lead employees to view sanctions as arbitrary or unfair. This suggests a potential interdependent relationship between subjective norms and sanctions in shaping intentions. Uncovering whether these factors truly interact or if the patterns observed in Table 1 lack relevance is pivotal for deepening theoretical insights and informing practical interventions.

Second, the effectiveness of sanctions has yielded inconsistent results; Table 1 highlights this variability. Moreover, some studies, e.g. Herath and Rao (2009a), observed that severe sanctions can backfire, leading to counterproductive behaviour. Notably, the presence of a construct can either complement, contradict or at times, have no effect on the other (Merhi and Ahluwalia, 2024). Studies, such as Hooper and Blunt (2020) and Hu *et al.* (2011) have not examined subjective norms in their model. Given that employees are more likely to follow security protocols not just to avoid penalties but also to gain favourable recognition from their peers and managers (Merhi and Ahluwalia, 2019), it is crucial to examine sanctions and subjective norms together.

Third, the literature has often inferred that strong subjective norms can amplify the effect of sanctions, but this has not been empirically tested. For example, Herath and Rao (2009a) argue that when integrated with DT, subjective norms can enhance the perceived severity and certainty of sanctions. However, they only examine the direct effects on intention, not the interaction between norms and sanctions. Similarly, Vance *et al.* (2020) propose that when influential peers promote security protocols, employees internalise these norms, making them less likely to engage in risky behaviour; strong subjective norms may also lead employees to perceive the consequences of non-compliance as more severe. Likewise, Kuo *et al.* (2017) suggest that in environments with a strong culture of compliance, individuals believe that peers will notice and report non-compliance. This heightened sense of surveillance acts as an additional deterrent, as individuals seek to align with peer expectations. Conversely, when exemplary peers are lax about security protocols, employees may be less likely to comply, necessitating stronger sanctions (Herath and Rao, 2009a; Vance *et al.*, 2020). While these studies imply a moderating effect of subjective norms on sanctions, this interaction has not been tested.

Human behaviour is influenced by multiple interacting factors rather than isolated variables. Examining subjective norms and sanctions separately overlooks these complexities. Although prior research has tested their individual effects on compliance intentions (see Table 1), no studies have explored their interaction. Without empirical evidence, assumptions about their combined influence remain theoretical, limiting practical applicability and potentially leading to ineffective security measures. For example, harsh sanctions without supportive subjective norms may foster resentment (Herath and Rao, 2009a), while strong norms without enforceable sanctions may lead to weak adherence, as social pressure alone may not sufficiently deter non-compliance (Prabhu and Dell, 2025). Evidence from tax compliance suggests that combining norms with sanctions enhances deterrence (Wenzel, 2004). Testing this interaction in organisational cybersecurity could validate widely held assumptions and inform more balanced, effective compliance strategies.

3. Research model

This section outlines the theoretical framework and rationale for each hypothesis in the research model (Figure 1). While prior studies have tested the direct effects of sanctions and subjective norms on security intention (*H1*, *H2*), the moderating relationship between them (*H3*) remains empirically untested. The model was controlled for age and work experience.

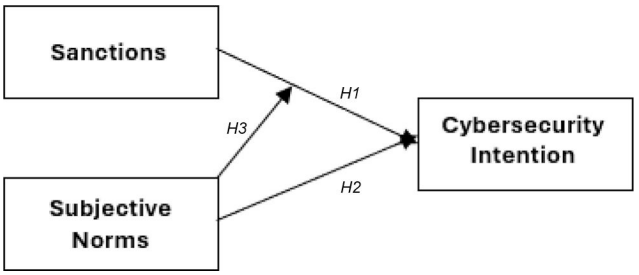


Figure 1. Research model
Source: Authors' own work

DT suggests that the perceived threat of sanctions influences individual behaviours, particularly in the context of computer abuse (Straub, 1990). Sanctions have been applied to deter misuse intentions (D'Arcy *et al.*, 2009), IS security policy violation intentions (Hu *et al.*, 2011), IS violation intentions (Cheng *et al.*, 2013), and to promote IS-compliant behaviour (Herath and Rao, 2009a). When individuals perceive that the punishment will impact them, their intention to comply with the desired behaviour is likely to increase. While sanctions may not deter all individuals, research has empirically shown that they can effectively prevent non-malicious employees from engaging in rule-breaking behaviour (Straub, 1990). In the context of this study, sanctions for reusing passwords could motivate employees to adopt unique passwords. Thus, the hypothesis:

H1. Sanctions positively influence employees' cybersecurity intentions.

According to TPB, subjective norms positively impact individuals' intentions (Ajzen, 1991). An individual's drive to conform to others, even at the risk of doing the wrong thing, may outweigh the inclination to contradict others in doing the right thing, particularly when those others hold significant influence (Vedadi *et al.*, 2021). Influential figures within the work environment serve as role models, setting the standard for acceptable behaviours (Prabhu and Thompson, 2022). Employees are more likely to avoid behaviours, such as password reuse, if they evaluate these behaviours negatively and believe that influential others disapprove of such actions (Vafaei-Zadeh *et al.*, 2019; Syed *et al.*, 2021). Several studies, including Jaeger *et al.* (2021), Safa *et al.* (2019), and Kuo *et al.* (2017), have found that subjective norms significantly influence behavioural intentions. In the context of this study, when role-model colleagues value and insist on using unique passwords, it could motivate employees to adopt similar practices. Based on the tenets of TPB and the literature above, the hypothesis:

H2. Subjective norms positively influence employees' cybersecurity intentions.

From a deterrence perspective, the subjective value of an individual's anticipated consequences is influenced by formal sanctions and social disapproval (Straub, 1990). In studies showing significant subjective norms, sanctions are also typically significant (see Table 1). This suggests that when employees believe their peers disapprove of security breaches and expect strict adherence to security protocols, their drive to conform to these social expectations can significantly enhance the impact of sanctions. Specifically, strong social expectations amplify the deterrent effect of sanctions, while weak social expectations diminish their effectiveness. Sanctions can motivate compliance not only by deterring violations but also by appealing to an individual's drive to avoid social disapproval

(Merhi and Ahluwalia, 2019; Jaeger *et al.*, 2021). The collective impact of subjective norms and sanctions, and their interaction, remains underexplored.

This study addresses this gap by exploring whether the combined influence of these factors is key to explaining inconsistent findings in past research on the efficacy of sanctions. Therefore, this study proposes that subjective norms moderate the relationship between sanctions and cybersecurity intentions. Specifically, when employees believe that influential peers view sanctions as legitimate and value compliance, they are more likely to perceive sanctions as meaningful. In such contexts, the motivation to comply stems not only from the fear of formal consequences but also by a drive to maintain social approval and avoid peer disapproval. Conversely, when influential peers disregard sanctions, employees may be less influenced by them. Hence, the hypothesis:

H3. Subjective norms positively moderate the influence of sanctions on employees' cybersecurity intentions.

4. Methodology

To examine the RQ, this study focuses on password reuse, a prevalent yet risky insider security behaviour. Despite advancements in authentication methods, passwords remain the dominant form of authentication (Davis *et al.*, 2022; Stainbrook and Caporusso, 2018). As individuals manage multiple accounts, reusing passwords has become widespread, increasing security risks. Wang *et al.* (2018) found that 38% of 28.8 million users reused passwords across services, and 21% made minor variations. Additionally, DBIR (2022) reports that 80% of security breaches involve stolen or weak passwords, with over one million passwords compromised weekly. Given that lapses with passwords can expose organisations to major security risks, understanding what drives such behaviours is critical to improving cybersecurity compliance.

Given the nature of the research, where security concerns may prevent organisations from sharing sensitive data or allowing direct observation, a survey method was deemed the most appropriate. This approach enables the collection of self-reported behaviour, which is crucial for understanding individual intentions in cybersecurity contexts, as supported by Johnston *et al.* (2015); Vance *et al.* (2020); Safa *et al.* (2019), among others. The survey method aligns with the research objectives of examining subjective norms and sanctions, as it allows for the direct measurement of individuals' perceptions of social influence and sanctions regarding password reuse.

The survey was developed using the platform Qualtrics and distributed through Prolific. SPSS 29 was used for descriptive statistics, exploratory factor analysis (EFA), reliability tests, and initial validity tests. AMOS 29 was used for confirmatory factor analysis, validity tests, and structural equation modelling, providing the necessary rigour for testing the hypothesised relationships. This approach supports the research objectives by providing robust, quantifiable insights into the dynamics between sanctions, subjective norms and cybersecurity intentions.

This study measured employees' cybersecurity intention (CSI), their perception of sanctions (SAN) through sanction certainty and severity, and subjective norms (SN). Each variable was assessed using five items. To ensure measurement reliability and validity, items were adapted from Herath and Rao (2009b) and (Vedadi *et al.*, 2021). Some items were reworded to address the behaviour of password reuse. However, certain items were removed during the validation processes, as detailed in Section 5.2. The full list of measurement items is in Appendix.

Section 1 of the survey obtained participants' consent and outlined the study's objectives. Participants were assured of confidentiality and informed that participation was voluntary, with the option to withdraw at any time. Participants had to meet two eligibility criteria:

(1) they must be employed; and

(2) they must use computers in their daily work.

While the study focuses on password reuse, the second criterion reflects the broader project on general security behaviours. Those who did not meet the criteria were informed and directed to the end of the survey.

In the next section, participants answered construct-related questions in a matrix format using a 7-point Likert scale, ranging from strongly agree to strongly disagree. To minimise order effects, survey items were randomised. To help mitigate social desirability bias, the survey was conducted anonymously and online, encouraging honest and uninfluenced responses (Bagozzi, 2011). The final section of the survey collected demographic details. Ethics approval for the study was granted by the university's Ethics Office.

An a-priori power analysis using G*Power 3.1 indicated that a sample size of 111 would be sufficient to detect an effect size of 0.3, with a power of 0.8 and a significance of 0.05. Data was collected from 162 UK participants. Responses were manually reviewed, and those completed in less than half the estimated time were excluded. Further quality checks removed responses with over 50% unknown data or a standard deviation of less than 0.5 (indicating very similar responses). As a result, 42 responses were excluded, leaving a final sample size of 120, exceeding the recommended minimum.

5. Results

5.1 Descriptive statistics

The sample included 47.5% (57) identifying as female and 52.5% (63) as male. They represented a broad age range, mostly from 21 to over 60 years, with only three participants over 60, and none under 20. 71.7% (86) of participants reported having 12 or more years of professional experience. Only 2.5% (3) had under 2 years of work experience. These demographics indicate a mature and experienced participant group.

5.2 Measurement validation

The SPSS analysis produced a KMO measure of sampling adequacy of 0.888 and a significant Bartlett's test of sphericity ($p < 0.001$), confirming the suitability of the data for factor analysis. All thresholds and methods follow the guidelines by Hair *et al.* (2021), unless otherwise noted.

The lowest communality extraction value was 0.640. Given a sample size of 120, factor loadings needed to be above 0.500, with the lowest observed factor loading being 0.694, meeting this criterion. Additionally, the cross-loading difference exceeded 0.200, and no correlations in the Factor Correlation Matrix surpassed 0.700. The model accounted for 75.25% of the total variance, well above the 60% threshold, and satisfied all model fit requirements, as detailed in Table 2.

A clean EFA was achieved by ensuring that survey items were designed to measure specific constructs loaded together under a single factor, demonstrating convergent validity, while remaining distinct from other factors, demonstrating discriminant validity. Items that aligned significantly with a factor were assigned to the corresponding construct and appropriately labelled. The EFA extracted three distinct factors:

(1) Sanctions (SAN), 6 items;

Table 2. Validation and model fit summary

	EFA validation		Model fit summary		
Measure	Threshold value	Observed value	Measure	Threshold value	Observed value
KMO	>0.700	0.888	cmin/df	Between 1 and 3	1.284
Cronbach's alpha	>0.700	0.856–0.944	CFI	>0.950	0.981
Factor loadings	>0.550	0.694–0.908	RMSEA	<0.050	0.049
Extracted communalities	>0.500	0.640–0.879	PCLOSE	>0.050	0.508
Total variance explained	>60%	75.254%			
Inter-factor correlation	<0.700	0.441–0.514			

Source(s): Authors' own work

(2) Subjective Norms (SN), 4 items; and

(3) Cybersecurity Intention (CSI), 4 items. Although sanction certainty and severity were conceptualised as separate dimensions, they loaded together onto a single factor, suggesting they are perceived as a unified construct.

This outcome aligns with the notion that individuals may not differentiate sharply between the likelihood and severity of sanctions when forming compliance intentions. The full list of measurement items is presented in Appendix.

After meeting the model fit requirements, tests for convergent validity, discriminant validity, and reliability were conducted. Fit indices met recommended thresholds, with a cmin/df of 1.284, CFI of 0.981, RMSEA of 0.049, PCLOSE of 0.508, the lowest Composite Reliability (CR) being 0.818, the lowest Average Variance Extracted (AVE) being 0.535, and the Maximum Shared Variance (MSV)<AVE and the √AVE>absolute inter-construct correlations. All validity and reliability concerns were eliminated in the CFA solution, as shown in Tables 2 and 3.

A hierarchical regression analysis assessed the impact of sanctions and subjective norms on intentions, controlling for age and work experience. Control variables alone did not significantly predict CSI [$F(2,110) = 0.698$, $p = 0.500$, $R^2 = 0.013$]. Adding sanctions and subjective norms significantly improved the model [$F(4,108) = 18.073$, $p < 0.001$, $R^2 = 0.401$, $\Delta R^2 = 0.388$], with both emerging as significant predictors, while age and years of experience remained non-significant.

Three methods were used to assess Common Method Bias (CMB). First, Harman's single-factor test showed that a single factor accounted for only 35.89% of the total variance. Second, the Common Latent Factor (CLF) technique was used to evaluate the measurement model. Finally, the marker variable approach was applied utilising gender as the marker variable. All three techniques converged, indicating no evidence of CMB.

Table 3. Validity measures

Construct	CR	AVE	MSV	MaxR(H)	SN	SAN	CSI
SAN	0.947	0.751	0.292	0.958	*0.867*		
SN	0.818	0.535	0.469	0.878	0.540	*0.732*	
CSI	0.940	0.798	0.469	0.944	0.500	0.685	*0.893*

Source(s): Authors' own work

To analyse the moderation effect, the mean-centred values of subjective norms and sanctions were multiplied to create the interaction term. This new term, SAN×SN, was included in the structural model developed for hypothesis testing using AMOS 29.

5.3 Hypothesis testing

To investigate the moderating effect of subjective norms on sanctions, a comprehensive moderation analysis was conducted using three methods:

(1) examining the interaction term's effect;

(2) performing a simple slope analysis; and

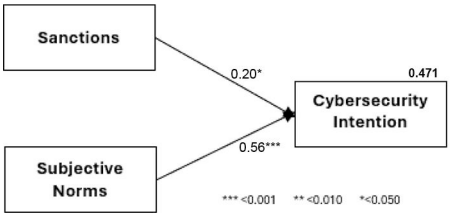
(3) evaluating the effects at high and low levels of subjective norms.

The results of each method are presented below.

First, following the guidelines of Aiken *et al.* (1991) and Hair *et al.* (2021), the moderating effect of subjective norms on sanctions was assessed by comparing the model without the interaction term (Figure 2) to the model including the interaction term (Figure 3).

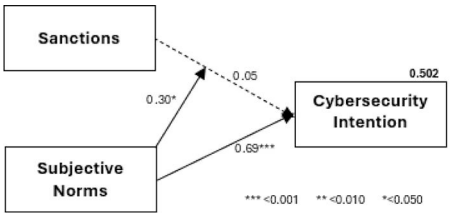
Figure 2 presents the R^2 value (top right of the dependent variable), standardised regression coefficient (β), *t*-values and the *p*-value for the research model without the interaction term. The results indicate that the direct effects of sanctions ($\beta = 0.203$, $t = 2.166$, $p = 0.030$) and subjective norms ($\beta = 0.555$, $t = 4.539$, $p < 0.001$) were both significant and positive. This model explains 47.1% of the variance in behavioural intention.

Next, the model was re-evaluated with the interaction term included (Figure 3). This moderator model, which represents our research model, accounts for 50.2% of the variance in behavioural intention.



H	Path	β	t-value	p-value
H1	SAN→CSI	0.203	2.166	0.030 (s)
H2	SN→CSI	0.555	4.539	*** (s)

Figure 2. Research model results without the interaction term
Source: Authors' own work



H	Path	β	t-value	p-value
H1	SAN→CSI	0.049	0.417	0.677 (ns)
H2	SN→BI	0.686	5.249	*** (s)
H3	SAN×SN →CSI	0.302	2.214	0.027 (s)

Figure 3. Research model (moderator model) hypotheses testing
Source: Authors' own work

In the moderator model, the relationship between sanctions and intentions represents a simple impact rather than a direct impact. The non-significant finding for *H1* indicates that the simple effect of sanctions did not show a significant influence on intentions ($\beta = 0.049$, $t = 0.417$, $p = 0.677$). However, this non-significant *simple* impact should not be misinterpreted as if it were a direct effect, as this can lead to inaccurate and misleading conclusions (Hair *et al.*, 2021). On the other hand, both subjective norms and the interaction term (SAN×SN) had a significant positive impact on intention ($\beta = 0.686$, $t = 5.249$, $p < 0.001$; $\beta = 0.302$, $t = 2.214$, $p = 0.027$, respectively). These findings support hypotheses *H2* and *H3*, confirming that subjective norms not only have a direct effect but also enhance the influence of sanctions through interaction.

Comparing Figures 2 and 3, subjective norms remained significant in both models, while the impact of sanctions changed. This shift suggests that subjective norms moderate the relationship between sanctions and intention. Specifically, subjective norms had a stronger positive effect ($\beta = 0.686$ versus 0.555) when the interaction term was included, indicating a moderating role. The increased significance of subjective norms in the moderator model confirms their positive moderating effect on the sanctions–intention relationship. This implies that sanctions exert a stronger effect on intention when subjective norms are strong. Although sanctions alone did not have a significant simple impact on intention, the significant interaction effect (*H3*) demonstrates that their influence emerges in the presence of strong subjective norms.

Additionally, the interaction effect size (f^2) was calculated by comparing the R^2 values between the models with and without the interaction. The obtained effect size of 0.0622 suggests a large interaction effect. An interaction effect size above 0.025 is considered large (Hair *et al.*, 2021).

Second, a simple slope analysis was conducted to better understand the interaction effects, as shown in Figure 4. The slope for high subjective norms (solid line) is steeper than that for low norms (dashed line), suggesting that high subjective norms significantly amplify the intention to comply as sanctions increase. Conversely, when subjective norms are low, the increase in intention is less pronounced as sanctions rise, reinforcing their moderating role in the relationship between sanctions and intentions to reuse passwords in the workplace. Notably, intention improves in both groups, but the effect is stronger for individuals with high subjective norms.

Finally, the impact of sanctions was examined under conditions of high (>=mean) and low (<mean) subjective norms. Regression analysis revealed that sanctions significantly influenced intentions in both cases, with a stronger effect under high subjective norms ($\beta = 0.442$, $p < 0.001$) compared to low subjective norms ($\beta = 0.362$, $p = 0.009$). This finding suggests that strong subjective norms amplify the effect of sanctions on intentions more than weak subjective norms. Thus, there is robust evidence supporting *H3*, confirming a significant moderation effect of subjective norms on the sanctions–intentions relationship.

To gain further insights, we also tested whether sanctions moderate the impact of subjective norms. In both models (Figures 2 and 3), subjective norms remained significant regardless of the inclusion of the interaction term. Slope analysis also indicated no significant effect of sanctions on subjective norms, affirming that subjective norms indeed moderate the effect of sanctions rather than the reverse. Thus, the interaction reflects subjective norms moderating the effect of sanctions, consistent with the theoretical rationale outlined in Section 2.3.

6. Discussion

This study examined how subjective norms and sanctions jointly influence employees' cybersecurity intentions. Specifically, whether subjective norms moderate the effect of

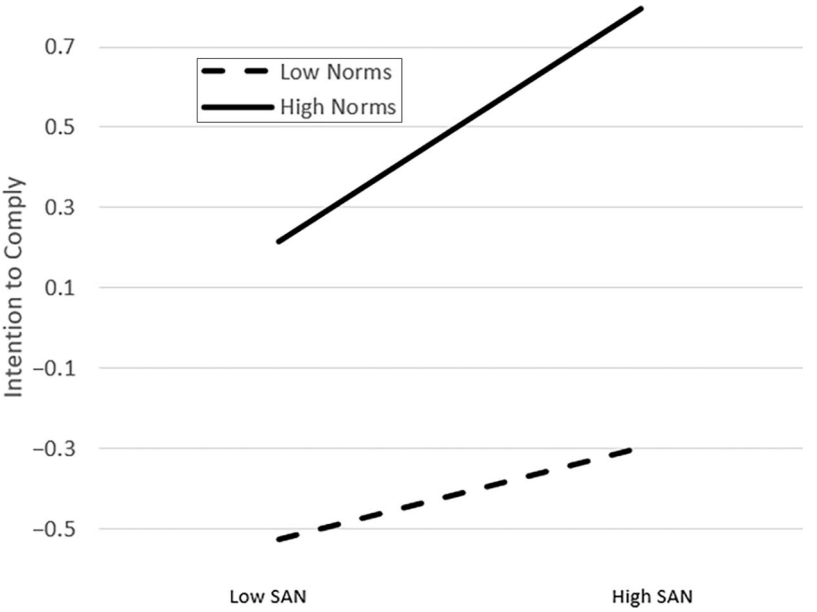


Figure 4. Interaction effect
Source: Authors' own work

sanctions. The results indicate that subjective norms play a dual role: they not only directly influence intentions but also shape the strength of the relationship between sanctions and intentions. This finding highlights the importance of integrating social mechanisms, such as fostering a security-oriented culture and reinforcing peer expectations, alongside formal controls like rules and penalties.

Although sanctions significantly influenced intentions, consistent with DT and previous research [e.g. Vance *et al.* (2020), Siponen *et al.* (2010), Li *et al.* (2010)], their effect became non-significant when subjective norms were low. These findings extend existing work by showing that while sanctions can foster a "have-to" culture, where employees follow rules due to fear of punishment. Whereas subjective norms help create a "want-to" culture, where compliance is driven by a sense of shared responsibility and long-term commitment. This suggests that organisations should not rely solely on sanctions but rather complement them with efforts to cultivate a security-minded culture. Such alignment provides legitimacy to sanctions and fosters acceptance, thereby increasing their impact on intentions. Despite the diminished influence of sanctions in the absence of strong norms, they remain a necessary foundation. Managers should continue to enforce sanctions for misconduct while also implementing complementary mechanisms that enhance their effectiveness.

The significant influence of subjective norms, consistent with TPB and previous research [e.g. Safa *et al.* (2019), Kuo *et al.* (2017), Foth (2016)], suggests that employees are more likely to comply with password protocols when they perceive strong peer support for such behaviour; this complements Grimes and Marquardson (2019). This study extends the role of subjective norms by demonstrating both a significant direct effect and a moderating influence on the relationship between sanctions and compliance intentions.

Prior IS research has largely focused on the individual effects of sanctions and subjective norms. This study advances the literature by empirically testing their interaction. The significant positive interaction effect suggests that strong subjective norms enhance the impact of sanctions rather than conflict with them. This supports *H3* and aligns with the pattern identified in Section 2.3. Figure 4 also shows how high subjective norms amplify the positive relationship between sanctions and intention compared to low subjective norms. This suggests that when employees perceive that peers and managers view sanctions as legitimate, they become a more effective deterrent, a finding that complements Merhi and Ahluwalia (2019). Conversely, in environments with weak subjective norms, sanctions may need to be more severe – a finding that challenges the assumption that sanctions sufficiently drive behaviour.

The moderating role of subjective norms may help explain the mixed findings in the literature on sanctions. Studies reporting a non-significant impact of sanctions may have overlooked the influence of weak subjective norms, which this study identifies as a critical moderating factor. While this interaction may seem evident in studies that examined both constructs (see Table 1), it may also shed light on inconsistent results in studies that did not account for subjective norms. For example, findings by Prabhu and Ahmed (2024) and Hooper and Blunt (2020) may reflect contexts where subjective norms were comparatively weaker, thereby diminishing the observed impact of sanctions.

6.1 Contributions

While prior research suggests that subjective norms may enhance the effectiveness of sanctions, this relationship was not tested in the context of cybersecurity. By analysing both the direct and interaction effects, this study refines our understanding of how formal deterrence mechanisms (sanctions) and informal social influences (subjective norms) jointly shape cybersecurity behaviour.

Refining the role *of sanctions:* Traditional security policies often assume that stronger sanctions directly improve compliance. This study challenges that view, showing that the effectiveness of sanctions is contingent upon the strength of subjective norms within an organisation. Our findings reveal that sanctions are most effective when reinforced with strong peer expectations. It identifies subjective norms as a key boundary condition influencing formal enforcement.

Reconceptualising the role *of subjective norms:* This study reveals that subjective norms do more than directly shape security intentions; they also moderate the impact of sanctions, either amplifying or diminishing their effectiveness. This insight reframes subjective norms as active agents that influence sanctions rather than merely co-existing alongside them.

Explaining inconsistencies in sanction effectiveness: Prior studies have yielded mixed results on the impact of sanctions on cybersecurity intentions. This study suggests that such discrepancies may be due to variations in the strength of subjective norms across contexts. By empirically establishing the moderating role of subjective norms, this study provides a compelling explanation for the conflicting outcomes observed in the literature.

6.1.1 Practical contributions. Optimising sanctions based on norms: The findings suggest that a balanced approach, where formal deterrence controls are reinforced by informal social influences, yields optimal outcomes. Where strong subjective norms exist, moderate sanctions may suffice, avoiding overly harsh penalties that could harm morale. Conversely, in organisations with weak norms, sanctions alone may be ineffective. Managers should consider building a stronger security culture through peer influence and leadership engagement to enhance the impact of formal deterrents.

Building a "want-to" security culture: Our findings highlight the importance of moving beyond a sanction-only approach to security compliance. While sanctions help establish behavioural boundaries, their impact is greater when supported by strong subjective norms. Organisations should foster a "want-to" culture, where employees internalise security best practices through peer influence and shared responsibility. This can be supported by leadership modelling secure behaviours, recognising good practices, and promoting peer accountability.

Designing more effective security awareness programs: The findings support a balanced approach that combines appropriate sanctions with strong subjective norms. Security awareness programs should go beyond rules and penalties to leverage social influence. For example, through engaging influential employees as security champions, embedding compliance expectations within team dynamics, and reinforcing positive norms. This integrated approach is more likely to lead to stronger, sustained compliance outcomes.

Aligning sanctions with strong subjective norms allows organisations to encourage compliance not just as a means of avoiding penalties but as a socially valued and professionally rewarding behaviour. This approach minimises the risk of resistance or diminished morale, which can occur when employees perceive sanctions as punitive rather than supportive. Overall, this study contributes to the literature by highlighting the critical role of subjective norms in enhancing the effectiveness of sanctions, offering a more comprehensive understanding of how both factors work together to shape intentions.

6.2 Limitations

This study has some limitations that should be acknowledged. First, it focuses on a specific insider IS behaviour, password reuse, providing valuable insights into this behaviour. However, this specific focus may restrict the applicability of the findings to other cybersecurity practices. Second, the use of self-reported data raises concerns about potential social desirability bias and recall inaccuracies, which could affect the accuracy of the responses. Third, while the methodological choice to examine intentions aligns with established research in cybersecurity behaviour (as illustrated in Table 1), intentions may not always directly translate into actual behaviour. Finally, the use of a UK-based sample limits the generalisability of the results, as perceptions of sanctions and normative influences may differ across cultural contexts.

6.3 Future research

The limitations offer opportunities for further research. To gain a more comprehensive understanding of insider cybersecurity practices, future studies should expand the scope to include a wider range of common security behaviours. Methodological diversification, including experimental designs to establish causal relationships or qualitative methods such as interviews or focus groups to explore underlying motivations, could further enrich research. Additionally, future research could explore the extent to which intentions translate into actual password reuse. Finally, cross-cultural studies may allow researchers to explore how cultural dimensions, such as individualism versus collectivism and power distance, influence the perception and effectiveness of sanctions and the strength of subjective norms. Such research could inform the development of culturally tailored and contextually appropriate cybersecurity interventions.

7. Conclusion

This study examined how subjective norms and sanctions jointly influence employees' cybersecurity behaviour, focusing on workplace password reuse. The research examined the

potential interaction between these two factors, and the results provide a model where both formal deterrence and informal social influences work synergistically to shape intentions. The findings reveal that subjective norms exert a dual impact: they directly influence cybersecurity intentions and significantly moderate the effect of sanctions on those intentions. This suggests that strong subjective norms can amplify the effectiveness of sanctions, making them more impactful in promoting compliance.

References

Aigbefo, Q.A., Blount, Y. and Marrone, M. (2022), "The influence of hardiness and habit on security behaviour intention", *Behaviour and Information Technology*, Vol. 41 No. 6, pp. 1151-1170.

Aiken, L.S., West, S.G. and Reno, R.R. (1991), *Multiple Regression: Testing and Interpreting Interactions*, Sage Publications, Newbury Park.

Ajzen, I. (1985), "From intentions to actions: a theory of planned behavior", *Action Control: From Cognition to Behaviour*, Springer, Heidelbery, pp. 11-39.

Ajzen, I. (1991), "The theory of planned behaviour", *Organizational Behaviour and Human Decision Processes*, Vol. 50, pp. 179-211.

Ajzen, I. and Fishbein, M. (1970), "The prediction of behavior from attitudinal and normative variables", *Journal of Experimental Social Psychology*, Vol. 6 No. 4, pp. 466-487.

Anderson, L.S., Chiricos, T.G. and Waldo, G.P. (1977), "Formal and informal sanctions: a comparison of deterrent effects", *Social Problems*, Vol. 25 No. 1, pp. 103-114.

Bagozzi, R.P. (2011), "Measurement and meaning in information systems and organizational research: methodological and philosophical foundations", *MIS Quarterly*, Vol. 35 No. 2, pp. 261-292.

Brown, D.A. (2017), "Examining the behavioral intention of individuals' compliance with information security policies", Ph.D Dissertation, Walden University.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013), "Understanding the violation of is security policy in organizations: an integrated model based on social control and deterrence theory", *Computers and Security*, Vol. 39, pp. 447-459.

D'Arcy, J. and Devaraj, S. (2012), "Employee misuse of information technology resources: testing a contemporary deterrence model", *Decision Sciences*, Vol. 43 No. 6, pp. 1091-1124.

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*, Vol. 20 No. 1, pp. 79-98.

Davis, D.K., Chowdhury, M.M. and Rifat, N. (2022), "Password security: what are We doing wrong? ", *2022 IEEE International Conference on Electro Information Technology, 2022*. *IEEE*, pp. 562-567.

DBIR (2022), *Data Breach Investigations Report*, Verizon Threat Research Advisory Centre.

DBIR (2024), *2024 Data Breach Investigations Report.*

Fishbein, M. and Ajzen, I. (1975), "Beliefs, attitude, intention and behavior: an introduction to theory and research", Addison-Wesley, Massachusetts.

Foth, M. (2016), "Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence", *European Journal of Information Systems*, Vol. 25 No. 2, pp. 91-109.

Grimes, M. and Marquardson, J. (2019), "Quality matters: evoking subjective norms and coping appraisals by system design to increase security intentions", *Decision Support Systems*, Vol. 119, pp. 23-34.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Danks, N.P. and Ray, S. (2021), "Moderation analysis", *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*, Springer International Publishing, Cham.

Herath, T. and Rao, H.R. (2009a), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Herath, T. and Rao, H.R. (2009b), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Hooper, V. and Blunt, C. (2020), "Factors influencing the information security behaviour of IT employees", *Behaviour and Information Technology*, Vol. 39 No. 8, pp. 862-874.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol. 54 No. 6, pp. 54-60.

Jaeger, L., Eckhardt, A. and Kroenung, J. (2021), "The role of deterrability for the effect of multi-level sanctions on information security policy compliance: results of a multigroup analysis", *Info. and Management*, Vol. 58, p. 103318.

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*, Vol. 39 No. 1, pp. 113-134.

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*, Vol. 25 No. 3, pp. 231-251.

Kuo, K.-M., Talley, P.C., Hung, M.-C. and Chen, Y.-L. (2017), "A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy", *Journal of Medical Systems*, Vol. 41 No. 12, pp. 1-10.

Liao, Q., Gurung, A., Luo, X. and Li, L. (2009), "Workplace management and employee misuse: does punishment matter?", *Journal of Computer Information Systems*, Vol. 50 No. 2, pp. 49-59.

Li, H., Zhang, J. and Sarathy, R. (2010), "Understanding compliance with internet use policy from the perspective of rational choice theory", *Decision Support Systems*, Vol. 48 No. 4, pp. 635-645.

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*, Vol. 92, pp. 37-46.

Merhi, M.I. and Ahluwalia, P. (2024), "Predicting compliance of security policies: norms and sanctions", *Journal of Computer Information Systems*, Vol. 64 No. 5, pp. 683-697.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly*, Vol. 42 No. 1.

Prabhu, S. and Ahmed, M. (2024), "The impact of security incidents on employee behaviour", Australasian Conference of Information Systems (ACIS 2024), 2024.

Prabhu, S. and Dell, P. (2025), "The nexus between sanctions and neutralization in information security", 58th HI International Conference on System Sciences, 2025.

Prabhu, S. and Thompson, N. (2022), "A primer on insider threats in cybersecurity", *Information Security Journal: A Global Perspective*, Vol. 31 No. 5, pp. 602-611.

Rajab, M. and Eydgahi, A. (2019), "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education", *Computers and Security*, Vol. 80, pp. 211-223.

Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M. and Sookhak, M. (2019), "Deterrence and prevention-based model to mitigate information security insider threats in organisations", *Future Generation Computer Systems*, Vol. 97, pp. 587-597.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, pp. 487-502.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with information security policies: an empirical investigation", *Computer*, Vol. 43 No. 2, pp. 64-71.

Stainbrook, M. and Caporusso, N. (2018), "Convenience or strength? Aiding optimal strategies in password generation", *International Conference on Applied Human Factors and Ergonomics, 2018*, *Springer*, pp. 23-32.

Straub, D.W. (1990), "Effective is security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-469.

Syed, T.A., Wiener, M., Mehmood, F. and Abdelrahman, M. (2021), "Control-style ambidexterity and information systems project performance: an expanded view of control activities", *European Journal of Information Systems*, Vol. 32 No. 3, pp. 1-23.

Turner, J.C. and Oakes, P.J. (1986), "The significance of the social identity concept for social psychology with reference to individualism, interactionism and social influence", *British Journal of Social Psychology*, Vol. 25 No. 3, pp. 237-252.

Vafaei-Zadeh, A., Thurasamy, R. and Hanifah, H. (2019), "Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior", *Kybernetes*, Vol. 48 No. 8, pp. 1565-1585.

Vance, A., Siponen, M.T. and Straub, D.W. (2020), "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures", *Information and Management*, Vol. 57 No. 4, p. 103212.

Vedadi, A., Warkentin, M. and Dennis, A. (2021), "Herd behavior in information security decision making", *Information and Management*, Vol. 58 No. 8, p. 103526.

Wang, C., Jan, S.T., Hu, H., Bossart, D. and Wang, G. (2018), "The next domino to fall: empirical analysis of user passwords across online services", *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy, 2018*, pp. 196-203.

Wenzel, M. (2004), "The social side of sanctions: personal and social norms as moderators of deterrence", *Law and Human Behavior*, Vol. 28 No. 5, pp. 547-567.

Appendix

Table A1. Survey measurement items

Measurement item	Loading	Mean	S.D.
Sanctions			
My organisation monitors employees' password behaviour	0.842	3.577	2.065
It is likely that reusing unique work passwords will be detected	0.841	3.211	1.924
If I reuse my work password, I would probably be caught	0.893	2.953	1.829
My organisation disciplines employees who reuse work passwords	0.825	2.928	1.754
If my organisation caught me not using unique work, I would be severely punished	0.856	3.136	2.000
If my organisation caught me reusing work passwords, the consequences would be very bad for me	0.850	3.396	1.900
Subjective norms			
People whose opinions I value would approve of me not reusing work passwords	0.749	5.248	1.709
People who are important to me would agree that not reusing work passwords is good practice	0.694	5.570	1.410
My boss thinks that I should use unique work passwords	0.731	5.427	1.575
My organisation's IT department thinks that I should use unique work passwords	0.859	6.151	1.303
Cybersecurity intentions			
I am certain that I will not reuse my work passwords	0.816	5.050	1.726
I am likely to use unique work passwords	0.895	5.588	1.520
I intend to keep my work passwords unique	0.857	5.600	1.475
I plan to use unique work passwords	0.908	5.742	1.446

Note(s): 1 = strongly disagree to 7 = strongly agree
Source(s): Authors' own work

Corresponding author
Sunitha Prabhu can be contacted at: s.sunitha.prabhu@gmail.com