Behaviour & Information Technology

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tbit20

Keeping the gates closed: the effect of conflict management styles, anxiety, and technical skills on security noncompliance intention among smartphone users

Diyako Rahmani, Hamed Jafarzadeh & Alexandra Claudia Hess

To cite this article: Diyako Rahmani, Hamed Jafarzadeh & Alexandra Claudia Hess (12 Aug 2024): Keeping the gates closed: the effect of conflict management styles, anxiety, and technical skills on security noncompliance intention among smartphone users, Behaviour & Information Technology, DOI: 10.1080/0144929X.2024.2390059

To link to this article: https://doi.org/10.1080/0144929X.2024.2390059

Published online: 12 Aug 2024.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2024.2390059

Taylor & Francis
Taylor & Francis Group

Keeping the gates closed: the effect of conflict management styles, anxiety, and technical skills on security noncompliance intention among smartphone users

Diyako Rahmani [a], Hamed Jafarzadeh [b] and Alexandra Claudia Hess [a]

[a]School of Communication, Journalism, and Marketing, Massey University, Auckland, New Zealand; [b]Department of Actuarial Studies and Business Analytics, Macquarie University Business School

ABSTRACT

Using personal mobile phones for work-related purposes is an increasingly common trend in organisations yet adding to cyber security concerns. It is vital to identify employees' characteristics that impact security noncompliance behaviours when using mobile phones at work, as it could open a channel for cyber-attacks in the enterprise's IT systems. Using the unique context of personal smartphones and building on the theoretical framework of the Dual-Concern Model, this study identifies key characteristics of employees' intention to engage in security noncompliance activities. Through a scenario-based survey of 391 mobile phone users in the United States, we examined the impact of personal characteristics (specifically conflict management style, context-specific anxiety, and technological skills) in explaining people's intention to demonstrate security noncompliance behaviours. Younger individuals, those with higher conflict approach tendencies, and those with online communication apprehension tend to show higher noncompliance with information system security policies. Also, technical skills were found to moderate the association of online communication apprehension with increased noncompliance with security policies. The findings offer a range of theoretical implications and practical insights for strengthening organisations' cyber security.

ARTICLE HISTORY
Received 17 January 2023
Accepted 4 August 2024

KEYWORDS
Online anxiety; conflict management style; technical skills; compliance; structural equation modelling; dual-concern model

1. Introduction

The widespread adoption of the Bring Your Own Device (BYOD) policy has led to significant changes in organisations (Palanisamy, Norman, and Mat Kiah 2024). BYOD offers numerous benefits to both employees and organisations, including saving costs (Aguboshim and Udobi 2019), increasing productivity and enhancing efficiency (Doargajudhur and Dell 2020). BYOD has become indispensable for organisational success, especially since the COVID-19 pandemic necessitated remote and hybrid work environments. The BYOD market has demonstrated significant growth, with a compound annual growth rate (CAGR) of 15.4%. This expansion has seen the market value increase from $70.1 billion in 2023 to a projected $239.5 billion by 2032 (Munde 2024; Palanisamy, Norman, and Mat Kiah 2020). However, the BYOD practice introduces additional security risks to organisations (Chen et al. 2021; Ratchford et al. 2022), including data leakage and malware risks, necessitating robust device security, employee training, and policy enforcement to mitigate threats posed by outdated operating systems, malicious applications, and device loss or theft (Yacono 2023).

Individuals using personal devices often prioritise convenience over security, leading to higher levels of security noncompliance (Ratchford et al. 2022). Moreover, the specific risks associated with employees using their BYOD devices (including mobile phones) at work extend beyond mere convenience concerns. Employees may inadvertently expose sensitive organisational data to potential threats through unsecured personal devices (Ratchford et al. 2022). For instance, accessing work-related documents on personal devices might occur in less secure environments, increasing the likelihood of data breaches or unauthorised access. This problem is exhilarating because organisational IT services have less control over personal devices than organisational devices, resulting in BYODs lacking the necessary security configurations or software updates to adequately protect sensitive organisational data. This lack of control introduces a heightened level of

CONTACT Diyako Rahmani d.rahmani@massey.ac.nz School of Communication, Journalism and Marketing, Massey University, Albany, Auckland, 0632, New Zealand

risk and creates a conflict of noncompliance with Information System Security Policies (ISSP) as employees strive to balance smooth and efficient work processes with the need for conscious attention to security and data preservation (Ratchford et al. 2022; Vorakulpipat et al. 2017). Reports show that employees' ISSP compliance behaviour remains a challenge in organisations (Ogbanufe, Crossler, and Biros 2021; Parsons et al. 2017), especially in the government and public sector due to weak enforcement (Teoh, Kamil Mahmood, and Dzazali 2018). To address this problem, it is critical for organisations to develop targeted strategies to manage noncompliance with ISSPs, promote responsible BYOD usage, and ultimately mitigate the risks associated with it. To achieve those goals, organisations need to identify relevant employee characteristics associated with noncompliance in the context of Information Technology (IT) usage.

We investigate user characteristics at two context (i.e. broader context and narrow context). First, our broader context (i.e. IT use) points towards the relevance of anxiety as a potential antecedent of noncompliance with ISSP. Namely, Online Communication Apprehension (OCA) and Digital Technology Anxiety (DTA) are two forms of anxiety associated with the use of IT. OCA is the anxiety one endures during actual or anticipated online communication (Ledbetter 2009), while DTA is defined as the fear of working with technology, also known as computer anxiety, technophobia, and technology anxiety (Scott and Rockwell 1997). Previous research has shown that OCA decreases the use of new technologies, especially the more complicated ones (Scott and Timmerman 2005) while DTA knowingly affects the decisions and perceptions of technology use (Celik and Yesilyurt 2013) such as associations with security system anxiety in organisational settings (Hwang et al. 2017). Based on previous research, we reason that those forms of IT-related anxiety affect decision-making and compliance behaviours and intentions (D'Arcy, Herath, and Shoss 2014; Lee, Lee, and Lee 2022) and the likelihood of ISSP noncompliance. Second, in our narrower context, the nature of personal mobile devices used for work purposes and its associated need for ISSP points towards a conflict between employees' (i.e. the self) needs for convenience (linked to noncompliance), and employers' (i.e. others) need for security (linked to compliance). Adapting the Dual Concern Model (DCM) (Cai and Fink 2002), we predict that employees conflict management style impacts noncompliance. The ISSP-IT context points towards conflict management styles and online anxiety (OCA and DTA) as a potential leverage point for intervention that has the potential to impact ISSP noncompliance.

Further, existing literature points towards the importance of technical skills in manging ISSP noncompliance (LaRose 2010; Nwokeji et al. 2019; Sundar 2008; Vishwanath 2016). Technical skills, defined as proficiency in utilising security features and understanding security protocols, are also crucial for users' ability to adhere to security measures and safeguard organisational information (Tsohou and Holtkamp 2018). We propose that individuals with advanced technical skills are more likely to use heuristics compared to users with less advanced technical skills. Those cognitive heuristics (and the associated deployment of mental shortcuts) can impact the way they deal with the cognitive burden caused by the convenience/security conflict. Consequently, the application of heuristics could 'cognitively handicap' them (Hinds 1999), making them neglectful in adhering to ISSP protocol.

Despite the importance of ISSP compliance for organisations, no research has identified and tested the critical context-relevant variables that can potentially influence ISSP compliance. Namely, no study has comprehensively investigated how (1) IT-associated anxiety (OCA and DTA) and (2) conflict management style associated with BYOD impact ISSP compliance. Furthermore, no research has looked at the role of (3) technical skills in the interactions between conflict management styles, OCA, and DTA with the intention to noncomply with information systems. We address this gap in the literature by drawing on cognitive psychology theory (MacLeod 1996) and the DCM (Cai and Fink 2002). Our study investigates the impact of anxiety associated with IT, conflict management style, and their interaction with technical skills on ISSP compliance in the context of BYOD.

Our research makes several distinct contributions to extant literature. Fist, we contribute to the literature on ISSP compliance by identifying and testing key variables associated with noncompliance. Second, we contribute to the literature on DCM (Cai and Fink 2002) and its applicability to ISSP compliance in the context of BYOD. The DCM is a widely utilised and efficient framework for comprehending and addressing conflicts across diverse contexts such as education (Miller 2022), intercultural management (Li, Worm, and Xie 2018), construction management (Musenero, Baroudi, and Gunawan 2021), and finance (Awadallah 2018) to name a few. The model identifies different conflict management styles, including approaching and avoiding styles. These styles have different implications for the outcomes and relationships of the parties involved in the conflict and significantly influence how individuals respond to security-related situations when conflict is present.

The remainder of this paper is organised as follows. First, the primary constructs will be reviewed, and the

hypothesis and research questions will be presented. Then, the sample and measurement scales will be introduced and the test results of measurement validation and hypotheses using confirmatory factor analysis and structural equation modelling will be reported. Following the method section, the study will discuss the main findings, theoretical and practical implications, and present the limitations and conclusions.

2. Literature review and research model

2.1. ISSP noncompliance

Noncompliance is explicated as the manifestation of conduct that deviates from established norms or prescribed behaviour within a specified time frame (Lipschultz and Wilder 2017). Previous studies showed that negative feelings and reactance (Tatum, Olson, and Frey 2018), cultural orientation, and personal characteristics (Golish 1999), such as education (Rahmani et al. 2021), could influence noncompliance. ISSP Noncompliance is a counterproductive behaviour that undermines organisational goals, values, and norms, causing negative outcomes for both individuals and the organisation (Greenberg 2003; Klotz and Buckley 2013; Marcus and Schuler 2004).

Various theories have been employed to study ISSP noncompliance. Khatib and Barki (2020) applied activity theory, highlighting that contradiction and conflict among components like subjects, community, rules, division of labour, tools, and objects contribute to ISSP noncompliance. General deterrence theory emphasises the lack of anxiety about sanctions as a cause of noncompliance (D'Arcy, Herath, and Shoss 2014). Protection motivation theory builds on deterrence theory, incorporating self-efficacy and social influence in assessing ISSP threats (Vance, Siponen, and Pahnila 2012). Neutralisation theory suggests employees justify noncompliance through various strategies (Siponen and Vance 2010), while moral reasoning theory posits that internalised ISSPs create a sense of obligation to comply, thereby reducing the likelihood of noncompliance (Jaeger, Eckhardt, and Kroenung 2021). Social and contextual circumstances and cognitive elements such as cost and benefit analysis related to ISSP noncompliance are further explained by the rational choice theory (Balozian, Leidner, and Xue 2022), the theory of reasoned action (Siponen, Adam Mahmood, and Pahnila 2014), and the theory of interpersonal behaviour (Pee, Woon, and Kankanhalli 2008).

Previous research has explored individual characteristics, organisational policies, and social influences that affect counterproductive behaviours (Pee, Woon, and Kankanhalli 2008; Ratchford et al. 2022), which could also be attributed to ISSP noncompliance. The reviewed literature encompasses various variables and categories that significantly contribute to understanding information security policy compliance. Deterrability is a key focus, with Jaeger, Eckhardt, and Kroenung (2021) challenging traditional theories and emphasising the role of sanctions. Protection Motivation Theory (PMT) is examined by Mou et al. (2022), revealing nuances in its predictors, the mediating role of fear, and the impact of cultural factors and context. McLeod and Dolezel (2022) investigate factors influencing end users' capitulation, including privacy loss, vulnerability, distrust of security, and self-efficacy. Ifinedo (2014) integrates the theory of planned behaviour, social bond theory, and social cognitive theory, highlighting the importance of socialisation, influence, and cognition in shaping ISSP compliance intentions. Hwang et al. (2017) identify factors influencing noncompliance, extending the health belief model and protection motivation theory. Hadlington et al. (2019) explore individual differences, linking locus of control, work identity commitment, work identity reconsideration, and demographic factors to information security awareness. Cram, Proudfoot, and D'Arcy (2021) introduce security fatigue, identifying antecedents (inconvenience, perceived legitimacy, quantity, and method of communication of security policy requirements) and consequences (ignoring requirements, utilising workarounds, minimising security effort), challenging the traditional compliance dichotomy.

The consequences of ISSP noncompliance are well-documented in prior research. Noncompliance can also result in increased security risks, compromised data, and vulnerability to cyber-attacks (Hwang et al. 2017; Kim and Kim 2017; Siponen, Adam Mahmood, and Pahnila 2014) as well as diminished job performance, impaired decision-making, decreased job satisfaction, and elevated levels of negative emotional responses (D'Arcy, Herath, and Shoss 2014; Lee, Lee, and Kim 2016; Trang and Nastjuk 2021). Furthermore, ISSP noncompliance can result in data loss or theft (Puhakainen and Siponen 2010; Siponen and Vance 2010) increased errors in detecting and preventing security incidents (Cram, Proudfoot, and D'Arcy 2021), reputational damage to individuals and organisations, compromised intellectual property, and negative impact on performance and innovation (Balozian, Leidner, and Xue 2022; Pee, Woon, and Kankanhalli 2008).

Research suggests diverse strategies to address counterproductive behaviours and ISSP noncompliance. Bauer, Bernroider, and Chudzikowski (2017) emphasise a comprehensive, long-term approach in Information

Security Awareness (ISA) programmes, tailoring interventions to user groups. Chang and Seow (2019) introduce scales for measuring IT vision conflict and suggest user-focused communication strategies. Karlsson, Kolkowska, and Petersson (2022) provide requirements for ISSP compliance research, proposing short-term use of user stories and mid-to-long-term efficiency improvements. Khatib and Barki (2022) highlight the role of perceived noncompliance rewards, recommending management strategies. Kim and Kim (2017) stressed the role of organisational efforts in creating a compliance culture. Kolkowska, Karlsson, and Hedström (2017) advocated the value-based compliance (VBC) method to analyze rationalities related to information security. Martin, Wellen, and Grimmer (2016) explore attitudes towards surveillance and suggest mitigating negative effects through work empowerment. Puhakainen and Siponen (2010) offer insights from an IS compliance training programme, emphasising systematic training, personal relevance, continuous communication, and management support as key elements for improving compliance with IS security policies. Amankwa, Loock, and Kritzinger (2018) showed that top management support, education, awareness, ISSP acceptance, IS leadership, and user involvement reduce ISSP noncompliance.

While the current research on ISSP noncompliance has investigated the various organisational decision-making processes, the impact of the personal characteristics and emotional profile of the involved parties on ISSP noncompliance tendencies are understudied. ISSP noncompliance of BYODs provides a particular context that can help identify such characteristics. Hence, we identify conflict management style (due to the conflict of using a personal device in a corporate setting), anxiety related to IT, and technical skills as characteristics that are likely to impact ISSP compliance. Conflict management style in its associated DCM has the potential to explain the possible outcomes related to convenience/security conflict related to the use of BYODs in organisations.

2.2. Conflict management styles in the context of BYOD

Conflict, defined as 'the perceived and/or actual incompatibility of values, expectations, processes, or outcomes between two or more parties' (Ting-Toomey 1994, 360), decreases cognitive flexibility and creative thinking (De Dreu and Weingart 2003), and freezes cognitive schemas (Bar-Tal, Kruglanski, and Klar 1989). Various conflict management styles may have cognitive consequences, such as approaching conflict, which is characterised by a self-focused and explicit communication style with high concern for one's own interests and a lack of interest in others' concerns, or avoiding conflict, which is marked by low cooperativeness and assertiveness with no interest in either party's concerns (Elgoibar, Euwema, and Munduate 2017; Zhang et al. 2017). Although individuals may employ different conflict management styles based on situational factors, previous studies suggest a connection between personality differences and specific conflict management styles (Ayub et al. 2017; Moberg 2001). This implies that, notwithstanding occasional variations, individuals tend to consistently manage conflicts in specific styles. This tendency may extend to both interpersonal and intrapersonal conflicts. The cognitive impact of engaging in and managing conflicts can impact the decisions made about security compliance because online interaction entails processing an increasingly massive amount of data coming from diverse sources and contents, which could cause information overload (i.e. cognitive overload or communication overload) (Schmitt, Debbelt, and Schneider 2018).

The application of technology in organisations entails making social choices that can continuously create interpersonal and intrapersonal conflict (Kling 1996). Previous studies also showed that conflicting values, such as the conflict in information availability and confidentiality (Hedström et al. 2011) and between functionality and IS goals (Albrechtsen 2007), can hinder ISSP compliance because employees are more lenient toward least-effort work rather than preventing information loss (Sundaramurthy et al. 2017). Also, organisational conflict and anxiety impair effective decision-making (Kuhn and Poole 2000). Barki and Hartwick (2001) showed that interpersonal conflict could cause disagreement and dissatisfaction in Information System Development (ISD) process, and various conflict management styles influence the ISD outcomes in organisations. However, conflict management positively affects the various forms of organisational compliance, such as budget and schedule compliance (Barki and Hartwick 2001; Robey, Smith, and Vijayasarathy 1993). Abraham and Chengalur-Smith (2011) found out that while conflict can cause a delay in implementation of ISSP, it could benefit the organisation by bringing pragmatism to security policies, and approaching conflict increases positive IS organisational outcomes.

Despite the important role of conflict in shaping ISSPs, previous research on the impact of various conflict management styles on noncompliance is relatively scarce yet contradictory. Previously, Carnevale and Probst (1998) showed that the decreasing impact of being competitive (i.e. approaching conflict) on

cognitive flexibility is mediated by (a) the level of arousal and anxiety one feels during a conflict and (b) attentional overload as it takes away cognitive resources and shrinks the possibility of finding the optimal solution. While a study of social network sites showed that approaching conflict increases privacy risk and avoiding conflict has no significant effect on it (Zhang et al. 2017), another one showed approaching conflict increases behavioural compliance, and both approaching and avoiding conflict decrease attitudinal compliance (Cenkci 2018). The DCM explains the various styles of conflict management across two dimensions, concern for oneself and concern for others, and it is particularly relevant in the context of BYOD.

Conflict management styles in the context of BYOD are crucial due to the potential conflicts arising from the integration of personal devices into the workplace. Research emphasises the significance of managing conflict effectively to ensure satisfactory outcomes (Wertheim 2011). Effective conflict management styles can significantly enhance the adoption and success of BYOD practices by reducing stress and work-life conflicts among employees (Chen et al. 2021). Moreover, conflict management styles play a vital role in determining employees' willingness to adopt BYOD practices, as information security-related conflict can lead to information security fatigue, hindering BYOD adoption (Chen et al. 2021). Additionally, implementing conflict resolution algorithms that integrate operational transformation and multi-versioning can help address conflicts that arise from shared document modifications in BYOD environments (Citro, McGovern, and Ryan 2007).

2.3. Dual-concern model

According to DCM, higher concern for one's own interests increases one's approach to conflict, while higher concern for other's interests increases the accommodating and integrating styles (Cai and Fink 2002; Sorenson, Morse, and Savage 1999). The DCM has been used to investigate conflict in various contexts, such as public-private partnership in infrastructure projects, where it showed partial adaptability and proved useful in developing a framework integrating behavioural aspects into conflict management for this context (Musenero, Baroudi, and Gunawan 2021). Previous studies employing the DCM explored the impact of communication traits (e.g. argumentativeness, aggressiveness, benevolence, and attitude certainty) on conflict management (Guerrero and Gross 2014; Rios, DeMarree, and Statzer 2014). These studies demonstrated that attitude certainty affects conflict management styles, influencing the perceptions of partners based on their exhibited traits. The observed traits go beyond the predictions of the dual-concern model, highlighting the significance of individual and interactive traits in shaping conflict styles. A study of family business management revealed that three key concerns, i.e. relationship, interpersonal and family norms, and collective interest, strongly influence the selection of conflict management styles (Yan and Sorenson 2004). A DCM approach to organisational management showed that older workers exhibit strengths in applying constructive conflict management strategies and demonstrate well-developed emotional competence, contributing to effective conflict management (Beitler, Scherer, and Zapf 2018).

While the DCM hasn't been directly studied regarding human compliance, prior research suggests that cooperative and conciliatory conflict resolution styles enhance trust and cooperation, fostering willingness to comply. In contrast, competitive styles may prompt resistance, reducing the likelihood of adherence (Elgoibar, Euwema, and Munduate 2017). The competitive conflict management style is characterised by an approach to a conflict marked by a high concern for one's own interest (in the context of this study higher convenience) while disregarding the interests of others (in this context of this study, higher security). In contrast, the avoiding conflict management style is defined by a lack of interest in both one's own concerns and those of others, indicating neither a focus on security nor convenience (Cai and Fink 2002; Sorenson, Morse, and Savage 1999). Thus, applying the DCM to the context of this study, it is anticipated that a higher approaching style would be associated with increased noncompliance and a preference for convenience. Conversely, due to the lack of interest in the concerns of either side, an increase in avoiding styles should not be linked to changes in noncompliance. This conceptualisation is visually represented in Figure 1.

According to the DCM, the approaching conflict management style is characterised by a high concern for one's own interests while neglecting the interests of others, associated with enhanced privacy risk (Zhang et al. 2017). Individuals with an approaching style are likely to prioritise noncompliance with ISSP. These individuals either seek a balanced solution that satisfies both personal and organisational needs or prioritise personal convenience over organisational security, leading to higher noncompliance levels. In contrast, the avoiding conflict management style is defined by a lack of interest in both one's own concerns and those of others (Cai and Fink 2002; Sorenson, Morse, and Savage 1999), with no implications for the convenience/security conflict (Zhang et al.

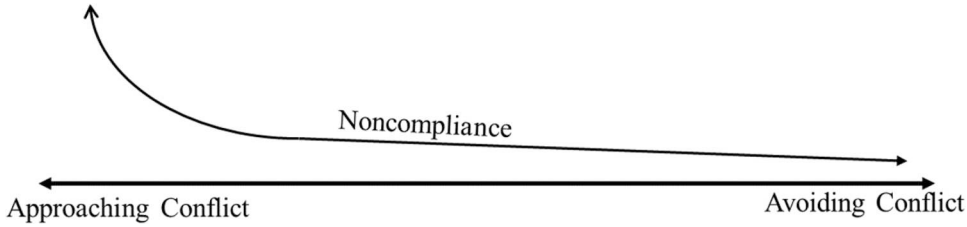

Figure 1. Implementation of the dual-concern model in the current study.

2017). This style is not associated with ISSP noncompliance intention, as these individuals tend to disengage from the conflict altogether rather than actively choosing to comply (prioritise organisational security) or not comply (prioritise personal convenience). Therefore, it is expected that a higher approaching style would be correlated with increased noncompliance. Conversely, due to the lack of interest in the concerns of either side, an elevation in avoiding styles is not expected to be associated with changes in noncompliance. Thus, the following hypotheses are proposed:

H1: A higher level of approaching conflict management style is associated with a higher level of ISSP noncompliance intention.

H2: Avoiding conflict management style is not associated with ISSP noncompliance intention.

2.4. Anxiety in the context of IT use

Anxiety decreases information processing capacity and impairs cognitive system performance concerning mathematic competence, verbal skills, and reasoning abilities (MacLeod 1996). Previously, D'Arcy, Herath, and Shoss (2014) showed that security-related stress, including cognitive overload, task complexity, and uncertainty, affects cognitive rationalisation and increases ISSP noncompliance. Khatib and Barki (2020) proposed that the anxiety and contradiction in the relationship among the different organisational stakeholders influence ISSP noncompliance.

There are different types of anxiety related to online communication, including OCA and DTA. Online communication apprehension is the anxiety one endures during actual or anticipated online communication (Ledbetter 2009). DTA is defined as the fear of working with technology, also known as computer anxiety, technophobia, and technology anxiety (Scott and Rockwell 1997). OCA in organisations causes lower performance among virtual team members and more social-oriented messages than more effective task-oriented messages (Fuller, Vician, and Brown 2016). It also decreases the use of new technologies, especially the more complicated ones (Scott and Timmerman 2005). Previous studies showed that anxiety generally reduces the intention and attitude to use technology and work efficiency and negatively affects security compliance (Hwang et al. 2017). Furthermore, as anxiety has cognitive consequences (D'Arcy, Herath, and Shoss 2014; MacLeod 1996), it is likely that OCA, similar to approaching conflict, divides cognitive resources between dealing with the anxiety-creating situation and making the right ISSP decisions. As such, it is likely to increase the ISSP noncompliance. Therefore, the following hypothesis is proposed:

H3: A higher level of online communication apprehension is associated with a higher level of ISSP noncompliance intention.

Also, DTA affects the decisions and perceptions of technology use (Celik and Yesilyurt 2013). The effect of DTA on ISSP compliance has yet to be studied, but similar constructs, such as security system anxiety, showed a decreasing influence on ISSP compliance in organisational settings (Hwang et al. 2017). Previous studies showed that DTA negatively correlates with computer self-efficacy, computer knowledge, math and logic skills, attitude toward computers, and perceived ease and usefulness of computer use (Powell 2013). Therefore, DTA has cognitive effects and is likely to impact the proper security decision-making in online communication. Accordingly, the following hypothesis is proposed:

H4: A higher level of digital technology anxiety is associated with a higher level of ISSP noncompliance intention.

2.5. Technical skills

Technical competence is the cognitive ability to solve issues and problems related to using technology (Nwokeji et al. 2019). In working with mobile technology, expertise and technical skills are integral to organising

and decision-making (Verhulst and Rutkowski 2018). In this study, the extent of technical skills refers to individuals' proficiency in fundamental IT and IT security concepts, such as advanced search, PDF, spyware, wiki, cache, and phishing. These skills are important as they are essential for effectively managing security in online communication. Previous studies showed that technical skills are associated with ISSP compliance (Chen and Benusa 2017; Vance, Siponen, and Pahnila 2012). Technical skills, especially in cases of higher cognitive overload, facilitate the mental shortcuts one could take to process information, for example, via heuristics and habitual patterns (Sundar 2008; Vishwanath 2016). The heuristic facilitates online information processing via already memorised judgmental rules that function as mental shortcuts and cues to make online information processing more feasible (Sundar 2008), and habitual patterns reduce the need for constant effortful attention (LaRose 2010). In dealing with high-risk situations, individuals make decisions not only by cost–benefit analysis but also using previous experiences and pattern recognitions (Okoli et al. 2016), such as their technical skills (Rosen, Shuffler, and Salas 2010). Importantly, previous research suggests that experts, when relying on heuristics, may sometimes struggle to leverage their superior knowledge effectively. This reliance can lead to cognitive biases, resulting in incorrect judgments (Hinds 1999). Therefore, technical skills are proposed to negatively impact ISSP compliance, and we propose the following hypothesis:

H5a: A higher level of technical skills is associated with a higher level of ISSP noncompliance intention.

Furthermore, we propose that technical skills moderate the impact of conflict management styles on noncompliance with ISSP. Employees with higher technical skills are more likely to use heuristics. Using heuristics can reinforce existing cognitive patterns and biases (Kahneman 2011). Heuristics simplify decision-making processes, leading individuals to rely more on ingrained cognitive frameworks. Consequently, these employees might exhibit more pronounced behaviours aligned with their established conflict management styles. Therefore, we hypothesise that high technical skills amplify behaviours associated with conflict management styles. We previously hypothesised that the approaching style increases noncompliance with ISSP. Using heuristics (i.e. employees with high technical skills) should intensify this behaviour. Hence, we propose:

H5b: Approaching conflict management enhances ISSP noncompliance intention more when technical skills are high (as compared to low)

Further, we theorised that avoidance style alone does not significantly alter ISSP compliance, due to a lack of interest in one's own or the other party's interests. However, we argue that the use of heuristics in conjunction with avoidance style can trigger these behaviours. Therefore, we propose the following hypothesis:

H5c: Avoiding conflict management style enhances ISSP noncompliance intention more when technical skills are high (as compared to low).

Next, we propose that technical skills moderate the impact of anxiety on noncompliance with ISSP. As previously argued, anxiety can impair cognitive abilities and decision-making in the context of ISSP (Hwang et al. 2017). When employees with high technical skills rely on heuristics, the combination of anxiety and heuristic use can further undermine their ability to make sound judgments, such as adhering to ISSP requirements. Thus, we propose the following hypothesis:

H5d: Online communication apprehension enhances ISSP noncompliance intention more when technical skills are high (as compared to low).

H5e: Digital technology anxiety enhances ISSP noncompliance intention more when technical skills are high (as compared to low).

2.6. Age

This study will control for the impact of age on making proper ISSP decisions. Human cognitive ability increases with aging to its peak in the mid-thirties (Germine, Duchaine, and Nakayama 2011). Previous studies investigated the impact of age on ISSP compliance in the organisational and instructional context and found mixed results of no effect (Siponen and Vance 2010), and significant correlation (Nord et al. 2020). Previously, Clarke et al. (2020) showed that middle-aged users are more concerned with computer security than younger and senior users while communicating their healthcare information. Studies of medical compliance among patients with type 2 diabetes showed that younger age is correlated with a higher possibility of noncompliance because the importance of adherence at a younger age is not immediately understood (Yang et al. 2009). Thus, the following hypothesis is proposed:

H6: Higher age decreases the intention of noncompliance with ISSP.

Figure 2 depicts the model incorporating the study propositions and hypotheses.

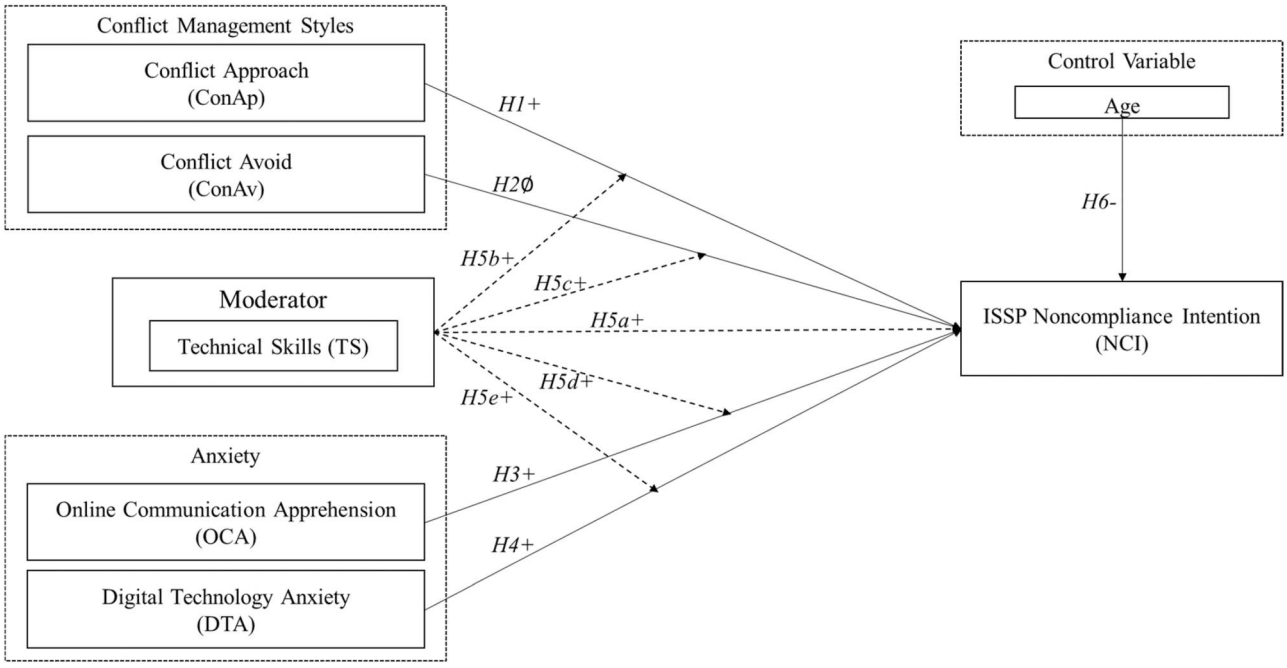

Figure 2. The theoretical model of the study.

3. Method

3.1. Participants

After obtaining approval from the ethics committee, we invited individuals to voluntarily participate in the study. The recruitment process involved utilising the services of Qualtrics, a reputable international panel data company. Participants themselves decided to take part in the study and were provided with online survey questionnaires, which included Likert-type scales. The surveys were accessible on various platforms, such as PCs, tablets, and smartphones. To ensure data quality, Qualtrics conducted checks to exclude participants who exhibited excessive response speed or demonstrated straight-lining behaviour. As a result, we obtained a complete sample of 395 participants who successfully completed the survey. Subsequently, to establish multivariate normality, 4 outliers were removed, and 391 participants were retained for data analysis (Males = 116 (29.6%), Females = 274 (70.1%), other = 1 (<1%), 18 ≤ age ≥79, M_{age} = 37.79, SD_{age} = 13.8). During data collection, Qualtrics continued the process until the required quota of quality participants was achieved. Previous research showed Qualtrics is a reliable method of data collection when demographic variability is sought (Boas, Christenson, and Glick 2020). Upon completing the questionnaire, participants received financial incentives from the company. Participants also answered questions about their highest-achieved educational degree. Engagement in online communication was the inclusion criterion for this study. A summary of the participant's demographic information is presented in Table 1.

3.2. Measurements

3.2.1. Conflict management style

Conflict management styles were measured using a two-dimensional 16-item Likert-type scale of the Attitude Toward Conflict Scale (ATCS) developed by Bresnahan et al. (2009), ranging from (1) Strongly disagree to (7) strongly agree. ATCS has two factors: approaching conflicts (9 items) and avoiding conflict (7 items). An example of the statements in approaching conflicts is, 'I believe conflict is healthy because it forces people to face their problems'. An example of the statements in

Table 1. Demographic information of the sample.

Variable		*N* (391)	%	M	SD	Min	Max
Age				37.79	13.8	18	79
Age groups	18–29	128	32.7				
	30–39	117	29.9				
	40–49	65	16.7				
	50 and above	81	20.7				
Gender	Female	274	70.1				
	Male	116	29.6				
	Other	1	0.3				
Education	lower than HD	9	2.3				
	HD	160	40.9				
	Bachelor	161	41.2				
	Master	50	12.8				
	Doctorate	11	2.8				

Note: HD: High school diploma.

avoiding conflict is, 'I usually avoid open discussion of my differences with others'.

3.2.2. OCA

OCA was measured using a unidimensional 8-item Likert-type scale of Measure of Online Communication Attitude (MOCA) developed by Ledbetter (2009), ranging from (1) Strongly disagree to (7) strongly agree. An example of the statements used in this scale is 'I feel awkward when communicating online'.

3.2.3. DTA

DTA was measured using 8 items of the adapted format of the Computer Anxiety Scale (CAS), which is a Likert-type scale developed by Cohen and Waugh (1989), ranging from (1) strongly disagree to (7) strongly agree with items like 'I feel anxious whenever am using smartphones'.

3.2.4. Technical skills

Technical skill was measured using a unidimensional 6-item Likert-type scale of Web-Use Skills developed by Hargittai and Hsieh (2012) that asked the participants to evaluate their knowledge of advanced search, PDF, spyware, wiki, cache, and phishing ranging from (1) not familiar at all to (5) extremely familiar.

3.2.5. Noncompliance intention

Noncompliance intention was measured using a unidimensional 2-item Likert-type scale developed by Piquero and Piquero (2006), ranging from (1) Strongly disagree to (7) strongly agree. The participants were asked to indicate their intention to follow a hypothetical scenario where a gender-neutrally named person (Casey) commits one of the three major ISSP violations (Hur and Shamsi 2017; Kaspersky), namely insecure WiFi connection, insecure application installation, and insecure smartphone password. Following Moody, Siponen, and Pahnila (2018), several Ph.D. academics in a business school at a New Zealand university were consulted to prepare the scenarios. As Siponen and Vance (2010) suggested, noncompliance intention was measured after a consensus over the relevance, realism, and readability of the scenarios was achieved. The data collection platform used in this study randomly ascribed each scenario to one-third of the participants. Using scenarios instead of a direct question of intention to noncompliance allows (a) indirect measurement of unethical or socially undesirable behaviours or intentions such as violation of ISSP, (b) incorporation of important decision-making situational details, and (c) prospective measurement of unethical or socially undesirable behaviours or intentions, such as violation of ISSP (Siponen and Vance 2010). An example of the statements used in this scale is 'There is a high chance that I would do what Casey did in the described scenario'.

4. Analysis

The data analysis process involved several steps. Firstly, the normal distribution of the data was examined to ensure its suitability for further analysis. Next, Confirmatory Factor Analysis (CFA) was conducted to validate the measurements employed in the study. Structural Equation Modeling (SEM) was employed to assess the relationships among the variables. SEM is a statistical technique for modelling complex relationships between observed variables and latent constructs (Byrne 2010). CFA and SEM analyses were performed using IBM SPSS AMOS Graphics software, specifically version 27, which provided the user-friendly implementation of advanced SEM analyses. AMOS enhances SEM by delivering more precise analysis for models with multiple dependent and mediating variables, surpassing the capabilities of standard multivariate statistical methods (Do-Thi and Do 2022).

4.1. Measurement validation

A test of normality by investigating skewness and kurtosis of the items was performed using IBM SPSS statistics 27, which did not reveal any item exceeding the ±2.2 threshold, indicating a normal distribution of data (Sposito, Hand, and Skarpness 1983). Furthermore, to ensure the multivariate normal distribution, Mahalanobis' distance test was run using SPSS statistics 27, which yielded a maximum amount of 29.08. The critical Chi-square value for the degree of freedom = 5 and p = .001 is 20.52, and 4 outliers with Mahalanobis distances exceeding this critical number were removed from the sample (Tugtekin and Koc 2020). A subsequent Mahalanobis' distance test yielded an acceptable maximum amount of 18.72.

The factorial structure of the initial model was assessed using Confirmatory Factor Analysis (CFA). However, the results showed an unsatisfactory fit for the model, as indicated by the following statistics: $\chi^2(687) = 1648.95$ (chi-square statistic), $p < .001$, CFI = .89 (Comparative Fit Index), SRMR = .07 (Standardised Root Mean Square Residual), RMSEA = .06 (Root Mean Square Error of Approximation), and PClose = .000 (p-value for the RMSEA test of close fit). The CFA statistics were compared against the established thresholds for model fit, where excellent fit is indicated by CMIN/DF between 1 and 3, CFI > 0.95,

SRMR < 0.08, RMSEA < 0.06, and PClose > 0.05. Alternatively, an acceptable fit falls within the range of CMIN/DF between 3 and 5, CFI between .90 and .95, SRMR between .08 and .1, RMSEA between .06 and .08, and PClose between .01 and .05 (Hu and Bentler 1999). Based on these criteria, the initial model did not meet the standards for an acceptable or excellent fit. In the CFA stage, we employed Modification Indices (MI) to identify misspecifications in the model and improve model fit. Following Kaplan (1990), who argued for prioritising the removal of potentially significant specification errors, and Sörbom (1989), who highlighted the utility of modification indices in detecting misspecifications, we iteratively removed items with the highest MI. After this iterative process, 6 items from the approaching conflict factor, 4 items from the avoiding conflict factor, and 1 item from the technical skills factor were removed. As a result of these adjustments, an acceptable model fit was achieved (Latent Model), indicating that the retained items effectively captured the underlying constructs in the study: $\chi^2(390) = 815.39$, $p < .001$, CFI = .94, SRMR = .05, RMSEA = .05, PClose = .17.

In order to establish the distinctiveness of the constructs, particularly in light of the relatively high correlation (exceeding .8) between OCA and DTA, we conducted a comparison of models. Specifically, we compared our preferred Latent Model with two alternative models: the Alternative Latent Model and the Single-Factor Latent Model. In the Alternative Latent Model, we combined the items of OCA and DTA to load on a single latent factor. However, this model did not demonstrate an acceptable fit to the data: $\chi^2(395) = 1438.13$, $p < .001$, CFI = .86, SRMR = .06, RMSEA = .08, PClose = .000. Similarly, in the Single-Factor Latent Model, all items were loaded onto the same factor, but this model also yielded a poor fit: $\chi 2(405) = 3449.36$, $p < .001$, CFI = .53, SRMR = .13, RMSEA = .14, PClose = .000. These results indicate the superiority of our preferred latent model, where OCA and DTA are treated as separate and distinct constructs.

We assessed the convergent and discriminant validity, as well as the reliability of the Latent Model. To assess the convergent and discriminant validity, we utilised an AMOS plugin (Gaskin 2019) to compute several validity indicators. These included the Average Variance Extracted (AVE), the Maximum Shared Variance (MSV), the square root of AVE, the maximum likelihood estimation of inter-construct correlation, and the HeteroTrait-MonoTrait Ratio of Correlations (HTMT) for each variable. These measures are essential for evaluating the reliability and distinctiveness of the constructs in the model. AVE amounts higher than .5 indicated that the model has convergent validity (Hair et al. 2014). The discriminant validity of the model was tested and proved as MSV for each construct was less than its correspondent AVE, the square root of AVE for each construct was higher than the inter-construct correlations for it, and the HTMT amounts were less than .85 (Hair et al. 2014; Henseler, Ringle, and Sarstedt 2015). Also, Cronbach α, Composite reliability, and maximum reliability (MaxR(H)) for each factor yielded amounts higher than .70. Thus, the measurement is reliable (Hair et al. 2014). The details of measurement validation tests are presented in Table 2.

Moreover, to address the potential common method bias in our data collected using a single method, we conducted a Common Latent Factor (CLF) test. The CLF test compared the standard estimation weights of the model items with and without CLF. The results indicated that there was no significant item-wise difference (>.20) (Serrano Archimi et al. 2018). Additionally, we examined the latent variable correlations, as presented in Table 3, and found no correlations above .9, which could indicate common method bias (Pavlou, Liang, and Xue 2007).

Furthermore, the Variance inflation factor (VIF) and tolerance statistics were checked to detect collinearity in the data. The VIF statistics were below 5, and the tolerance amounts were over .1, which shows the lack of collinearity in the data (Field 2009). The details of the collinearity test are presented in Table 4.

Also, due to the significant difference in the number of male and female participants, scalar invariance tests of measurement weights, intercepts, covariances, and residuals were run. The study models generated from males and females did not significantly differ in measurement weights. Also, after removing the 8 biggest intercept differences and 6 highest residual differences between the models, scalar invariances of the intercepts, covariances, and residuals were established. Thus, the study results were not significantly affected by the difference in the gender composition of the sample. The details of scalar invariance tests are presented in Table 3.

4.2. Path model analysis

In this study, the regression-weighted factors for approaching conflict, avoiding conflict, OCA, technical skills, and DTA were computed. Additionally, age was included as a control variable in the model. Furthermore, the interactions of technical skills with approaching conflict, avoiding conflict, OCA, and DTA were added as additional exogenous variables. The dependent variable in the model was Noncompliance Intention (NCI). Structural equation modelling was used to

Table 2. Validity and invariance measurements of the study models.

	Model invariance tests						
	CMIN	DF	CMIN/DF	CFI	SRMR	RMSEA	PClose
Initial Model	1648.50***	687	2.40	0.89	0.07	0.06	0.00
Alternative Latent Model	1438.13***	395	3.64	0.86	0.06	0.08	0.00
Single-Factor Latent Model	3449.36***	405	8.52	0.53	0.13	0.14	0.00
Latent Model	815.39***	390	2.09	0.94	0.05	0.05	0.17
Path Model	86.01***	19	4.53	0.91	0.11	0.07	0.03

	Construct validity measurements					**√AVE** (on diagonal), Correlations (blow diagonal) & *HTMT Measurements* (above diagonal)					
	α	CR	AVE	MSV	Max(H)	1	2	3	4	5	6
1. DTA	0.94	0.94	0.67	0.63	0.95	**0.82**	*0.80*	*0.01*	*0.11*	*0.20*	*0.34*
2. OCA	0.93	0.93	0.63	0.63	0.94	.79***	**0.80**	*0.02*	*0.21*	*0.20*	*0.34*
3. Technical Skills	0.86	0.86	0.56	0.05	0.87	0.01	−0.01	**0.75**	*0.10*	*0.23*	*0.11*
4. Avoiding Conflict	0.8	0.80	0.51	0.04	0.82	0.07	.19***	−0.1†	**0.71**	*0.17*	*0.06*
5. Approaching Conflict	0.75	0.75	0.50	0.07	0.76	.19***	.20***	.22***	−.17**	**0.71**	*0.28*
6. NCI	0.92	0.92	0.85	0.12	0.96	.34***	.35***	0.13*	0.03	.27***	**0.92**

	Scalar invariance tests		
	CMIN	DF	*p*
Measurement weights	26.90	30	0.63
Measurement intercepts	68.49	52	0.06
Structural covariances	82.71	67	0.09
Measurement Residuals	114.22	91	0.05

Note: CMIN: Minimum Discrepancy; DF: Degree of Freedom; CFI: Comparative Fit Index; SRMR: Standard Root Mean Square Residual; RMSEA: Root Mean Square Error of Approximation; PClose: Probability of Close fit; DTA: Digital Technology Anxiety; OCA: Online Communication Apprehension; NCI: Noncompliance Intention; SQR: Square Root; AVE: Average Variance Extracted; α: Cronbach's Alpha; CR: Construct Reliability; MSV: Maximum Shared Variance; MaxR(H): Maximum Reliability; HTMT: HeteroTrait-MonoTrait Ratio of Correlations; †: $p < .1$; *: $p < .05$; **: $p < .01$; ***: $p < .001$.

analyze the resulted path model. To assess the assumption of homoskedasticity and ensure valid regression results, the White Test for Heteroskedasticity was conducted (White 1980). The test revealed significant heteroskedasticity in the model ($\chi^2(55) = 105.50$, $p < .001$), indicating that the assumption of constant variance of errors in ordinary least squares (OLS) regression was violated. To address this issue, Generalized Least Squares (GLS) estimates were employed for the path model analysis, providing more robust and accurate estimates when dealing with heteroskedastic data (Wooldridge 2016). Using GLS aimed to obtain more reliable and efficient estimates, reducing potential bias introduced by heteroskedasticity and improving the validity of the findings. The path model showed an acceptable fitness, $\chi^2(19) = 86.01$, $p < .001$, CFI = .91, SRMR = .11, RMSEA = .07, PClose = .03. The GLS analysis results are presented in Table 5.

5. Findings

The data analysis revealed that the approaching conflict management style exhibited a positive association with ISSP noncompliance intention ($\beta = .21$, $p < .001$), supporting *H1*. However, the avoiding conflict management style did not significantly influence noncompliance intention ($\beta = .06$, $p > .05$), leading to the non-support of *H2*. Moreover, the study found a positive correlation between a higher level of OCA and noncompliance intention ($\beta = .15$, $p < .05$), providing support for *H3*. On the other hand, the effect of DTA on noncompliance intention was found to be marginally significant ($\beta = .13$, $p = .088$), partially supporting *H4*. Additionally, the analysis indicated that higher levels of technical skills were not significantly correlated with noncompliance intention ($\beta = .08$, $p > .05$).

The results of the study suggest that, with the exception of the interaction between technical skills and

Table 3. Means, standard deviations, and two-tailed Pearson correlations.

	N	Mean	SD	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1) Digital Technology Anxiety	391	1.73	.97							
(2) Online Communication Apprehension	391	2.00	.96	.81**						
(3) Technical Skills	391	3.03	.93	.01	−.01					
(4) Avoiding Conflict	391	3.61	.91	.09	.21**	−.11*				
(5) Approaching Conflict	391	3.48	.88	.23**	.22**	.27**	−.20**			
(6) ISSP Noncompliance Intention	391	2.16	.98	.35**	.36**	.14**	.04	.31**		
(7) Age	391	37.80	13.80	−.13**	−.12*	−.14**	.09	−.07	−.18**	
(8) Gender	391	1.71	.46	−.16**	−.08	−.13**	.20**	−.11*	−.12*	−.02

Note: **: $p < .01$, *: $p < .05$.

Table 4. Collinearity statistics.

	Tolerance	VIF
Conflict Approach	0.83	1.21
Conflict Avoidance	0.88	1.14
Technical Skill	0.92	1.09
Online Communication Apprehension	0.32	3.17
Digital Technology Apprehension	0.33	3.00

Dependent Variable: ISSP Noncompliance Intention.

avoiding conflict management style, which shows marginal significance at $p < .1$, there is no statistically significant moderation effect in the model for the interactions of technical skills with approaching conflict ($\beta = .05$, $p > .05$), avoiding conflict ($\beta = -.05$, $p > .05$), OCA ($\beta = .10$, $p > .05$), and DTA ($\beta = -.06$, $p > .05$). Despite the lack of statistical significance in most cases, we decided to further investigate the interaction effects by employing two-way interaction plots, as shown in Figure 3. Incorporating estimation graphics alongside traditional statistical tests enhances data comprehension, aids in identifying treatment effects, and facilitates a more comprehensive analysis of the study (Ho et al. 2019; Wolfe et al. 2019). Interestingly, we observed a crossing line of effect, indicating that technical skills may moderate the relationship between OCA and ISSP noncompliance intention. Consequently, *H5d* is supported, while the remaining hypotheses (*H5a* to *H5e*) were not supported. Getting older has a decreasing correlation with noncompliance intention ($\beta = -.12$, $p < .05$). Thus, H6 is supported. Finally, the presented model could explain 15% of the variance in NCI.

6. Discussion

This research explores the application of the DCM in understanding the relationship between conflict management styles, anxiety, technical skills, and ISSP noncompliance among smartphone users. The study confirmed the applicability of DCM in the context, establishing a positive correlation between approaching conflict and ISSP noncompliance intention while finding no significant association between avoiding conflict and noncompliance intention as hypothesised. Additionally, the study supported the hypothesis of a significant positive association between OCA and the intention of ISSP noncompliance. However, contrary to expectations, no correlation was found between DTA and noncompliance. Additionally, while higher technical skills are not directly associated with higher ISSP noncompliance intention, they do moderate the correlation between OCA and ISSP noncompliance intention. However, technical skills do not moderate the correlations of either form of conflict management styles or DTA with ISSP noncompliance. These findings align with prior research indicating that competitive behaviour during conflicts can deplete cognitive resources required for decision-making (Carnevale and Probst 1998). Additionally, previous studies have demonstrated that anxiety, in a broader sense, can lead to reduced compliance with ISSP (Hwang et al. 2017). The results have significant theoretical and practical implications for promoting information security compliance among smartphone users.

6.1. Theoretical implications

The application of the DCM in the study is crucial as it validates the theoretical framework within the context of ISSP noncompliance among smartphone users and enhances the overall theoretical robustness of the research. Successfully predicting associations between conflict management styles and ISSP noncompliance provides a structured framework to interpret the observed behaviours. It also offers a deeper understanding of why certain styles, such as approaching conflict, are positively correlated with noncompliance, while others, like avoiding conflict, may not show significant associations. This validation contributes to the advancement of knowledge in conflict management literature and offers empirical support for the DCM's utility in explaining real-world behaviours related to ISSP noncompliance. The findings also have implications for

Table 5. Summary of study findings.

Proposition	Research Finding	Path	Unstandardized Estimate	Standardised Estimate	*p*
H1	Supported	ConAp* → NCI	0.24	0.21	<.001
H2	Supported	ConAv → NCI	0.06	0.06	0.252
H3	Supported	OCA → NCI	0.17	0.15	0.046
H4	Not Supported	DTA → NCI	0.14	0.13	0.088
H5a	Not Supported	TS → NCI	0.08	0.08	0.108
H5b	Not Supported	TS *x* ConAp → NCI	0.04	0.05	0.389
H5c	Not Supported	TS *x* ConAv → NCI	−0.05	−0.05	0.362
H5d	Visually Supported**	TS *x* OCA → NCI	0.10	0.10	0.241
H5e	Not Supported	TS *x* DTA → NCI	−0.06	−0.06	0.486
H6	Supported	Age → NCI	−0.01	−0.12	0.012

Note: * ConAp: Approaching Conflict Management Style; ConAv: Avoiding Conflict Management Style; DTA: Digital Technology Anxiety; OCA: Online Communication Apprehension; NCI: Noncompliance Intention; TS: Technical Skills; ** Supported via visual analysis of the two-way interaction plot in Figure 3.

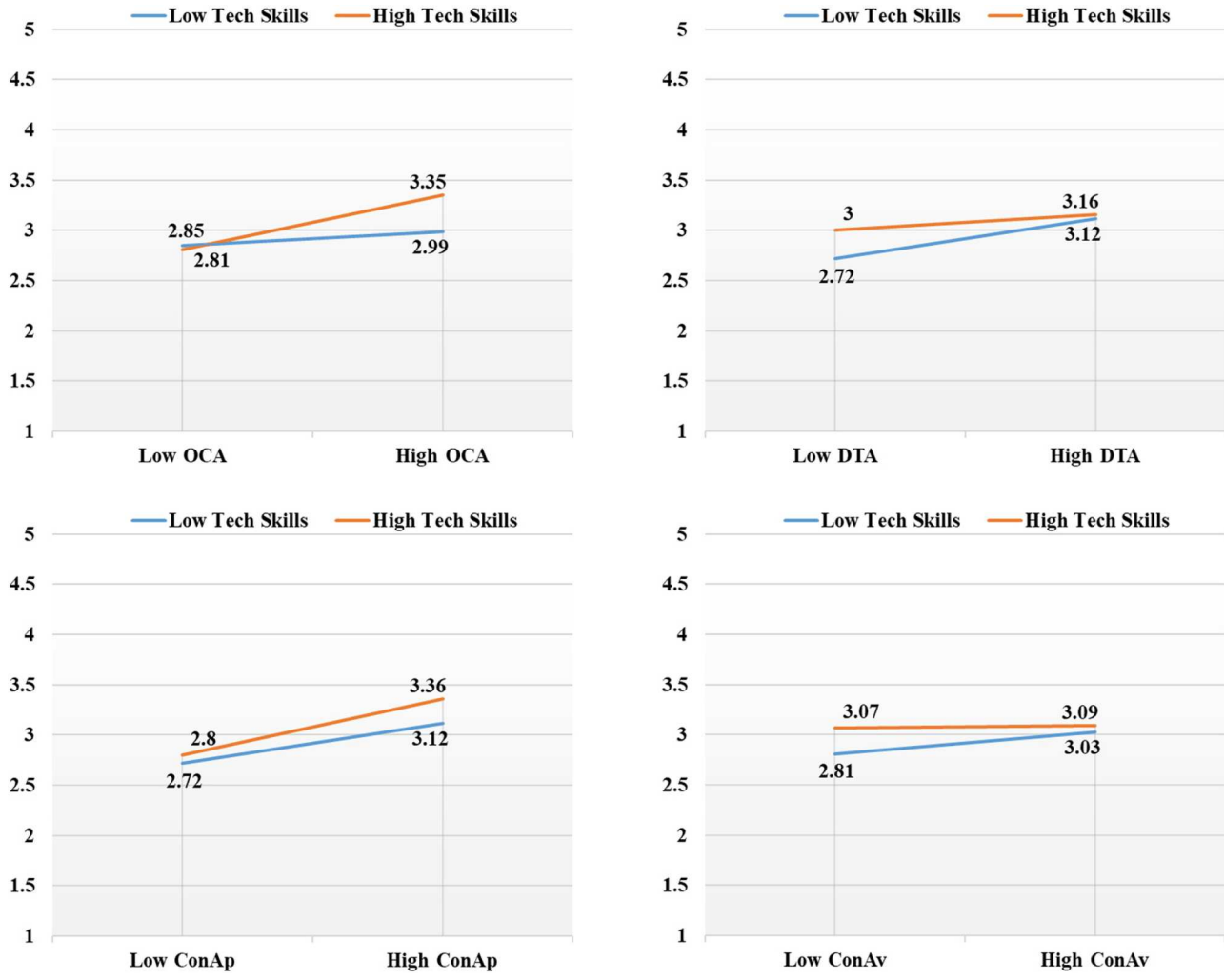

Figure 3. Two-way interaction plots.

Note: OCA: Online Communication Apprehension; ConAv: Conflict Avoidance; ConAp: Conflict Approach; DTA: Digital Technology Anxiety.

future research and interventions targeting noncompliance issues in this specific domain.

The study's first two hypotheses aimed to explore the relationship between conflict management styles and ISSP noncompliance intention. The analysis provided support for both hypotheses (*H1*), indicating a positive association between approaching conflict and ISSP noncompliance intention, and (*H2*) proposing no association between avoiding conflict and noncompliance intention. A plausible explanation for these findings could suggest that the cognitive engagement and focus required during conflicts prevent individuals from fully comprehending the potential risks associated with noncompliance. Also, these findings may highlight that individuals' perceptions of security risks could be influenced differently depending on their conflict management styles. This could impact their ISSP compliance intentions. This is in line with the previous research showing that individual characteristics and traits could influence decision-making in conflict management (Carnevale and Probst 1998; Köther et al. 2021; Wu et al. 2022). Previous research suggests conflict management styles influence how individuals perceive and react to security-related conflicts (Barki and Hartwick 2001; Moody and Siponen 2013; Moody, Siponen, and Pahnila 2018; Siponen and Vance 2010).

Furthermore, these findings affirm the relevance of the DCM within the study's context. DCM proposes that various conflict management styles could be defined as the interaction of two forms of concern for one's own interest and for another's interest (Elgoibar, Euwema, and Munduate 2017). According to DCM, the approaching conflict management style, characterised by a heightened concern for one's own interest and a lack of interest in others' concerns, here translated as a preference for convenience over security. Conversely, individuals favouring the avoiding conflict management style, as per the DCM, passively evade

conflict without consideration for either party's concerns, making them indifferent to adhering to higher security compliance or the convenience of noncompliance (Cai and Fink 2002; Sorenson, Morse, and Savage 1999). This finding underscores the significance of cognitive processes in shaping organisations' ISSPs. A shift in employees' perception of what constitutes their interests and prioritising security over convenience may motivate compliance with ISSP for personal benefits, mitigating potential risks to both personal devices and organisational security. A preceding study indicated that variations in the perception of security risks contribute to differences in noncompliance with ISSPs (Pham, El-Den, and Richardson 2016).

Our study's third and fourth hypotheses proposed that there would be a positive association between OCA and DTA with ISSP noncompliance intention. The analysis indeed supported the third and refused the fourth hypothesis, indicating that OCA plays a significant role in increasing the risk of ISSP noncompliance intention. This finding is in line with previous research showing that OCA can have cognitive effects (Brown, Fuller, and Vician 2004) and the counterproductive behaviour studies emphasising that stress and anxiety lead to information overload in decision-making (Klotz and Buckley 2013) and lead to negative emotions and consequently to counterproductive behaviours (Fox, Spector, and Miles 2001).

The divergence in associations between OCA and DTA with noncompliance among smartphone users may stem from the nuanced nature of these psychological factors. OCA taps into individuals' discomfort or unease in engaging with others through digital platforms, which could directly impact their willingness to comply with ISSP (Ledbetter 2009). This apprehension might be rooted in concerns about potential conflicts, negative interactions, or misunderstandings in the online realm. On the other hand, DTA centres more on a general discomfort or fear related to using technology (Scott and Rockwell 1997) but is not necessarily tied to specific interpersonal interactions or security-related considerations. Individuals with DTA may harbour concerns about their ability to effectively use technology rather than experiencing apprehension about the social dynamics within the online space. Moreover, this finding may indicate that, for smartphone users, concerns about technology use do not directly translate into noncompliant behaviour with ISSPs. This could suggest that, while users may have reservations about technology use, these concerns might not extend to intentional violations of security protocols.

This finding underscores the significance of the social and psychological dimensions of ISSP within organisations, aligning with previous research advocating for a holistic understanding of these aspects. Previous research emphasised the importance of more effective ISSP compliance approaches that move away from sanction and fear-based models and advocated for systems that combine employees' personal resources with organisational resources and appropriate security demands (Pham, El-Den, and Richardson 2016). In such systems that prioritise employee engagement and provide adequate resources while minimising burnout and overload, employees experience enhanced self-control and autonomy in complying with ISSP (D'Arcy, Herath, and Shoss 2014; Vance, Siponen, and Pahnila 2012). This aspect becomes even more critical in the case of personal devices, where most ISSP activities are performed by employees themselves without the support of IT services in organisations.

In the fifth hypothesis, we explored the potential influence of technical skills on the relationships between anxiety, conflict management styles, and ISSP noncompliance intention. The analysis revealed that technical skills only mediate the association between OCA and ISSP noncompliance intention. Specifically, individuals with high technical skills are more likely to exhibit noncompliance intention with ISSP when they experience higher levels of OCA. This could be attributed to overwhelming technology options, fear of misusing technology, perceived expectations, technological complexity, cybersecurity concerns, social anxiety, and contextual factors, which may lead to cognitive overloading, distraction, and noncompliance intention. However, more research is needed to investigate these possible reasons. This finding emphasises the importance of vigilance in online interactions, especially among those relying on their technical skills to avoid online security risks.

Hypothesis 6 examined the association of age with ISSP noncompliance. The study found a negative impact of age on noncompliance intention, which further supports the idea that cognitive resources may be affected when dealing with conflicting and stressful situations. Previous research has shown that cognitive competence typically peaks in the mid-30 s (Germine, Duchaine, and Nakayama 2011). Given that 62.6% of the participants in this study were between 18 and 39 years old, it is likely that older users with more developed cognitive abilities make less risky decisions regarding information security. Future studies could delve deeper into the relationship between age and noncompliance intention in the context of ISSP. Understanding how age influences users' decision-making processes can provide valuable insights for improving information security practices.

6.2. Practical implications

The findings of this study offer a spectrum of implications and insights for organisations seeking to address the potential occurrence of security noncompliance behaviours among employees using personal mobile phones for work-related tasks. The results underscore the significance of adopting a comprehensive perspective on personal device security, one that factors in the psychological and individual attributes of technology users. This approach advocates for acknowledging the diverse functionalities inherent in technology and recognising the distinct personal outcomes arising from its utilisation. As organisations navigate the complexities of personal device security, integrating this multifaceted understanding can pave the way for more effective strategies and policies.

First, our results demonstrated a connection between individuals' style of conflict management and their likelihood to engage in noncompliant security behaviours. We unveil a substantial link between individuals who adopt an 'approaching conflict' style – characterised by assertively addressing conflicts – and their heightened likelihood of demonstrating noncompliant security behaviours while using personal mobile devices at work. In view of these findings, managers and organisational leaders are advised to incorporate conflict resolution training within cybersecurity awareness programmes. Such training should empower employees with constructive conflict management skills, enabling them to address security concerns assertively and collaborate effectively. By nurturing a workplace environment that encourages open discourse and equips employees with conflict-resolution competencies, managers can foster both a culture of security compliance and productive conflict engagement.

Second, our results highlighted the significant role of anxiety – characterised by the instantiation of OCA in the context of our study – in the propensity to engage in noncompliant security intentions. The findings underscored that managers and organisational leaders should recognise the pivotal role of OCA in shaping employees' security intentions. To mitigate the potential increase in noncompliant security behaviours driven by OCA, managers can implement multifaceted strategies. These may include tailored training programmes that not only enhance employees' cybersecurity skills but also provide guidance on effective and secure online communication practices, fostering a sense of familiarity and confidence. Furthermore, cultivating an open and non-punitive organisational culture that encourages individuals to voice their communication apprehension and seek assistance can contribute to reducing the likelihood of noncompliant security actions. By addressing the psychological barriers posed by communication apprehension, managers can cultivate a more resilient cybersecurity posture while nurturing a workforce that is both technically adept and psychologically equipped to navigate secure online environments.

Finally, contrary to prevailing assumptions, our empirical analysis challenges the conventional wisdom that higher levels of technical proficiency inherently lead to greater adherence to secure behaviours. We found that the level of technical skills alone exhibits no discernible impact (direct or indirect) on staff members' inclination to undertake noncompliant security actions. This unexpected outcome underscores the multifaceted nature of cybersecurity attitudes and highlights the significance of psychological, cultural, and organisational factors that may significantly influence security intentions beyond mere technical competence. Managers and organisational leaders are advised to adopt a more nuanced approach to enhancing cybersecurity practices among staff members. While technical training remains essential in any situation, it is imperative to recognise that fostering a secure organisational culture goes beyond technical skills alone. Managers should prioritise non-technical initiatives such as emphasising the importance of shared responsibility, clear communication of security policies, and the alignment of security goals with broader organisational objectives.

7. Future areas of research

The study's outcomes pave the way for future research to further explore and build upon the insights gained with specific considerations. Firstly, while DCM studies have identified five distinct conflict management styles, this investigation solely focuses on two of these styles. Future research should consider incorporating a broader range of conflict management styles to offer a more comprehensive understanding of this theoretical framework. Second, the overall explained amount of variance in the dependent variable and the impact size of independent variables are relatively small. Thus, it is likely that other constructs not included in this study have more significant impacts on NCI. For example, Technostress defined as

> the phenomenon of stress experienced by end users in organizations as a result of their use of ICTs […] caused by an individual's attempts to deal with constantly evolving ICTs and the changing physical, social, and cognitive responses demanded by their use (Ragu-Nathan et al. 2008, 417–418)

might have an impact of noncompliance in the context of BYOD. Third, the scope of our conclusion on the effect of habits on IS decision-making is limited, as technical skills are a specific type of habit. Habits could also include other behaviours that are independent of technical skills independent behaviours. Broader future studies on the role of habits in ISSP implantation could further develop this finding. Fourth, there are specific constraints related to the cross-sectional self-report survey-based research. Common method variance may inflate correlations among variables despite our efforts to mitigate it through robust survey design and statistical controls. The reliance on self-reported measures introduces limitations, with respondents referring to hypothetical rather than actual behaviour. Additionally, the study lacks data on actual mobile phone use at work, specific job roles, and organisational policies, limiting the contextualisation of our findings within the organisational landscape.

8. Conclusion

Motivated by the importance of managing the cybersecurity risks associated with using personal mobile devices, this study delved into the intricate interplay between individual psychological attributes of conflict management styles and anxiety, technical skills, and noncompliance intentions within the realm of personal mobile device usage. The insights garnered shed light on the multifaceted dynamics that influence employees' ISSP decisions. This study reveals the nuanced relationship between psychological attributes, conflict management styles, anxiety, technical skills, and noncompliance intentions in the context of using personal mobile devices for work tasks. The findings underscore the importance of conflict resolution training to address noncompliance driven by an 'approaching conflict' style. They emphasise the need for training that alleviates communication apprehension and promotes secure online practices to mitigate the impact of anxiety. Surprisingly, technical skills alone do not significantly influence noncompliance intentions, emphasising the need for a comprehensive approach that includes cultural and organisational aspects. Overall, this research provides insights that can guide organisations in fostering secure behaviours and building a resilient cybersecurity culture in the age of digital connectivity.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Diyako Rahmani http://orcid.org/0000-0003-1230-7758
Hamed Jafarzadeh http://orcid.org/0000-0001-9880-5496
Alexandra Claudia Hess http://orcid.org/0000-0003-1889-9539

References

Abraham, S., and I. N. Chengalur-Smith. 2011. *The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective*. Detroit, MI: Americas Conference on Information Systems.

Aguboshim, F. C., and J. I. Udobi. 2019. "Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD)." *Information Technology (IT)* 9 (1). https://doi.org/10.7176/JIEA/8-1-07.

Albrechtsen, E. 2007. "A Qualitative Study of Users' View on Information Security." *Computers & Security* 26 (4): 276–289. https://doi.org/10.1016/j.cose.2006.11.004.

Amankwa, E., M. Loock, and E. Kritzinger. 2018. "Establishing Information Security Policy Compliance Culture in Organizations." *Information & Computer Security* 26 (4): 420–436. https://doi.org/10.1108/ICS-09-2017-0063.

Awadallah, E. 2018. "Auditor-client Negotiations: Applying the Dual Concerns Model in an Emerging Economy." *International Journal of Managerial and Financial Accounting* 10 (3): 250–272. https://doi.org/10.1504/IJMFA.2018.093497.

Ayub, N., M. AlQurashi Suzan, A. Al-Yafi Wafa, and K. Jehn. 2017. "Personality Traits and Conflict Management Styles in Predicting Job Performance and Conflict." *International Journal of Conflict Management* 28 (5): 671–694. https://doi.org/10.1108/IJCMA-12-2016-0105.

Balozian, P., D. Leidner, and B. Xue. 2022. "Toward an Intellectual Capital Cyber Security Theory: Insights from Lebanon." *Journal of Intellectual Capital* 23 (6): 1328–1347. https://doi.org/10.1108/JIC-05-2021-0123.

Bar-Tal, D., A. W. Kruglanski, and Y. Klar. 1989. "Conflict Termination: An Epistemological Analysis of International Cases." *Political Psychology* 10 (2): 233–255. https://doi.org/10.2307/3791646.

Barki, H., and J. Hartwick. 2001. "Interpersonal Conflict and its Management in Information System Development." *MIS Quarterly* 25 (2): 195–228. https://doi.org/10.2307/3250929.

Bauer, S., E. W. N. Bernroider, and K. Chudzikowski. 2017. "Prevention is Better than Cure! Designing Information Security Awareness Programs to Overcome Users' Noncompliance with Information Security Policies in Banks." *Computers & Security* 68:145–159. https://doi.org/10.1016/j.cose.2017.04.009.

Beitler, L. A., S. Scherer, and D. Zapf. 2018. "Interpersonal Conflict at Work: Age and Emotional Competence Differences in Conflict Management." *Organizational Psychology Review* 8 (4): 195–227. https://doi.org/10.1177/2041386618808346.

Boas, T. C., D. P. Christenson, and D. M. Glick. 2020. "Recruiting Large Online Samples in the United States and India: Facebook, Mechanical Turk, and Qualtrics."

Political Science Research and Methods 8 (2): 232–250. https://doi.org/10.1017/psrm.2018.28.

Bresnahan, M. J., W. A. Donohue, S. M. Shearman, and X. Guan. 2009. "Research Note: Two Measures of Conflict Orientation." *Conflict Resolution Quarterly* 26 (3): 365–379. https://doi.org/10.1002/crq.238.

Brown, S. A., R. M. Fuller, and C. Vician. 2004. "Who's Afraid of the Virtual World? Anxiety and Computer-Mediated Communication." *Journal of the Association for Information Systems* 5 (2): 79–107. https://doi.org/10.17705/1jais.00046.

Byrne, B. M. 2010. *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming*. 2nd ed. New York: Routledge.

Cai, D., and E. Fink. 2002. "Conflict Style Differences between Individualists and Collectivists." *Communication Monographs* 69 (1): 67–87. https://doi.org/10.1080/03637750216536.

Carnevale, P. J., and T. M. Probst. 1998. "Social Values and Social Conflict in Creative Problem Solving and Categorization." *Journal of Personality and Social Psychology* 74 (5): 1300. https://doi.org/10.1037/0022-3514.74.5.1300.

Celik, V., and E. Yesilyurt. 2013. "Attitudes to Technology, Perceived Computer Self-efficacy and Computer Anxiety as Predictors of Computer Supported Education." *Computers & Education* 60 (1): 148–158. https://doi.org/10.1016/j.compedu.2012.06.008.

Cenkci, A. T. 2018. "Leader Power, Conflict Handling Styles, and Subordinate Compliance: A Study on Information Technology Professionals in Turkey." *International Journal of Management and Economics* 54 (1): 18–35. https://doi.org/10.2478/ijme-2018-0003.

Chang, K.-C., and Y. M. Seow. 2019. "Protective Measures and Security Policy Non-compliance Intention: IT Vision Conflict as a Moderator." *Journal of Organizational and End User Computing* 31 (1): 1–21. https://doi.org/10.4018/JOEUC.2019010101.

Chen, J. Q., and A. Benusa. 2017. "Hipaa Security Compliance Challenges: The Case for Small Healthcare Providers." *International Journal of Healthcare Management* 10 (2): 135–146. https://doi.org/10.1080/20479700.2016.1270875.

Chen, H., Y. Li, L. Chen, and J. Yin. 2021. "Understanding Employees' Adoption of the Bring-Your-Own-Device (BYOD): The Roles of Information Security-related Conflict and Fatigue." *Journal of Enterprise Information Management* 34 (3): 770–792. https://doi.org/10.1108/JEIM-10-2019-0318.

Citro, S., J. McGovern, and C. Ryan. 2007. "Conflict Management for Real-time Collaborative Editing in Mobile Replicated Architectures." *ACM International Conference Proceeding Series*.

Clarke, M. A., A. L. Fruhling, M. Sitorius, T. A. Windle, T. L. Bernard, and J. R. Windle. 2020. "Impact of age on Patients' Communication and Technology Preferences in the Era of Meaningful Use: Mixed Methods Study." *Journal of Medical Internet Research* 22 (6): e13470. https://doi.org/10.2196/13470.

Cohen, B. A., and G. W. Waugh. 1989. "Assessing Computer Anxiety." *Psychological Reports* 65 (3): 735–738. https://doi.org/10.2466/pr0.1989.65.3.735.

Cram, W. A., J. G. Proudfoot, and J. D'Arcy. 2021. "When Enough is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue." *Information Systems Journal* 31 (4): 521–549. https://doi.org/10.1111/isj.12319.

D'Arcy, J., T. Herath, and M. K. Shoss. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective." *Journal of Management Information Systems* 31 (2): 285–318. https://doi.org/10.2753/MIS0742-1222310210.

De Dreu, C. K., and L. R. Weingart. 2003. "Task versus Relationship Conflict, Team Performance, and Team Member Satisfaction: A Meta-analysis." *Journal of Applied Psychology* 88 (4): 741–749. https://doi.org/10.1037/0021-9010.88.4.741.

Do-Thi, P., and I. Do. 2022. "Quantitative Methodology: Applied Modeling by Using AMOS (Step-by-step)." In *Intelligent Systems Modeling and Simulation II: Machine Learning, Neural Networks, Efficient Numerical Algorithm and Statistical Methods*, edited by S. A. Abdul Karim, 645–660. Springer International Publishing. https://doi.org/10.1007/978-3-031-04028-3_40.

Doargajudhur, M. S., and P. Dell. 2020. "The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation." *Journal of Computer Information Systems* 60 (6): 518–529. https://doi.org/10.1080/08874417.2018.1543001.

Elgoibar, P., M. Euwema, and L. Munduate. 2017. "Conflict Management." In *Oxford Research Encyclopedia of Psychology*, edited by O. Braddick. Oxford, UK: Oxford University Press.

Field, A. 2009. *Discovering Statistics Using SPSS*. 3rd ed. Los Angeles, CA: Sage.

Fox, S., P. E. Spector, and D. Miles. 2001. "Counterproductive Work Behavior (CWB) in Response to Job Stressors and Organizational Justice: Some Mediator and Moderator Tests for Autonomy and Emotions." *Journal of Vocational Behavior* 59 (3): 291–309. https://doi.org/10.1006/jvbe.2001.1803.

Fuller, R. M., C. M. Vician, and S. A. Brown. 2016. "Longitudinal Effects of Computer-Mediated Communication Anxiety on Interaction in Virtual Teams." *IEEE Transactions on Professional Communication* 59 (3): 166–185. https://doi.org/10.1109/TPC.2016.2583318.

Gaskin, J. 2019. *Plugins*, August 31. Accessed September 16, 2019. from http://statwiki.kolobkreations.com/index.php?title=Plugins.

Germine, L. T., B. Duchaine, and K. Nakayama. 2011. "Where Cognitive Development and Aging Meet: Face Learning Ability Peaks after Age 30." *Cognition* 118 (2): 201–210. https://doi.org/10.1016/j.cognition.2010.11.002.

Golish, T. D. 1999. "Students' Use of Compliance Gaining Strategies with Graduate Teaching Assistants: Examining the Other end of the Power Spectrum." *Communication Quarterly* 47 (1): 12–32. https://doi.org/10.1080/01463379909370121.

Greenberg, J. 2003. *Organizational Behavior: The State of the Science*. 2nd ed. Mahwah, NJ: Lawrence Erlbaum Associates Publishers.

Guerrero, L. K., and M. A. Gross. 2014. "Argumentativeness, Avoidance, Verbal Aggressiveness, and Verbal Benevolence as Predictors of Partner Perceptions of an Individual's Conflict Style." *Negotiation and Conflict Management Research* 7 (2): 99–120. https://doi.org/10.1111/ncmr.12029.

Hadlington, L., M. Popovac, H. Janicke, I. Yevseyeva, and K. I. Jones. 2019. "Exploring the Role of Work Identity and Work Locus of Control in Information Security Awareness." *Computers & Security* 81:41–48. https://doi.org/10.1016/j.cose.2018.10.006.

Hair, J. F., W. C. Black, B. J. Babin, and R. E. Anderson. 2014. *Multivariate Data Analysis*. 7th ed. Upper Saddle River, NJ: Prentice Hall.

Hargittai, E., and Y. P. Hsieh. 2012. "Succinct Survey Measures of Web-use Skills." *Social Science Computer Review* 30 (1): 95–107. https://doi.org/10.1177/0894439310397146.

Hedström, K., E. Kolkowska, F. Karlsson, and J. P. Allen. 2011. "Value Conflicts for Information Security Management." *The Journal of Strategic Information Systems* 20 (4): 373–384. https://doi.org/10.1016/j.jsis.2011.06.001.

Henseler, J., C. M. Ringle, and M. Sarstedt. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling." *Journal of the Academy of Marketing Science* 43 (1): 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Hinds, P. J. 1999. "The Curse of Expertise: The Effects of Expertise and Debiasing Methods on Prediction of Novice Performance." *Journal of Experimental Psychology: Applied* 5 (2): 205–221. https://doi.org/10.1037/1076-898X.5.2.205.

Ho, J., T. Tumkaya, S. Aryal, H. Choi, and A. Claridge-Chang. 2019. "Moving Beyond *P* Values: Data Analysis with Estimation Graphics." *Nature Methods* 16 (7): 565–566. https://doi.org/10.1038/s41592-019-0470-3.

Hu, L. t., and P. M. Bentler. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives." *Structural Equation Modeling: A Multidisciplinary Journal* 6 (1): 1–55. https://doi.org/10.1080/10705519909540118.

Hur, J. B., and J. A. Shamsi. 2017. "A Survey on Security Issues, Vulnerabilities and Attacks in Android Based Smartphone." In *2017 International Conference on Information and Communication Technologies (ICICT)*, 30–31 December.

Hwang, I., D. Kim, T. Kim, and S. Kim. 2017. "Why not Comply with Information Security? An Empirical Approach for the Causes of non-Compliance." *Online Information Review* 41 (1): 2–18. https://doi.org/10.1108/OIR-11-2015-0358.

Ifinedo, P. 2014. "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition." *Information & Management* 51 (1): 69–79. https://doi.org/10.1016/j.im.2013.10.001.

Jaeger, L., A. Eckhardt, and J. Kroenung. 2021. "The Role of Deterrability for the Effect of Multi-level Sanctions on Information Security Policy Compliance: Results of a Multigroup Analysis." *Information & Management* 58 (3): 1–14. https://doi.org/10.1016/j.im.2020.103318.

Kahneman, D. 2011. *Thinking, Fast and Slow*. New York: Macmillan.

Kaplan, D. 1990. "Evaluating and Modifying Covariance Structure Models: A Review and Recommendation." *Multivariate Behavioral Research* 25 (2): 137–155. https://doi.org/10.1207/s15327906mbr2502_1.

Karlsson, F., E. Kolkowska, and J. Petersson. 2022. "Information Security Policy Compliance-eliciting Requirements for a Computerized Software to Support Value-Based Compliance Analysis." *Computers & Security* 114:102578. https://doi.org/10.1016/j.cose.2021.102578.

Kaspersky. *Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store*. https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store.

Khatib, R., and H. Barki. 2020. "An Activity Theory Approach to Information Security non-Compliance." *Information & Computer Security* 28 (4): 485–501. https://doi.org/10.1108/ICS-11-2018-0128.

Khatib, R., and H. Barki. 2022. "How Different Rewards Tend to Influence Employee Non-compliance with Information Security Policies." *Information & Computer Security* 30 (1): 97–116. https://doi.org/10.1108/ICS-01-2021-0008.

Kim, S. S., and Y. J. Kim. 2017. "The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behavior." *Journal of Knowledge Management* 21 (4): 986–1010. https://doi.org/10.1108/JKM-08-2016-0353.

Kling, R. E. 1996. *Computerization and Controversy: Value Conflicts and Social Choices*. 2nd ed. Morgan Kaufmann.

Klotz, A. C., and M. R. Buckley. 2013. "A Historical Perspective of Counterproductive Work Behavior Targeting the Organization." *Journal of Management History* 19 (1): 114–132. https://doi.org/10.1108/17511341311286222.

Kolkowska, E., F. Karlsson, and K. Hedström. 2017. "Towards Analysing the Rationale of Information Security non-Compliance: Devising a Value-based Compliance Analysis Method." *The Journal of Strategic Information Systems* 26 (1): 39–57. https://doi.org/10.1016/j.jsis.2016.08.005.

Köther, A. K., G. W. Alpers, B. Büdenbender, M. Lenhart, M. S. Michel, and M. C. Kriegmair. 2021. "Predicting Decisional Conflict: Anxiety and Depression in Shared Decision Making." *Patient Education and Counseling* 104 (5): 1229–1236. https://doi.org/10.1016/j.pec.2020.10.037.

Kuhn, T., and M. S. Poole. 2000. "Do Conflict Management Styles Affect Group Decision Making? Evidence from a Longitudinal Field Study." *Human Communication Research* 26 (4): 558–590. https://doi.org/10.1111/j.1468-2958.2000.tb00769.x.

LaRose, R. 2010. "The Problem of Media Habits." *Communication Theory* 20 (2): 194–222. https://doi.org/10.1111/j.1468-2885.2010.01360.x.

Ledbetter, A. M. 2009. "Measuring Online Communication Attitude: Instrument Development and Validation." *Communication Monographs* 76 (4): 463–486. https://doi.org/10.1080/03637750903300262.

Lee, C., C. C. Lee, and S. Kim. 2016. "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity." *Computers & Security* 59:60–70. https://doi.org/10.1016/j.cose.2016.02.004.

Lee, E. H., T. Lee, and B.-K. Lee. 2022. "Understanding the Role of new Media Literacy in the Diffusion of Unverified Information During the COVID-19 Pandemic." *New*

Media & Society 24 (9): 14614448221130955. https://doi.org/10.1177/14614448221130955.

Li, X., V. Worm, and P. Xie. 2018. "Towards an Integrative Framework of Conflict-handling Behaviour: Integrating Western and Chinese Perspectives." *Asia Pacific Business Review* 24 (1): 22–36. https://doi.org/10.1080/13602381.2017.1357322.

Lipschultz, J. L., and D. A. Wilder. 2017. "Behavioral Assessment and Treatment of Noncompliance: A Review of the Literature." *Education and Treatment of Children* 40 (2): 263–298. https://doi.org/10.1353/etc.2017.0012.

MacLeod, C. 1996. "Anxiety and Cognitive Processes." In *Cognitive Interference: Theories, Methods and Findings*, edited by I. G. Sarason, G. R. Pierce, and B. R. Sarason, 47–76. New York: Routledge.

Marcus, B., and H. Schuler. 2004. "Antecedents of Counterproductive Behavior at Work: A General Perspective." *Journal of Applied Psychology* 89 (4): 647–660. https://doi.org/10.1037/0021-9010.89.4.647.

Martin, A. J., J. M. Wellen, and M. Grimmer. 2016. "An Eye on Your Work: How Empowerment Affects the Relationship between Electronic Surveillance and Counterproductive Work Behaviours." *The International Journal of Human Resource Management* 27 (21): 2635–2651. https://doi.org/10.1080/09585192.2016.1225313.

McLeod, A., and D. Dolezel. 2022. "Information Security Policy Non-compliance: Can Capitulation Theory Explain User Behaviors?" *Computers & Security* 112:102526. https://doi.org/10.1016/j.cose.2021.102526.

Miller, L. E. 2022. "How Can We Resolve This? Two Classroom Exercises on Conflict Management." *Management Teaching Review* 8 (3): 246–259. https://doi.org/10.1177/23792981221096852.

Moberg, P. J. 2001. "Linking Conflict Strategy to the Five-Factor Model: Theoretical and Empirical Foundations." *International Journal of Conflict Management* 12 (1): 47–68. https://doi.org/10.1108/eb022849.

Moody, G. D., and M. Siponen. 2013. "Using the Theory of Interpersonal Behavior to Explain non-Work-related Personal Use of the Internet at Work." *Information & Management* 50 (6): 322–335. https://doi.org/10.1016/j.im.2013.04.005.

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

Mou, J., J. F. Cohen, A. Bhattacherjee, and J. Kim. 2022. "A Test of Protection Motivation Theory in the Information Security Literature: A Meta-analytic Structural Equation Modeling Approach." *Journal of the Association for Information Systems* 23 (1): 196–236. https://doi.org/10.17705/1jais.00723.

Munde, S. 2024. *Bring Your Own Device (BYOD) Market Research Report Information By Device Outlook (Smartphones, Tablets, Laptops), By End-User (Mid-to-large Sized Businesses, Small Businesses), And By Region (North America, Europe, Asia-Pacific, And Rest Of The World) –Market Forecast Till* 2032. https://www.marketresearchfuture.com/reports/bring-your-own-device-market-1286.

Musenero, L., B. Baroudi, and I. Gunawan. 2021. "Application of Dual Concern Theory in Elucidating Conflict Behavior in Infrastructure Public-private Partnership Projects." *Journal of Construction Engineering and Management* 147 (7): 04021061. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002099.

Nord, J. H., A. Koohang, K. Floyd, and J. Paliszkiewicz. 2020. "Impact of Habits on Information Security Policy Compliance." *Issues in Information Systems* 21 (3): 217–226. https://doi.org/10.48009/3_iis_2020_217-226.

Nwokeji, J. C., R. Stachel, T. Holmes, and R. O. Orji. 2019. "Competencies Required for Developing Computer and Information Systems Curriculum." In *2019 IEEE Frontiers in Education Conference (FIE)*. Covington, KY, USA.

Ogbanufe, O., R. E. Crossler, and D. Biros. 2021. "Exploring Stewardship: A Precursor to Voluntary Security Behaviors." *Computers & Security* 109:102397. https://doi.org/10.1016/j.cose.2021.102397.

Okoli, J., J. Watt, G. Weller, and W. B. L. Wong. 2016. "The Role of Expertise in Dynamic Risk Assessment: A Reflection of the Problem-solving Strategies Used by Experienced Fireground Commanders." *Risk Management* 18 (1): 4–25. https://doi.org/10.1057/rm.2015.20.

Palanisamy, R., A. A. Norman, and M. L. Mat Kiah. 2020. "Byod Policy Compliance: Risks and Strategies in Organizations." *Journal of Computer Information Systems* 62 (1): 61–72. https://doi.org/10.1080/08874417.2019.1703225.

Palanisamy, R., A. A. Norman, and M. L. Mat Kiah. 2024. "Employees' BYOD Security Policy Compliance in the Public Sector." *Journal of Computer Information Systems* 64 (1): 62–77. https://doi.org/10.1080/08874417.2023.2178038.

Parsons, K., D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. 2017. "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies." *Computers & Security* 66:40–51. https://doi.org/10.1016/j.cose.2017.01.004.

Pavlou, P. A., H. Liang, and Y. Xue. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-agent Perspective." *MIS Quarterly* 31 (1): 105–136. https://doi.org/10.2307/25148783.

Pee, L. G., I. M. Y. Woon, and A. Kankanhalli. 2008. "Explaining Non-work-related Computing in the Workplace: A Comparison of Alternative Models." *Information & Management* 45 (2): 120–130. https://doi.org/10.1016/j.im.2008.01.004.

Pham, H.-C., J. El-Den, and J. Richardson. 2016. "Stress-based Security Compliance Model: An Exploratory Study." *Information & Computer Security* 24 (4): 326–347. https://doi.org/10.1108/ICS-10-2014-0067.

Piquero, N. L., and A. R. Piquero. 2006. "Control Balance and Exploitative Corporate Crime." *Criminology; An Interdisciplinary Journal* 44 (2): 397–430. https://doi.org/10.1111/j.1745-9125.2006.00053.x.

Powell, A. L. 2013. "Computer Anxiety: Comparison of Research from the 1990s and 2000s." *Computers in Human Behavior* 29 (6): 2337–2381. https://doi.org/10.1016/j.chb.2013.05.012.

Puhakainen, P., and M. Siponen. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study." *MIS Quarterly* 34 (4): 757–778. https://doi.org/10.2307/25750704.

Ragu-Nathan, T. S., M. Tarafdar, B. S. Ragu-Nathan, and Q. Tu. 2008. "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation." *Information Systems Research* 19 (4): 417–433. https://doi.org/10.1287/isre.1070.0165.

Rahmani, D., C. Zeng, A. M. Goodarzi, and F. Vahid. 2021. "Organizational Compliance during Covid-19: Investigating the Effects of Anxiety, Productivity, and Individual Risk Factors among Iranian Healthcare Employees." *Frontiers in Communication* 6 (7). https://doi.org/10.3389/fcomm.2021.560451.

Ratchford, M., O. El-Gayar, C. Noteboom, and Y. Wang. 2022. "BYOD Security Issues: A Systematic Literature Review." *Information Security Journal: A Global Perspective* 31 (3): 253–273. https://doi.org/10.1080/19393555.2021.1923873.

Rios, K., K. G. DeMarree, and J. Statzer. 2014. "Attitude Certainty and Conflict Style: Divergent Effects of Correctness and Clarity." *Personality and Social Psychology Bulletin* 40 (7): 819–830. https://doi.org/10.1177/0146167214528991.

Robey, D., L. A. Smith, and L. R. Vijayasarathy. 1993. "Perceptions of Conflict and Success in Information Systems Development Projects." *Journal of Management Information Systems* 10 (1): 123–140. https://doi.org/10.1080/07421222.1993.11517993.

Rosen, M. A., M. Shuffler, and E. Salas. 2010. "How Experts Make Decisions: Beyond the JDM Paradigm." *Industrial and Organizational Psychology* 3 (4): 438–442. https://doi.org/10.1111/j.1754-9434.2010.01267.x.

Schmitt, J. B., C. A. Debbelt, and F. M. Schneider. 2018. "Too Much Information? Predictors of Information Overload in the Context of Online News Exposure." *Information, Communication & Society* 21 (8): 1151–1167. https://doi.org/10.1080/1369118X.2017.1305427.

Scott, C. R., and S. C. Rockwell. 1997. "The Effect of Communication, Writing, and Technology Apprehension on Likelihood to use new Communication Technologies." *Communication Education* 46 (1): 44–62. https://doi.org/10.1080/03634529709379072.

Scott, C. R., and C. E. Timmerman. 2005. "Relating Computer, Communication, and Computer-mediated Communication Apprehensions to New Communication Technology use in the Workplace." *Communication Research* 32 (6): 683–725. https://doi.org/10.1177/0093650205281054.

Serrano Archimi, C., E. Reynaud, H. M. Yasin, and Z. A. Bhatti. 2018. "How Perceived Corporate Social Responsibility Affects Employee Cynicism: The Mediating Role of Organizational Trust." *Journal of Business Ethics* 151 (4): 907–921. https://doi.org/10.1007/s10551-018-3882-6.

Siponen, M., M. Adam Mahmood, and S. Pahnila. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study." *Information & Management* 51 (2): 217–224. https://doi.org/10.1016/j.im.2013.08.006.

Siponen, M., and A. Vance. 2010. "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations." *MIS Quarterly* 34 (3): 487–502. https://doi.org/10.2307/25750688.

Sörbom, D. 1989. "Model Modification." *Psychometrika* 54 (3): 371–384. https://doi.org/10.1007/BF02294623.

Sorenson, R. L., E. A. Morse, and G. T. Savage. 1999. "A Test of the Motivations Underlying Choice of Conflict Strategies in the Dual Concern Model." *International Journal of Conflict Management* 10 (1): 25–44. https://doi.org/10.1108/eb022817.

Sposito, V. A., M. L. Hand, and B. Skarpness. 1983. "On the Efficiency of Using the Sample Kurtosis in Selecting Optimal l_p Estimators." *Communications in Statistics – Simulation and Computation* 12 (3): 265–272. https://doi.org/10.1080/03610918308812318.

Sundar, S. S. 2008. "The Main Model: A Heuristic Approach to Understanding Technology Effects on Credibility." In *Digital Media, Youth, and Credibility*, edited by M. J. Metzger and A. J. Flanagin, 73–100. Cambridge, MA: The MIT Press. https://doi.org/10.1162/dmal.9780262562324.073.

Sundaramurthy, S. C., M. Wesch, X. Ou, J. McHugh, S. R. Rajagopalan, and A. Bardas. 2017. "Humans are Dynamic. Our Tools Should be Too." *IEEE Internet Computing*, 40–46. https://doi.org/10.1109/MIC.2017.52.

Tatum, N. T., M. K. Olson, and T. K. Frey. 2018. "Noncompliance and Dissent with Cell Phone Policies: A Psychological Reactance Theoretical Perspective." *Communication Education* 67 (2): 226–244. https://doi.org/10.1080/03634523.2017.1417615.

Teoh, C. S., A. Kamil Mahmood, and S. Dzazali. 2018. "Cyber Security Challenges in Organisations: A Case Study in Malaysia." In *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, 1–6.

Ting-Toomey, S. 1994. "Managing Intercultural Conflict Effectively." In *Intercultural Communication: A Reader*, Vol. 7, edited by L. Samovar and R. Porter, 360–372. Belmont, CA: Wadsworth.

Trang, S., and I. Nastjuk. 2021. "Examining the Role of Stress and Information Security Policy Design in Information Security Compliance Behaviour: An Experimental Study of In-task Behaviour." *Computers & Security* 104:102222. https://doi.org/10.1016/j.cose.2021.102222.

Tsohou, A., and P. Holtkamp. 2018. "Are Users Competent to Comply with Information Security Policies? An Analysis of Professional Competence Models." *Information Technology & People* 31 (5): 1047–1068. https://doi.org/10.1108/ITP-02-2017-0052.

Tugtekin, E. B., and M. Koc. 2020. "Understanding the Relationship between New Media Literacy, Communication Skills, and Democratic Tendency: Model Development and Testing." *New Media & Society* 22 (10): 1922–1941. https://doi.org/10.1177/1461444819887705.

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49 (3–4): 190–198. https://doi.org/10.1016/j.im.2012.04.002.

Verhulst, M. J., and A.-F. Rutkowski. 2018. "Decision-making in the Police Work Force: Affordances Explained in Practice." *Group Decision and Negotiation* 27 (5): 827–852. https://doi.org/10.1007/s10726-018-9587-5.

Vishwanath, A. 2016. "Mobile Device Affordance: Explicating How Smartphones Influence the Outcome of Phishing Attacks." *Computers in Human Behavior* 63:198–207. https://doi.org/10.1016/j.chb.2016.05.035.

Vorakulpipat, C., S. Sirapaisan, E. Rattanalerdnusorn, and V. Savangsuk. 2017. "A Policy-based Framework for

Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives." *Security and Communication Networks* 2017:1–11. https://doi.org/10.1155/2017/2057260.

Wertheim, E. H. 2011. "Conflict Management Styles." In *The Encyclopedia of Peace Psychology*. https://doi.org/10.1002/9780470672532.wbepp047.

White, H. 1980. "A Heteroskedasticity-consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity." *Econometrica* 48 (4): 817–838. https://doi.org/10.2307/1912934.

Wolfe, K., T. S. Dickenson, B. Miller, and K. V. McGrath. 2019. "Comparing Visual and Statistical Analysis of Multiple Baseline Design Graphs." *Behavior Modification* 43 (3): 361–388. https://doi.org/10.1177/0145445518768723.

Wooldridge, J. M. 2016. *Introductory Econometrics*. 6th ed. Boston, MA: Cengage.

Wu, L. M., S. S. Chiou, P. C. Lin, Y. M. Liao, and H. L. Su. 2022. "Decisional Conflicts, Anxiety, and Perceptions of Shared Decision-Making in Cancer Treatment Trajectory among Adolescents with Cancer: A Longitudinal Study." *Journal of Nursing Scholarship* 54:589–597. https://doi.org/10.1111/jnu.12772.

Yacono, L. 2023. *The 8 Top BYOD Security Risks (and How to Mitigate Them)*. cimcor. Accessed July 25, 2024. https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate.

Yan, J., and R. L. Sorenson. 2004. "The Influence of Confucian Ideology on Conflict in Chinese Family Business." *International Journal of Cross Cultural Management* 4 (1): 5–17. https://doi.org/10.1177/1470595804041521.

Yang, Y., V. Thumula, P. F. Pace, B. F. Banahan, N. E. Wilkin, and W. B. Lobb. 2009. "Predictors of Medication Nonadherence among Patients with Diabetes in Medicare Part D Programs: A Retrospective Cohort Study." *Clinical Therapeutics* 31 (10): 2178–2188. https://doi.org/10.1016/j.clinthera.2009.10.002.

Zhang, J., H. Li, X. Luo, and M. Warkentin. 2017. "Exploring the Effects of the Privacy-handling Management Styles of Social Networking Sites on User Satisfaction: A Conflict Management Perspective." *Decision Sciences* 48 (5): 956–989. https://doi.org/10.1111/deci.12243.