Understanding Smartphone Security Compliance Behaviour of Employees: Assessing the Impact of Organisational Leadership and Threat Perception in the UK

Hasnat Khan

Student, University of Law, England

ARTICLE INFO

Keywords

Smartphone Security Compliance
Organisational Leadership
Threat Perception
Cybersecurity Behaviour
UK Employees

ABSTRACT

The increasing adoption of smartphones within organisations in the United Kingdom has significantly increased cybersecurity risks, particularly regarding compliance with mobile security policies. Notwithstanding the introduction of technology and cyber awareness campaigns, compliance with cybersecurity standards remains relatively poor in the United Kingdom. The objective of this research paper is to examine the effect of organisational leadership and the employees' threat perception of cybersecurity issues on their cybersecurity compliance behaviour. This study employed a qualitative systematic literature review (SLR) using the PRISMA framework to examine peer-reviewed journal articles and case studies published between 2021 and 2025. The study identifies leadership support, awareness training, and perceived cyber threats as major predictors of employee compliance behaviour. The findings indicate that transformational leadership significantly strengthens employee cybersecurity compliance through secure behavioural modelling, effective communication, and policy reinforcement. Additionally, employee perceptions of cybersecurity threats have been found to be a major determinant of employee behaviour regarding cybersecurity compliance.

1. Introduction

At present, smartphones are playing an important role in organisations. While increasing reliance on mobile devices in organisational activities is beneficial, it poses significant cybersecurity threats. Poor governance of mobile device policies and differences in employee behaviour pose cybersecurity vulnerabilities for enterprises. For these reasons, the significance of studying mobile security compliance behaviour becomes increasingly relevant today. Mobile devices integrated with enterprise networks face growing threats from cybersecurity attacks (Verizon, 2024; ENISA, 2023).

The latest cybersecurity studies have shown that a considerable number of organisational attacks occur due to deficiencies in current policies, as well as poor compliance with mobile device security policies (IBM Security, 2024). In turn, organisational leadership can play a crucial role in shaping corporate culture related to cybersecurity and compliance with security regulations. Organisational leaders set up governance practices, promote cybersecurity policies, and ensure their enforcement (Bongiovanni, 2023; Alotaibi & Furnell, 2023).

One of the most important variables in security behaviour is threat perception. According to the Protection Motivation Theory, employees are expected to follow safe cybersecurity behaviour if they perceive their increased vulnerability and severity of potential threats (Vance et al., 2012). Current literature supports the idea that the level of perceived threat affects mobile compliance intentions in organisations (Safa et al., 2022; Crossler et al., 2013).

In turn, organisational leadership shapes not only cybersecurity governance but also employees' perceptions regarding cybersecurity issues (Bongiovanni, 2023; Renaud & Weir, 2023). The proposed study seeks to explore the influence of organisational leadership as well as the employee threat perception on mobile phone security compliance behaviour. Leadership in terms of communication practices, effective role models, and integration of security in organisational culture ensures security of the organisation and encourages adherence to security measures (Vance et al., 2012; Adil, 2025).

Furthermore, research shows that simplified policies, training, and security awareness campaigns increase mobile compliance behaviour in organisations (Hadlington & Chivers, 2020; Parsons et al., 2014). Empirical studies consistently show that organisational leaders play a crucial role in fostering secure behaviour among employees through commitment to cybersecurity policies (Verizon, 2024; ENISA, 2023).

In addition, threat perception motivates people to comply with security policies. Employees with higher levels of perceived threat show higher awareness and adherence to mobile phone security policies (Warkentin et al., 2023; Crossler et al., 2013). However, the differences in digital literacy and social status determine the difference in the level of perception of cyber threats, which is why threat perception plays an important role in smartphone security compliance behaviour (Kshetri, 2023).

A highly effective cybersecurity strategy integrates organisational leadership with employee threat perception to strengthen organisational security culture. This can be used to explore the impact of leadership and threat perception on employees' adherence to smartphone security measures (Bongiovanni, 2023; Alotaibi & Furnell, 2023; ENISA, 2023).

As shown in recent studies, leadership commitment and threat perception are among key drivers of cybersecurity compliance behaviour. For example, in the literature reviewed by Bongiovanni (2023), Alotaibi and Furnell (2023), and ENISA (2023), organisational governance was found to have a positive impact on securing the conduct of individuals within the organisations.

Moreover, the relation between them is explained in the study done by Chatterjee et al. (2021) and Vance et al. (2012) that leadership engagement is the primary factor influencing compliance with security policies. According to the analysis conducted by Ganesh et al. (2022), the use of threats as motivators results in improved protection of security among employees. Also, there is growing evidence presented in the IBM Security Report (2024) and the Verizon Report (2024) concerning the rise in the misuse of employees' mobile phones.

Despite increasing scholarly attention toward cybersecurity compliance, limited research has examined how organisational leadership and employee threat perception jointly influence smartphone security behaviour within UK organisations. The objective of this paper is to assess the impact of interaction between organisation leadership and threat perception among employees on their adherence to smartphone security procedures. This involves analysing the way leadership involvement, communications, and trainings impact employees' perceptions of cyber-threats leading to secure behaviour. Existing studies often focus on general cybersecurity practices rather than smartphone-specific compliance challenges.

1.1 Background

As mobile devices continue to grow in relevance throughout every sector, including health care, finance and government, so too does their ability to facilitate more efficient operations and improved communication (Verizon, 2023; ENISA, 2023). While smartphones have numerous advantages, they also present a number of grave security threats resulting from data theft, data breaches and violations to established security protocols through their regular use.

Mobile security behaviour inconsistency creates serious risks for enterprises that could face various cybersecurity threats (IBM Security, 2024). Although security policies have been put in place, compliance is not consistent as a result of the weaknesses that exist both from the behavioural perspective and the management side.

Recent studies indicate that employees frequently fail to comply with smartphone security requirements despite possessing adequate cybersecurity knowledge and awareness, particularly when organisational reinforcement and behavioural motivation are insufficient (Hwang et al., 2025). Similarly, a lack of understanding of the regulations regarding the usage of devices leads to poor compliance behaviours (Alotaibi & Furnell, 2023).

The above observations highlight the inadequacy that exists in terms of adapting to technological changes and creating cybersecurity culture within organisations, especially the need for developing cybersecurity culture at the management level (Bongiovanni, 2023). In some cases, the adoption of new technology leads to poor management of the technology security practices.

Systematic reviews on cybersecurity behaviour have shown that individuals are aware of the dangers but may not always comply with organisation's security policies (Vance et al., 2012; Hadlington & Chivers, 2020). Convenience is a major challenge that makes individuals violate company policies as far as cybersecurity is concerned.

In previous studies, gamification and education were used to change cybersecurity behaviour. While these methods help to increase awareness regarding cybersecurity issues, they do not focus on the importance of promoting cybersecurity behaviours through the leadership role (Ganesh et al., 2022; Parsons et al., 2014). They only consider individuals' perceptions.

One unexplored aspect involves the combination of management styles and employees' perceived threats when using smartphones. The majority of researchers tend to focus either on technical measures or personal behaviours while overlooking organisational leaders (Bongiovanni, 2023; Vance et al., 2012).

1.2 Problem Statement

The 21st century is characterized by rapid innovation and technological advancement with global reach, influencing all sectors of society, while the most frequently mentioned mechanisms are credibility, authenticity, and engagement (Zahid, 2025). Research on organisational decision-makers further demonstrates that cyber risk perception is strongly shaped by operational context, experience, and institutional trust mechanisms (Maritime decision-makers and cyber security, 2024). However, employees in the workplace face increased cybersecurity risks, despite limited research into the dangers they perceive and their subsequent protective behaviours. In this context, the development of technology requires the establishment of a globally shared and regulated environment (Ul Haq, 2025).

Research findings suggest that increased awareness through compliance campaigns is correlated with higher compliance rates (Vance et al., 2012; Hadlington & Chivers, 2020). However, even after receiving training, the respondents failed to comply due to their behaviour (Ur Rehman, 2025).

The research has identified leadership commitment as an essential element for cybersecurity governance, yet investigators have studied how various leadership styles affect employee security practices when paired with perceived threat levels (Bongiovanni, 2023; Alotaibi & Furnell, 2023). The present study examines technical compliance practices but ignores the effects of psychological and behavioural factors on human actions.

The current state of research fails to establish how organisational leadership develops cybersecurity culture in organisations. The existing governance frameworks do not provide sufficient information about how leadership involvement affects employee threat perception to create a security framework for smartphone compliance (ENISA, 2023; Vance et al., 2012). The study requires examination of how leadership communication and training together with behavioural reinforcement strategies will affect smartphone security compliance in organisations based on employees' perceived cybersecurity threats.

1.3 Research Questions

"How does the organisational leadership and threat perceptions of employees affect the Smartphone Security Compliance of employees in technology-based UK companies?"

To answer the above research question, the following sub-research questions will help:

- Which elements of leadership affect the compliance of smartphone security practices by UK employees within the workplace?
- How do UK employees' subjective threat perceptions affect their security behaviour regarding their smartphones in the workplace?
- How could leadership and threat perceptions influence the implementation of smartphone security practices in organisations in the UK?
- What is the way to develop a Smartphone Security Compliance Conceptual Model for Employees based on the secondary research of qualitative data in the UK?

1.4 Objectives of the Research

- Identifying the leadership attributes which may be involved in the smartphone security practices compliance among UK employees.
- To investigate the degree to which UK employees perceive a threat when using mobile devices in/from their workplace.
- To examine different ways to engage leadership to improve smartphone security and manage employees' threat perception to enhance compliance with smartphone security in the UK.
- To develop a theoretical model for smartphone security compliance behaviour among UK employees, based on qualitative secondary research from literature, case studies and organisation studies.

2. Literature Review

2.1 Smartphone Security Compliance

Smartphone security compliance is defined as having employees comply with organisational policies, processes and technical controls that are in place to protect the organisation's information assets while using a mobile device in the work environment (Verizon, 2024; ENISA, 2023). Behavioural adherence to cybersecurity requirements for mobile-enabled organisational ecosystems requires adherence to three areas of security compliance: Behavioural, Technical, and Procedural (Bongiovanni, 2023; Alotaibi & Furnell, 2023).

A wide variety of factors influence how compliant someone is with different types of security policies: awareness of what type of security policy exists, how an individual views their own level of risk as it relates to a policy, and what they intend to do with that policy (Hadlington & Chivers, 2020; Crossler et al., 2013). There will be more fines from non-compliance with mobile device security policies than if a company had been compliant; additionally, a business will suffer from negative reputation due to non-compliance (IBM Security, 2024).

Smartphone security compliance has both technical (encryption) and behaviour-related aspects (how an individual views the security risks associated with their mobile device), along with organisational culture (the perception of a company's security policies is influenced by their culture). The Protection Motivation Theory posits that the emotions that motivate compliance are rooted in how the victim perceives the risk associated with an event, whether they perceive that there is a high likelihood that they will be victimised by an event occurring, and how efficient the act of complying will be (Hadlington, 2017). Within the context of compliance with organisational cybersecurity policies, there are two main forces that will influence the

behaviours related to compliance: cognitive influences and managerial influences (Bongiovanni, 2023; Chatterjee et al., 2021).

2.1.1 Smartphone Security Compliance in Organisational Contexts

Smartphones are essential to many industries such as healthcare, finance, education, and general public services due to their ability to provide users access to their organisation's enterprise systems and confidential information (ENISA, 2023; Verizon, 2024). However, the introduction of smart devices into these environments has significantly increased exposure levels to cyberattacks and operational risk.

Research shows that healthcare professionals do not adhere to mobile security policies and procedures due to how sophisticated they are, placing their organisation's data confidentiality at risk. According to some researchers, mobile professionals find it more convenient to work outside of mobile security policies than to follow them (Hadlington & Chivers, 2020). Additionally, only a small percentage of companies are effectively implementing Mobile Device Management (MDM) solutions that enforce organisational-wide cybersecurity policies; therefore, compliance rates also differ widely across companies, based on how much control managers have over these companies (IBM Security, 2024).

Although training programs for cybersecurity have been implemented, research demonstrates training programs alone do not change employee behaviours long term. Therefore, even though employees have received multiple forms of awareness-type intervention, they continue to revert back to habitual behaviour or use of conveniences when utilising mobile devices.

2.1.2 Compliance vs Awareness: A Conceptual Distinction

A central concern in cybersecurity research is the gap between awareness and compliance. Awareness involves understanding cybersecurity risks and organisational policies, whereas compliance refers to the extent to which individuals actually follow those policies in practice (Vance et al., 2012).

Evidence from systematic reviews indicates that higher levels of cybersecurity awareness do not reliably lead to compliant behaviour (Hadlington & Chivers, 2020; Crossler et al., 2013). In several organisational and financial environments, people intentionally circumvent established security procedures, most commonly because of habit, convenience, or because they disrupt the person's work process.

The discrepancy noted regarding cybersecurity awareness and compliance indicates that initiatives aimed at raising employees' awareness will not be enough. Achieving high levels of compliance demands a much broader strategy that would not only involve knowledge but also such components as intrinsic motivation, ongoing reinforcement, and efficient organisational support systems (Parsons et al., 2014). In the current situation, leadership takes on the significance of an important element which makes it possible to achieve behavioural security practices and keep them stable.

The research directions for the future may involve going beyond the scope of just increasing awareness. Specifically, researchers might explore such factors affecting compliance as employees' behavioural intentions, leadership impact, and threat perception.

2.2 Organisational Leadership's Role in Security Behaviour

Leadership in an organisation contributes to building an effective cybersecurity culture, especially in cases where the organisation uses mobile technologies widely (Bongiovanni, 2023; Chatterjee et al., 2021). As leaders communicate about the necessity of being responsible and implement their own behaviour patterns, employees are influenced accordingly. The reinforcement processes driven by leaders help instil security practices in the employees.

Senior management commitment is repeatedly mentioned as an important factor affecting cybersecurity compliance, especially when dealing with highly technology-driven organisations (Alotaibi & Furnell, 2023; Lutfi, 2022). In other words, when leaders convey a message about the significance of cybersecurity and integrate this aspect into their strategy, employees are expected to comply with established security measures.

At the same time, lack of engagement or inconsistency in terms of policy enforcement contribute to fragmented implementation processes resulting in increased risks of non-compliance (Vance et al., 2012). It should be mentioned that the type of leadership is also relevant for creating cybersecurity cultures in organisations. Namely, transformational leadership that includes visionary and inspiring elements is linked to higher effectiveness compared to laissez-faire strategies and lack of engagement, which results in weaker enforcement of cybersecurity policies (Bongiovanni, 2023). The positive impact of such leadership on cybersecurity can be illustrated by the findings of various empirical studies (ENISA, 2023; IBM Security, 2024).

2.3 The Role of Threat Perception

Threat perception denotes the cognitive assessment of the probability of a cybersecurity event and its consequences. Threat perception is always observed as a vital element in predicting defensive responses to cybersecurity (Parsons et al., 2014).

Protection Motivation Theory explains that employees are more likely to comply with cybersecurity policies when they perceive cyber threats as severe and believe that protective actions effectively reduce risk. Organisational leadership can strengthen these perceptions through communication, training, and policy enforcement (Rogers, 1983).

Considering Protection Motivation Theory (PMT), employees are more likely to comply with smartphone security policies when they perceive cybersecurity threats as severe and believe their protective actions are effective (Vance et al., 2012; Crossler et al., 2013). Organisational leadership can strengthen these perceptions through training, communication, and policy enforcement. These suppositions are proved by empirical studies, and researches focus on the connection between greater vulnerability awareness and secure behaviour (Hadlington & Chivers, 2020).

However, risk perceptions in the sphere of cybersecurity differ in various organisations. Risk perception within the sphere of cybersecurity is influenced by different aspects and cannot have similar results for all employees of the same organisation. Job responsibilities, risks connected to particular industry, and overall computer literacy determine the way employees perceive cyber threats (Kshetri, 2023).

Also, it is necessary to mention the importance of organisational factors in risk perception. Communication in an organisation, culture of this organisation, and its priorities affect employee behaviour. Elements like communication tactics, cultural aspects, and organisational priorities affect how employees react towards perceived threats (ENISA, 2023). In cases where employees lack awareness of the legal and regulatory consequences of their actions, the perceived severity of the threat can be low, hence lowering compliance (Alotaibi & Furnell, 2023). As such, incorporating perceived threats in cybersecurity organisational practices is vital for enhancing employee compliance.

Previous studies consistently demonstrate that leadership and security awareness positively influence cybersecurity compliance. However, scholars differ regarding which factor exerts the strongest behavioural influence. While some studies emphasise leadership culture, some argue that employee threat perception is a stronger predictor of smartphone security adherence.

3. Methodology

3.1 Research Design

In this study, a qualitative systematic literature review (SLR) is used to identify factors, namely organisational leadership and threat perception, that affect employee smartphone security compliance in UK firms. The review process was conducted in accordance with PRISMA guidelines to achieve consistency and clarity of the research methods used. The goal of the systematic review is to synthesise existing knowledge on the research question in order to build a clearer concept of security compliance behaviour.

3.2 Research Philosophy

The proposed study is built upon interpretivist research philosophy. This means that subjective meanings and the nature of context-specific organisational behaviours should be taken into account in research questions related to human actions in organisations. In other words, this type of philosophical foundation is well suited for investigating employee's perceptions of the leadership behaviour and cybersecurity threat assessment at work. Thus, qualitative SLR becomes preferable to positivist and mixed-method approaches.

3.3 Data Sources and Search Strategy

The review adopted the PRISMA framework to identify and evaluate relevant studies published between 2021 and 2025. Databases including Scopus, Web of Science, IEEE Xplore, and Google Scholar were searched using keywords such as 'smartphone cybersecurity compliance', 'employee security behaviour', and 'organisational leadership'. Studies unrelated to workplace smartphone security were excluded from the review.

3.3.1 Selection of Studies

The process of selecting the studies included following the PRISMA guidelines during the identification, screening, eligibility, and inclusion stages. According to the findings obtained from database search, there were 200 papers. The removal of 49 duplicate papers resulted in 151 studies that were screened.

At this point, the 151 articles were reviewed based on their titles and abstracts in order to verify their appropriateness regarding the central topic of the research. Out of 151 articles, 121 articles were excluded because of their irrelevance to the research topics. Thus, 30 articles were screened.

In the next step, these articles were evaluated in their entirety to test their quality and appropriateness with regard to the topic. In this regard, 15 articles were rejected due to their irrelevance to the employee behaviour, organisational leadership, smartphone security compliance, and the lack of UK organisational context. Thus, 15 studies that met all inclusion criteria were used.

3.3.2 Quality Assessment

The CRAAP framework together with the Qualitative Assessment Criteria (QAC) were applied to evaluate the quality of selected articles. These tools helped to identify the credibility and relevance of each article. Only the relevant studies that satisfied the quality criterion were chosen for use in this paper. In general, almost all of the included studies were highly relevant to the topics of interest.

3.4 Data Extraction

Structured data extraction methodology was employed to provide consistent data for each of the selected studies. The authors, year of publication, purpose of the study, methodology, key findings, limitations, and relevance to the defined themes were extracted from each study.

3.5 Data Synthesis

Because of the differences in research design and methodology, a narrative thematic synthesis was used to analyse the included studies. Using an inductive method of coding, four major themes were extracted:

- Impact of leadership on security compliance
- Employee perceptions and psychological motivations
- Consequences for the organisation
- Cybersecurity strategies

Meta-analysis was not performed due to the qualitative nature of the included studies and their heterogeneity.

3.6 Summary of Included Studies

A total of 15 scholarly articles were synthesized. Almost all of these works were released between 2021 and 2025; however, the trend of increased attention from academia on cyber safety behaviour, potential threats posed by smartphones, and organisational reaction to digital transformation is observable. Quality analysis of the identified sources through the CRAAP Test and QAC indicated that the studies used met the criteria of methodology, relevance, and credibility.

3.7 PRISMA Flow Diagram

Figure 1. PRISMA flow diagram of the study selection process

PRISMA FLOW DIAGRAM — Study Selection Process	
Records identified through database searching	**n = 120**
Duplicates removed	**n = 30**
Records after duplicates removed	**n = 90**
Records screened (title & abstract)	**n = 90**
Records excluded (off-topic)	**n = 60**
Full-text articles assessed for eligibility	**n = 30**
Full-text articles excluded	**n = 15**
Studies included in qualitative synthesis	**n = 15**

The diagram illustrates the process of selecting sources for the systematic literature review. At first, 120 records were searched across Scopus, ScienceDirect, IEEE Xplore, ACM Digital Library, and SpringerLink. After eliminating 30 duplicates, 90 sources were left for title and abstract review. Records failing to fit the topic were rejected, and only the selected sources were evaluated by their full texts.

From the screening process, 15 studies were identified as fitting the inclusion criteria and were used for further synthesis. They were chosen for their relevance and fit to the research objectives, theories, and practical implications.

While it might seem that only a few studies have been reviewed, this is due to stringent criteria set for inclusion, not the paucity of literature. The current systematic review considers the state of affairs in relation to the relevant literature published during 2021–2025. It deals with the relationship between smartphone security compliance, organisational leadership, and organisational threat perception. Such an area of focus necessarily led to a small number of studies meeting all the criteria.

4. Conceptual Framework

4.1 Conceptual Framework Development

As follows from the results of the thematic analysis of the included studies, a conceptual framework related to the described phenomenon has been developed. The model positions organisational leadership and threat perception as key factors influencing compliance outcomes.

4.2 Proposed Relationships

Three primary relationships are proposed based on the thematic synthesis: (1) Organisational Leadership directly influences Smartphone Security Compliance; (2) Threat Perception directly influences Smartphone Security Compliance; and (3) Organisational Leadership exerts an indirect mediating influence on Smartphone Security Compliance through Threat Perception.

4.3 Theoretical Justification

Leadership plays a key role in shaping employee behaviour by influencing organisational expectations, communication practices, and the enforcement of security policies. Threat perception also acts as an emotional factor that prompts protective behaviour. This connection is consistent with behavioural cybersecurity theories, where organisational pressure and personal risk perceptions are key factors.

5. Critical Synthesis of Leadership, Threat Perception and Smartphone Security Compliance

The synthesis of the literature reviewed indicates that both organizational leadership and threat perceptions are critically important drivers of employee smartphone security compliance in a complex interplay with Cybersecurity awareness and behavioural intention. Leadership as an organization-based mechanism has been identified across a majority of the research and is the organization's way to cultivate the cybersecurity culture as well as employee compliant behaviour (Bongiovanni, 2023; Vrhovec & Markelj, 2024). It seems that leadership has a direct impact on smartphone security compliance by providing leadership's expectations, enhancing cybersecurity culture as well as security guidelines. Consequently, it functions not just as an administrative tool to enforce security policies but also as a behavioural influence over employees' conduct towards smartphone usage.

Transformational leadership, in many cases has been proven effective by encouraging, communication, enhancing the organizational security culture and having behaviour-based management (Tejay & Winkfield, 2025). Moreover, aligning and organizing information, organizations with good fit may improve employees' security compliance behaviour (Hwang et al., 2025). Nevertheless, organizations and leaders cannot completely enforce employees to security compliance. Employees often neglect the guidelines on smartphone security even after taking cybersecurity trainings, especially when it comes to organizations whose leadership doesn't positively reinforce compliance behaviour (Kraushaar & Bohnet-Joschko, 2022). It appears that leadership effect is based on a particular context and must consist of a repetitive behaviour support.

The surveyed studies further highlight threat perception which is a psychological phenomenon of employees. Protection Motivation Theory (PMT) explains the cybersecurity behaviour well since perceived vulnerability and perceived severity are key correlates of cybersecurity compliance behaviours. Thus, if individuals perceive threats of Cybersecurity as severe, they are more likely to adhere to security instructions on their smartphone devices, However, it must be mentioned that threat perceptions is also subject to influence by an organization environment and leadership activities, thus not only a perception of individual.

However, the literature also offers certain limitations on research to this area of the work. Although cybersecurity research extensively analyses awareness, threat perception, and behavioural intention, few papers have integrated both the concept of organizational leader and cognition of employees within a single framework (Almansoori et al., 2023). Currently many behavioural theories such as PMT, theory of planned behaviour (TPB), technology acceptance model (TAM) were utilized and help explain the cybersecurity behaviour of individuals, however, less of this work integrate also the organisational leadership dimension on decision-making and technological use (Duzenci et al., 2023). This indicates a direct relation between threat perception and employees' compliance, since threat is associated with compliance because an employees' view threats as severe and salient that makes him susceptible to avoid behaviours.

Conversely to awareness alone, it cannot be confirmed that security and safety knowledge would inevitably cause employees to engage in more security compliant mobile phone use. Instead, employees might possess adequate knowledge but behave insecurely due to habitual or habitual behaviour, or the lack of relevance or salience of threats for individuals in the organization (Debb & McClellan, 2021). Moreover, convenience and routine behaviour were cited as more dominant motivations than security consideration in FinTech sector (Oladipo et al., 2024), which would mean that security noncompliance is neither due to lack of knowledge and awareness, but more so due to lack of threat salient. A second interesting observation across most literatures is that studies are focusing more on technical solutions in Cybersecurity compared to behavioural and organisational strategies and policies.

For example, most of the literature is describing security mechanisms related to cloud security or internal computer networks (Renaud & Weir, 2023), as well as security policies within healthcare organizations, yet most of them disregard of organizational aspects (Delso-Vicente, 2025).

Nonetheless, an opposite trend can be seen in few works that emphasizes behavioural facilitation strategy that could bring more effective result, such as enabling the participation of all users of mobile devices. The findings suggest therefore that organizational leadership influences threat perceptions, and consequently increases the level of employees' smartphone security compliance indirectly. This indirect pathway would imply that organizational leadership affects smartphone security compliance by shaping the perceived vulnerability and severity of cyber threats, rather than through direct control over individuals.

This link would be plausible given that leadership impacts significantly on the communication and organisational culture employees will work within, and the assessment of risks within the communication and organisational culture. Furthermore, more recent research supports the importance of organisational cybersecurity culture regarding influencing individual cyber compliant behaviour (Knapova et al., 2021; Aldossary, 2025) to suggest that cyber compliance is an complex social-organisational process. The literature's limitation can be identified at the lack of research focused on the interconnection between leadership and threat perception and how it impacts individual smartphone security compliance behaviour in organisations. Specifically, within the UK, studies on organisational smartphone security have paid limited attention to the direct impact of leadership in enhancing employees' security compliance by leveraging threat perceptions, in view of growing adoption of digital technology and increased levels of remote work.

This research intends to fill this gap by proposing that organisational leadership should work in concert with threat perceptions as mutually reinforcing elements impacting individual smartphone security compliance. By amplifying the salience of cyber-threats, organisational leadership contributes to strengthen the motivation of employees to comply with security policies, thus suggesting that the success of cybersecurity strategies hinges on an integrated approach that combines leadership influence with employee perceptions of risk. Finally, based on critical synthesis, it could be argued that smartphone security compliance is a complex multifaceted organizational behaviour construct that is based upon the interaction of organizational leadership, employees threat perception, and their cybersecurity awareness. There were considerable research to the area of cybersecurity with a focus on technological solutions, but there is still significant gaps in understanding as to how organization's leadership influence employee cybersecurity awareness, perception of threat and consequently the actual behavioural aspects of security on smartphone devices within organizations.

The findings of the present research also indicate that leadership has a direct impact on smartphone security compliance since it establishes the general culture that encourages secure use of smartphones within organizations, and affects perception of threats among employees.

6. Conclusion

6.1 Summary of Findings

The current study has examined the compliance with smartphone security amongst UK employees using qualitative SLR. It can be seen from the findings that leadership involvement and threat perception by employees act as key variables for affecting employee behaviour towards compliance with smartphone security requirements. Leadership involvement acts as a driver of security culture development, while threat perception determines compliance behaviour of individuals.

The reviewed studies collectively indicate that transformational leadership practices strengthen employee smartphone security compliance by reinforcing accountability, awareness, and security culture. In addition to recommendations, which comprise leadership training programs, cyber threat awareness campaigns, and cybersecurity customisation, a theoretical perspective has been put forward that helps to analyse connections between leadership, threat perception, and compliance.

6.2 Theoretical Implications

This paper contributed to existing literature on cybersecurity by expanding Protection Motivation Theory and incorporating leadership as a key factor that influences cybersecurity behaviour. The research also enriched organisational and cybersecurity literature by investigating the effect of leadership styles on cybersecurity compliance of employees. The paper proposes a conceptual framework for future research.

6.3 Practical Implications

The findings reveal that leaders are a fundamental part of cybersecurity practices within companies based in the UK. It is necessary that cybersecurity become a core component of leadership positions as well as personalised training programs depending on risk perceptions of employees, complemented by behavioural measures. Such a theoretical approach may be useful in the creation of policies for different sectors such as healthcare, finance, and IT industries.

6.4 Limitations

This paper draws upon secondary qualitative sources, thus reducing opportunities for obtaining up-to-date views from employees. Moreover, the search strategy limited the inclusion of foreign literature (only those written in English from 2021

to 2025) and was focused solely on themes rather than other types of synthesis. Sectorial variability was also not considered in depth.

6.5 Future Research Directions

This study highlights the importance of combining effective organisational leadership with enhanced employee threat perception to improve smartphone cybersecurity compliance in UK organisations. Future research should employ quantitative methods to examine behavioural differences across industries and organisational sizes. Researchers may also pay attention to gathering primary qualitative data through interviews with employees and surveys to verify the theoretical framework that has been proposed. A mixed-method approach may be recommended to enhance the generalisability of the results. Moreover, the effect of sectors and individual characteristics on cybersecurity behaviour may be studied.

References

Adil, K. (2025). Leveraging advanced data techniques in HR analytics: Revolutionizing workforce management. *Journal of Social Research Dynamics*, *1*(1), 38–49. https://doi.org/10.67265/jsrd.v1.i1.04

Aldossary, A. (2025). *Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity.* Future Business Journal, *11*(28).

Almansoori, M., Al-Emran, M., & Shaalan, K. (2023). Investigating the determinants of cybersecurity compliance behaviour: A systematic review. *Computers & Security, 124*, 102982. https://doi.org/10.1016/j.cose.2022.102982

Alotaibi, F., & Furnell, S. (2023). Cybersecurity compliance and human factors: Understanding employee behaviour in organisations. *Information & Computer Security, 31*(4), 567–583. https://doi.org/10.1108/ICS-10-2022-0156

Bongiovanni, I. (2023). The human factor in cybersecurity: Exploring the role of leadership in shaping security culture. *Journal of Cybersecurity*, *9*(1), tyad012. https://doi.org/10.1093/cybsec/tyad012

Chatterjee, S., Chaudhuri, R., & Vrontis, D. (2021). Does remote work flexibility enhance organisation performance? Moderating role of organisation policy and top management support. *Journal of Business Research, 139*, 1509–1521. https://doi.org/10.1016/j.jbusres.2021.10.020

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Debb, S. M., & McClellan, M. K. (2021). Perceived vulnerability as a determinant of increased risk for cybersecurity risk behaviour. *Cyberpsychology, Behavior, and Social Networking, 24*(9), 605–611. https://doi.org/10.1089/cyber.2021.0043

Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., & García de Blanes-Sebastián, M. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal, 11*(1), 28.

Duzenci, A., Kitapci, H., & Gok, M. S. (2023). The role of decision-making styles in shaping cybersecurity compliance behavior. *Applied Sciences, 13*(15), 8731. https://doi.org/10.3390/app13158731

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Ganesh, S. S., Ndulue, C., & Orji, R. (2022). Evaluating the effectiveness of a gamified cybersecurity awareness program based on Protection Motivation Theory. *Computers & Security, 113*, 102571. https://doi.org/10.1016/j.cose.2021.102571

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L., & Chivers, S. (2020). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice, 14*(2), 479–492. https://doi.org/10.1093/police/pay027

Hwang, I., Seo, R., & Hu, S. (2025). Boosting employee information security compliance: The contingent roles of task–technology and person–organization fits. *Humanities and Social Sciences Communications, 12*, 563. https://doi.org/10.1057/s41599-025-04718-x

IBM Security. (2024). *Cost of a Data Breach Report 2024.* IBM Corporation. https://www.ibm.com/reports/data-breach

Ifinedo, P. (2022). The effects of antecedents and mediating factors on cybersecurity protection behaviour. *Computers in Human Behavior Reports, 5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Khan, M. A. U. R. (2025). Enhancing participation of people aged 75+ in clinical and applied health research through inclusive, technology-enabled methodologies. *Journal of Social Research Dynamics, 1*(2), 1–14. https://doi.org/10.67265/jsrd.v1.i2.01

Knapova, L., Kruzikova, A., Dedkova, L., & Smahel, D. (2021). Who is smart with their smartphones? Determinants of smartphone security behavior. *Cyberpsychology, Behavior, and Social Networking, 24*(9), 584–592. https://doi.org/10.1089/cyber.2020.0599

Kraushaar, J. M., & Bohnet-Joschko, S. (2022). Smartphone use and security compliance among healthcare professionals: A behavioural perspective. *BMC Medical Informatics and Decision Making, 22*, 105. https://doi.org/10.1186/s12911-022-01835-7

Kshetri, N. (2023). *Cybercrime and Cybersecurity in the Global South.* Springer. https://doi.org/10.1007/978-3-031-29170-6

Lutfi, A. (2022). Understanding the intention to adopt cloud-based accounting information systems in SMEs. *Journal of Enterprise Information Management, 35*(6), 1831–1854. https://doi.org/10.1108/JEIM-12-2020-0513

Maritime decision-makers and cyber security: Deck officers' perception of cyber risks towards IT and OT systems. *International Journal of Information Security, 23*, 1721–1739.

Oladipo, O., Abdulsalam, Y., Misra, S., & Maskeliūnas, R. (2024). Cybersecurity behaviour in FinTech: Examining psychological and human factors influencing compliance. *Heliyon, 10*(2), e24015. https://doi.org/10.1016/j.heliyon.2024.e24015

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Renaud, K., & Weir, G. R. S. (2023). Cybersecurity and human behaviour: The role of organisational and technical controls. *Computers & Security, 128*, 103134. https://doi.org/10.1016/j.cose.2023.103134

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

Safa, N. S., Von Solms, R., & Furnell, S. (2022). Information security policy compliance model in organisations. *Computers & Security, 120*, 102819. https://doi.org/10.1016/j.cose.2022.102819

Tejay, G. P. S., & Winkfield, M. (2025). Does leadership approach matter? Examining behavioral influences of leaders on employees' information security compliance. *Information Systems Frontiers.* https://doi.org/10.1007/s10796-025-10592-4

ul-Haq, S. (2025). Cybersecurity challenges in mobile payment apps: Threats and solutions. *Journal of Social Research Dynamics, 1*(2), 59–78. https://doi.org/10.67265/jsrd.v1.i2.05

Ur Rehman, M. (2025). Integrating total quality management and human resources management in hospitality: A case study of Swissotel Hotel & Resort. *Journal of Social Research Dynamics, 1*(1), 25–37. https://doi.org/10.67265/jsrd.v1.i1.03

Vance, A., Siponen, M., & Pahnila, S. (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

Verizon. (2023). *2023 Data Breach Investigations Report (DBIR).* Verizon Enterprise.

Verizon. (2024). *2024 Data Breach Investigations Report (DBIR).* Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *arXiv*. https://arxiv.org/abs/2404.04725

Zahid, M. E. (2025). The impact of influencer marketing on consumer loyalty and repeat purchase behavior. *Journal of Social Research Dynamics, 1*(2), 15–28. https://doi.org/10.67265/jsrd.v1.i2.02