Science Discovery
2026, Vol. 14, No. 3, pp. 113–123
https://doi.org/10.11648/j.sd.20261403.18

Research Article

Cybersecurity Awareness and Social Engineering Vulnerabilities Among Public Sector Employees in Saudi Arabia: An Empirical Assessment

Khaled Almadhi, Olumide Olajide Ojo*, Syed Mehmood Hasan, Satya Shah

School of Engineering, Physical and Mathematical Sciences, University of London, Egham, United Kingdom

Abstract

As cyber threats increasingly target human vulnerabilities, understanding behavioural and organisational factors is vital for strengthening resilience. This study investigates cybersecurity awareness and social engineering vulnerabilities among public sector employees in Saudi Arabia, a context characterised by rapid digital transformation and heightened exposure to cyber threats. Despite significant national investment in cybersecurity, human-centred vulnerabilities remain a dominant cause of security breaches. Drawing on Protection Motivation Theory (PMT) and the Theory of Planned Behaviour (TPB), the study examines behavioural determinants of secure practices and evaluates the influence of organisational culture, policies, and training. A quantitative, positivist research design was employed, using a structured online survey distributed to public sector employees. Data were analysed using descriptive statistics, correlation analysis, t-tests, and regression modelling. Findings indicate that cybersecurity training, organisational policy clarity, and supportive organisational culture significantly enhance cybersecurity awareness, while notable gaps persist in recognising and responding to social engineering attacks such as phishing, pretexting, and baiting. The study provides empirical evidence on human-factor vulnerabilities within a critical national sector and highlights the need for continuous, context-specific training and policy reinforcement. Recommendations include adaptive awareness programmes, integration of simulated attack exercises, and alignment of organisational practices with established frameworks such as NIST SATE and HAIS-Q. The results support the development of resilient cybersecurity ecosystems within public institutions and advance an engineering-oriented understanding of socio-technical security risks.

Keywords

Cybersecurity Awareness, Social Engineering, Public Sector, Protection Motivation Theory, Theory of Planned Behaviour, Organisational Culture, Cybersecurity Training, Human Factor Vulnerabilities, Security Behaviour

1. Introduction

In contemporary digital work culture, protecting sensitive information and data has become a crucial priority for organisations. Cybercrime and data breach incidents are estimated to cost approximately $6 trillion by 2021, up from $3 trillion in 2015 [1]. Nearly 77% of data breaches faced by organisations are caused by human weaknesses [1]. Therefore, it is clear that organisations face a significant challenge in maintaining the security of their information. In this context, central public sector

*Correspondence: Olumide Olajide Ojo (olumide.ojo@rhul.ac.uk)

Received: 14 November 2025; **Accepted:** 6 January 2026; **Published:** 30 May 2026

organisations depend on digitally enabled services [1]. Hence, information system arrangement (ISA) is vital for both public- and private-sector enterprises, although it handles less risky information in the public sector. Several measures have been implemented to address common threats that make digitally enabled organisations vulnerable to data breaches and cyberattacks. Semi-automated information security risk assessments and security awareness measures developed by various governments are primary strategies for mitigating cybersecurity threats and data breaches [1, 2]. Cybersecurity threats primarily manifest as ransomware attacks in public-sector enterprises. The recent occurrence of such attacks underscores the need for a shared public-private response system and enhanced regional collaboration to foster improved cybersecurity awareness.

Globally, many countries face serious cybersecurity threats, including data breaches and ransomware attacks. Among them, Saudi Arabia has recently experienced a significant increase in cyberattacks due to its geopolitical prominence and wealth. It is one of the leading countries, with 93.31% of the population using the internet and 72.38% actively engaged on social media, spending an average of more than 7 hours daily [2]. The projected average expenditure per employee in Saudi Arabia's cybersecurity market is $26.98 million in 2024. According to a survey conducted in early 2021, cybersecurity awareness in Saudi Arabia is relatively high, with most participants believing cybercrimes will become a serious threat in the future [3].

The existing literature emphasises the importance of cybersecurity awareness but offers insufficient empirical insight into the specific vulnerabilities, behavioural determinants, and organisational factors that shape security practices among Saudi public-sector employees. Prior studies often focus on general populations, private-sector contexts, or technical threat landscapes, with limited attention to human-centred risks in government institutions. Furthermore, while theoretical models such as PMT and TPB offer explanatory value, their application to cybersecurity behaviour in Middle Eastern public sector environments remains underexplored. There is also a lack of an integrated assessment that combines awareness levels, organisational culture, policy clarity, and training effectiveness. This gap constrains the development of targeted, evidence-based interventions to strengthen national cyber resilience.

This study aims to assess cybersecurity awareness levels among employees in Saudi Arabia's public sector, with a particular focus on their vulnerability to social engineering attacks. It addresses a notable gap in the existing literature on cybersecurity awareness within this sector. Although previous research emphasises its importance, there remains a limited understanding of specific strategies to improve awareness and reduce social engineering threats. Using a quantitative approach, the study gathers empirical data on current levels of awareness, identifies specific knowledge gaps, and explores how public sector workers perceive and respond to cybersecurity risks amid digital transformation. This will contribute to academic discussions by linking behavioural insights with practical awareness strategies. Saudi Arabia's public sector handles sensitive data and provides essential services; as digitalisation and AI integration increase, these organisations face rising cyber threats [4].

Recent reports confirm a rise in attacks, emphasising the need for stronger cybersecurity measures [5]. Additionally, the study aims to inform government policy and training programmes by evaluating employee awareness, supporting enhanced cybersecurity practices, reducing vulnerabilities, and building resilience. A quantitative measure of the current level of cybersecurity awareness among public sector employees in Saudi Arabia involves identifying specific vulnerabilities and knowledge gaps. Further evaluation of the effectiveness of existing cybersecurity training programmes in the public sector was conducted to examine how organisational culture and policies influence cybersecurity awareness and behaviours. These results will help inform recommendations to enhance cybersecurity training and policies within the Saudi Arabian public sector. Ultimately, the research will help the Saudi government safeguard national security and maintain the integrity of public services.

This project's scope includes a comprehensive assessment of cybersecurity awareness among public sector employees in Saudi Arabia. To evaluate awareness levels, the study uses statistical methods to collect numerical data on public sector workers' awareness and vulnerabilities in Saudi Arabia. The project aims to address social engineering vulnerabilities and improve employee awareness within the public sector of Saudi Arabia. It will focus on factual, relevant information about this area. Additionally, the study investigates cyber awareness and explores measures to enhance cyber awareness programmes for public sector employees in Saudi Arabia. It considers perceptions of risks and threats posed by various types of cyberattacks. Furthermore, the research incorporates strategies to increase awareness among targeted groups and reduce cybersecurity threats. Protecting data and information within Saudi Arabia's public sector is a central focus of the project, with particular attention to the severity of risks and the development of measures to mitigate them through both public and government-supported initiatives.

2. Literature Review

2.1. Overview of Cybersecurity Awareness

Cybersecurity awareness is critical among public sector employees who handle sensitive data. This study reviews social engineering vulnerabilities. It assesses awareness programmes using frameworks such as the Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), the NIST SATE, the HAIS-Q, and the CSAT.

The guiding question is: How effective are current cybersecurity awareness programs at addressing social engineering

vulnerabilities among public-sector employees? Peer-reviewed sources were selected based on relevance and empirical strength to bridge theory and practice and inform the development of tailored training and policy in Saudi Arabia and are summarised in Figure 1.

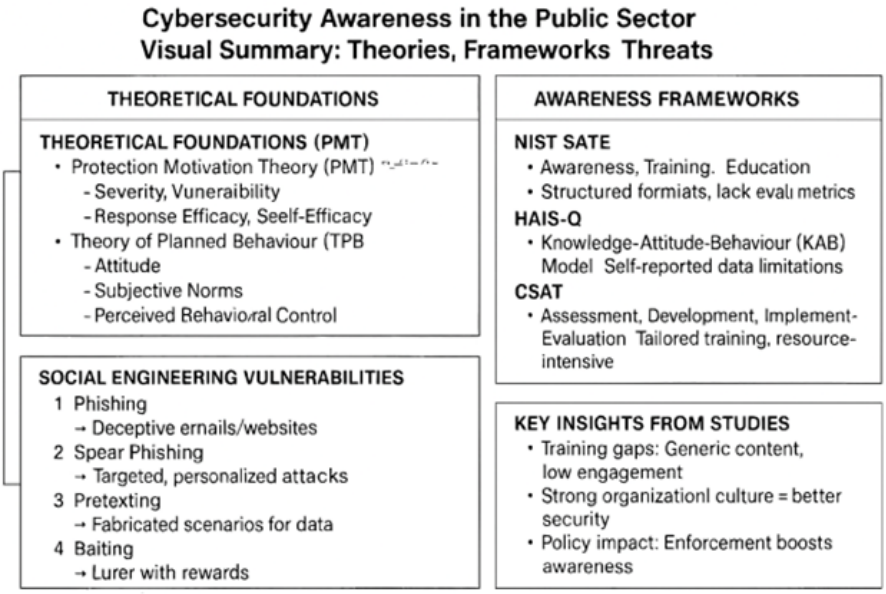

Figure 1. *Overview of Cybersecurity Awareness in the Public Sector.*

2.2. Theories and Frameworks

Several theories and frameworks have been researched and developed to enhance cybersecurity knowledge and awareness. Several theoretical foundations and frameworks relevant to cybersecurity awareness in Saudi Arabia's public sector have been adopted to enhance information security and cybersecurity nationwide [6]. A few of these theories and frameworks are listed below:

1) Protection Motivation Theory (PMT): PMT describes cybersecurity behaviour by considering perceived severity, vulnerability, response efficacy, and self-efficacy. It suggests that viewing cyber threats as serious and oneself as vulnerable encourages protective measures, such as following protocols and engaging in training [7].

2) Theory of Planned Behaviour (TPB): TPB links behaviour to intention, shaped by attitude, subjective norms, and perceived control. It helps evaluate employee attitudes and perceived control over cybersecurity actions, guiding the development of more effective awareness programmes [8].

3) NIST SATE Framework: NIST SP 800-50 details awareness, training, and education components. It encourages structured learning via instructor-led and e-learning methods [9, 10]. However, it may not be appropriate for all organisational settings and lacks metrics to assess its effectiveness [11].

4) Human Aspects of Information Security Questionnaire (HAIS-Q): HAIS-Q employs the knowledge-attitude-behaviour (KAB) model to evaluate awareness. It provides insights into employee understanding and compliance but depends on self-reported data, which may be biased [12, 13].

5) Cybersecurity Awareness Training (CSAT) Framework: CSAT includes assessment, development, implementation, and evaluation phases. It supports tailored training and feedback-based improvement [14, 15]. However, its effectiveness depends on accurate initial assessments and continuous updates, which may be resource-intensive.

2.3. Social Engineering Vulnerabilities

Social engineering vulnerabilities exploit human psychology rather than technical flaws to gain unauthorised access to systems, data, or physical spaces. These threats are especially dangerous because they target the weakest link in security, the human element. This section highlights six key types of social engineering threats: phishing, spear phishing, pretexting, baiting, tailgating, and quid pro quo. Phishing involves tricking individuals through fake emails or websites that appear trustworthy to steal sensitive information, such as login details or financial data [16]. To combat this, strategies include employee training, simulated phishing tests, email filtering, multi-factor authentication (MFA), and incident response planning. Spear phishing is a targeted approach that uses publicly available personal data to create convincing messages,

often impersonating colleagues or referencing recent projects. Preventive measures involve specialised training, strict data protection policies, and advanced threat detection through behavioural analysis.

Pretexting involves attackers creating false scenarios to impersonate trusted figures and coax victims into revealing sensitive data. Prevention tactics include identity verification, specialised training, and access controls. Baiting entices victims with rewards, such as malware-infected USB drives or fake downloads, which can be countered through awareness programs, device management policies, and web filtering. Tailgating manipulates employee trust to gain unauthorised physical access to secure zones. Prevention measures encompass physical security training, strong access control systems, and strict visitor procedures [14]. Quid pro quo attacks involve offering fake services, often claiming to be Information Technology (IT) support, in exchange for confidential information or system access [15]. These tactics depend on establishing trust to steal login details or install malicious software. All these threats highlight the importance of ongoing education, behavioural vigilance, and layered security strategies to counter human vulnerabilities.

From an engineering perspective, cybersecurity awareness constitutes a socio-technical control mechanism that complements technical safeguards [15]. Human-factor vulnerabilities are latent system weaknesses that can propagate through organisational processes, increasing the probability of system compromise. Integrating behavioural theories with engineering frameworks enables more accurate risk modelling, supports the design of resilient systems, and informs the development of adaptive training interventions [19]. This study positions cybersecurity awareness as an essential component of public-sector cybersecurity resilience engineering.

2.4. Knowledge Gaps

Previous studies have highlighted significant vulnerabilities and knowledge gaps in cybersecurity awareness among public sector employees in Saudi Arabia. Common issues include susceptibility to phishing and social engineering attacks, poor password habits, and limited understanding of multi-factor authentication [17]. Many employees lack detailed knowledge of specific threats and are unaware of the legal and ethical consequences of cybersecurity breaches. Despite ongoing technological advancements that introduce new risks, awareness levels remain low. Evaluations of current training programmes show that interactive, practical sessions are more effective than traditional methods, improving employees' ability to recognise and counter threats [16]. However, widespread training initiatives often fall short of departmental needs due to a one-size-fits-all approach, leading to disengagement and decreased relevance, especially in finance departments compared to human resources [18, 19].

Organisational culture and policy enforcement are vital in shaping cybersecurity awareness. A strong security culture encourages proactive behaviour, participation in training, and open communication about threats [20, 21]. In contrast, weak cultures lead to neglect of protocols and skipping training sessions, which increases vulnerability [22]. Effective policies raise awareness through regular audits and clear compliance expectations [23, 24]. However, implementing these policies often encounters bureaucratic hurdles and resource constraints, thereby reducing employee engagement and adherence [20]. Organisations that prioritise cybersecurity are expanding policies and promoting proactive involvement, supported by ongoing education and training to emphasise the importance of individual roles in protecting digital assets [20, 24].

3. Research Methodology

3.1. Research Strategy and Approach

This study employs a quantitative research design to evaluate cybersecurity awareness and susceptibility to social engineering among public-sector employees in Saudi Arabia. Guided by a positivist philosophy, the research relies on observable, measurable data to ensure objectivity and reproducibility [24]. Although positivism offers accuracy and neutrality, it may overlook contextual subtleties, suggesting the need to supplement quantitative data with qualitative insights, such as interviews. A deductive approach is employed, beginning with hypotheses about cybersecurity vulnerabilities and testing them against empirical data to validate existing theories and inform policy [21]. The primary method involves an online survey of 200 public-sector employees using a structured, closed-ended questionnaire [25], which was pretested and conducted anonymously to minimise bias and promote honest responses.

3.2. Data Collection and Analysis Methods

The study employs a cross-sectional design to collect data at a single point in time, establishing a baseline of cybersecurity awareness and identifying areas of urgent risk [26]. While this method is cost-effective and suitable for large samples, it doesn't track changes over time, suggesting that future research should incorporate historical data. Data collection was conducted using a self-developed Likert-scale questionnaire to measure cybersecurity awareness and perceived risks. Despite its efficiency, the questionnaire may limit depth and experience low response rates, which were addressed through reminders and incentives [27]. The target population includes public-sector employees with basic cybersecurity knowledge, excluding those without interaction with digital systems. A sample of 200 participants was selected via convenience sampling, with efforts to diversify participants across departments and regions, including outreach to working mothers through HR contacts [28].

Data analysis was conducted using SPSS, employing descriptive and inferential statistics, including cross-tabulations, chi-square tests, and regression analysis, to identify patterns and relationships in cybersecurity awareness [29]. Ethical approval was obtained from Royal Holloway University of London, ensuring compliance with ethical standards. Participants were informed of their rights, including the option to participate voluntarily and withdraw, and all data were anonymised to protect confidentiality. The study emphasised participant welfare, avoided sensitive questions, and ensured that no physical or psychological harm occurred. These ethical measures uphold the integrity of the research and safeguard the rights of all respondents.

4. Data Analysis, Findings and Discussion

4.1. Research Data Analysis and Demographics

This study's findings are based on quantitative data collected through surveys examining cybersecurity awareness among Saudi Arabian public servants, analysed using graphical and statistical methods. The results are systematically organised to meet the research objectives. Among 212 participants, 36.8% are aged 26–35, 26.4% are aged 36–45, 19.3% are aged 46–55, and 15.6% are aged 18–25, representing a diverse age range that offers valuable insights into different generations. The gender distribution shows 77% male and 22.6% female, providing varied perspectives and ensuring representation. In terms of education, 57.8% hold bachelor's degrees, 10% hold master's degrees, 11.4% hold diplomas, 10% have finished high school, and a few hold doctorates, broadening the academic perspective. Regarding experience in the public sector, 33.2% have over 10 years, 18.3% have between 1 and 10 years, 17.8% have between 11 and 20 years, and 13.5% have less than 1 year, providing comprehensive insights into cybersecurity practices across different career stages.

4.2. Quantitative Findings

This section provides detailed statistical data on cybersecurity awareness within the Saudi Arabian public sector. According to Figure 2, nearly 61.1% of respondents rated their awareness of various cybersecurity threats as high or very high. Conversely, only a small proportion of participants reported low or very low levels of awareness. Additionally, 28.4% of respondents expressed neutrality regarding their cybersecurity awareness. Based on these responses, it is evident that many public-sector employees have strong cybersecurity awareness. However, as some neutral and negative responses persist, management teams should continue to refine policies and practices to further enhance employees' cybersecurity awareness.

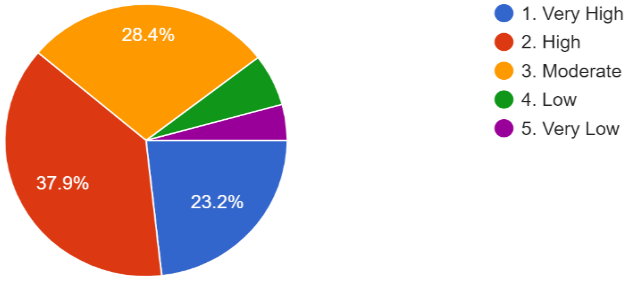

Figure 2. *Level of Cybersecurity Awareness.*

As shown in Figure 3, this section further explores the frequency and level of cybersecurity training provided to employees. Only 20.1% of survey participants reported receiving formal cybersecurity training from their employers, with just 7.2% indicating they receive very frequent training. Meanwhile, 19.1% reported never having access to formal cybersecurity training through their employers. Additionally, 29.2% and 24.4% of participants reported receiving formal cybersecurity training rarely and occasionally, respectively. Due to the persistent negative and unsatisfactory responses, it is evident that all employers in this sector must implement formal cybersecurity training programmes to improve their employees' skills awareness. A further assessment of access to cybersecurity training showed that only 39.2% of respondents reported receiving training at least once a year, while 26.4% reported receiving it twice a year. Meanwhile, 20.8% reported never having been offered cybersecurity training. These results highlight the urgency for employers in the sector to enhance the frequency of cybersecurity training programmes to boost employee awareness.

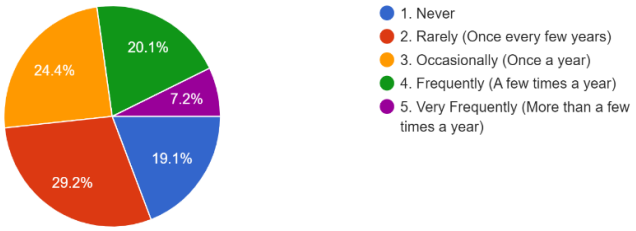

Figure 3. *Formal Cybersecurity Training Frequency.*

Figure 4 shows that 72.2% of survey respondents either agree or strongly agree that effective cybersecurity training enhances their ability to understand and address cybersecurity threats. Additionally, 19.6% responded neutrally. Conversely, 8.2% of participants disagreed or strongly disagreed, indicating that they believe cybersecurity training does not help them identify or mitigate cybersecurity issues or threats.

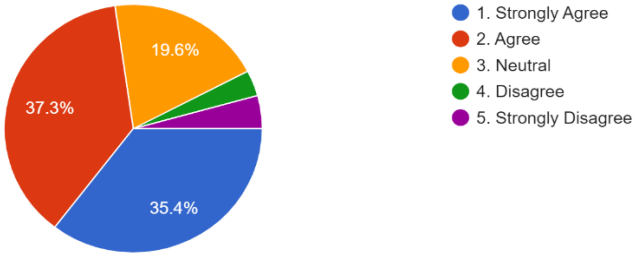

Figure 4. *Cybersecurity training helps to mitigate threats.*

A further evaluation was conducted to examine cybersecurity in the public sector from a social engineering perspective. The survey thus investigated participants' awareness of social engineering attacks and vulnerabilities. As shown in Figure 5, 20.1% and 16.7% of participants in this survey are very or extremely aware of various social engineering attacks, including pretexting, phishing, and baiting. Conversely, 10% of participants are identified as unaware of such social engineering attacks. However, 23.4% and 29.7% of the respondents have a low level of awareness regarding these types of attacks. Therefore, based on the majority of responses, it can be concluded that many people in this sector are aware of various social engineering attacks, but their levels of awareness differ.

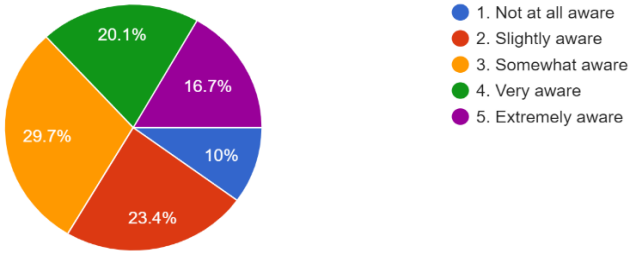

Figure 5. *Awareness of Social Engineering Attacks.*

More than 60% of participants feel confident or very confident in identifying phishing emails, while 14.4% lack confidence in recognising them as cybersecurity threats. Additionally, 23.8% are uncertain about their confidence levels. The overall response suggests that everyone needs to understand this identification process. Regarding password updates as a cybersecurity measure, 28.1% of participants consistently update their passwords and follow best practices for strong passwords. Another 24.6% often update their passwords and adhere to these practices, while 33.3% do so sometimes. Only 9% rarely update their passwords and do not follow best practices. This suggests that most employees in the Saudi public sector recognise the importance of updating passwords to prevent cyberattacks.

Figure 6 shows that 27.1% of participants are "slightly clear" about their organisational policies and procedures for cybersecurity incident reporting. Additionally, 13% have indicated that they are not at all "clear" about these policies and procedures. Conversely, only 31.4% of participants stated that they are "very or extremely clear" about their organisational policies and procedures for cybersecurity incident reporting. Therefore, it appears that most employees in this sector are unfamiliar with their organisation's policies and procedures for reporting cybersecurity incidents.

Further exploration reveals that 41.1% of participants consistently adhere to their workplace's cybersecurity policies and procedures. Meanwhile, 24.9% of participants report often complying with these policies and procedures. Additionally, 24.9% sometimes adhere to them. In contrast, a smaller percentage of the total participants rarely or never follow the cybersecurity policies and procedures at work. Based on the majority of responses, it can be concluded that many employees in Saudi Arabia's public sector follow their workplace cybersecurity policies and procedures.

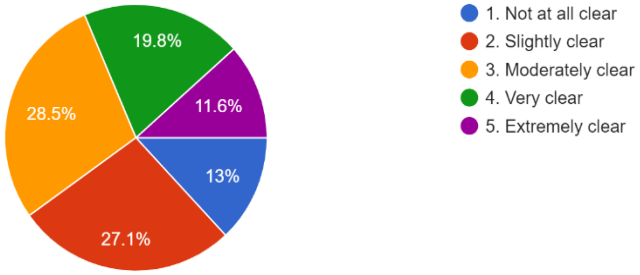

Figure 6. *Policy Access and Clarity.*

Furthermore, 61.4% of respondents agree or strongly agree that organisational culture at the workplace encourages best practices and cybersecurity awareness. Aside from that, 27.5% gave neutral responses, while the remaining 11.1% disagreed or strongly disagreed. Therefore, most responses suggest that organisational culture promotes best practices and cybersecurity awareness.

Figure 7 explores the frequency of cybersecurity attacks experienced by the participants. 42.45% of participants have never experienced a cybersecurity attack at their workplace. 25.2% of participants reported rarely experiencing any cybersecurity attacks at their workplace. 18.6% of participants reported having occasionally experienced a cybersecurity attack at their workplace. However, the remaining respondents reported that they either frequently or very frequently experienced a cybersecurity attack at their workplace.

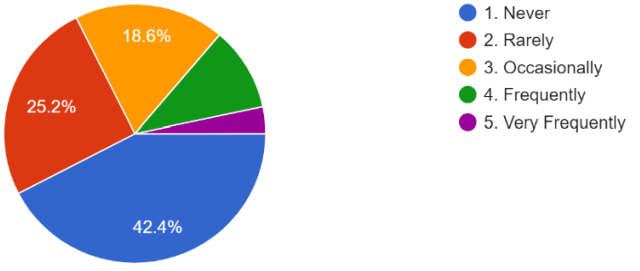

Figure 7. *Cybersecurity Attacks Experience.*

Among participants, 29.2% reported always using multi-factor authentication to access work-related systems and data. Conversely, 25.8% reported often using multi-factor authentication for the same purpose. Additionally, 28.2% of the participants use multi-factor authentication to access work-related systems and data. Only 9.6% of the total participants never use multi-factor authentication for this purpose. Therefore, based on the majority of responses, it can be concluded that many employees in Saudi Arabia's public sector frequently use multi-factor authentication to access work-related systems and data. Further evaluation was conducted to assess the understanding of the importance of cybersecurity and its training within the public sector in Saudi Arabia. Of the respondents, 45.9% and 28.7% indicated that cybersecurity is important or very important in their daily work routine. Also, 19.1% of the participants provided a neutral response. Conversely, a negligible percentage of respondents also stated that cybersecurity is “not important” or “not very important” in their daily work routine. Additionally, 79.8% of the survey respondents agree or strongly agree that extra cybersecurity training would enhance their ability to identify and respond to cyber threats. Furthermore, 16.3% of them remain neutral on this matter. Conversely, 3.9% of participants disagree or strongly disagree with this statement. Based on the majority of responses, it can be concluded that additional cybersecurity training would improve their capacity to handle cyber threats. Means of conducting training were also explored to identify the preferred method among public sector employees; 37.9% of participants preferred online courses for cybersecurity training. On the other hand, 27.5% of participants preferred in-person training for this purpose. Apart from that, 26.5% of them indicated workshops, while the remaining participants mentioned self-paced learning and webinars as suitable methods for receiving cybersecurity training. Hence, based on preferences, different organisations can develop strategies that align with their suitability and organisational policies.

4.2. Descriptive Analysis and Findings

Descriptive analysis showed that, for the most part, workers had an acceptable level of cybersecurity awareness. There appeared to be a good understanding of the basic principles of cybersecurity and the organisation's policies. However, some areas showed a considerable lack of knowledge, particularly regarding social engineering, including techniques such as pretexting, baiting, and quid pro quo. While several people felt they could detect phishing attacks, few followed through with practices such as changing passwords and verifying the sender's credentials.

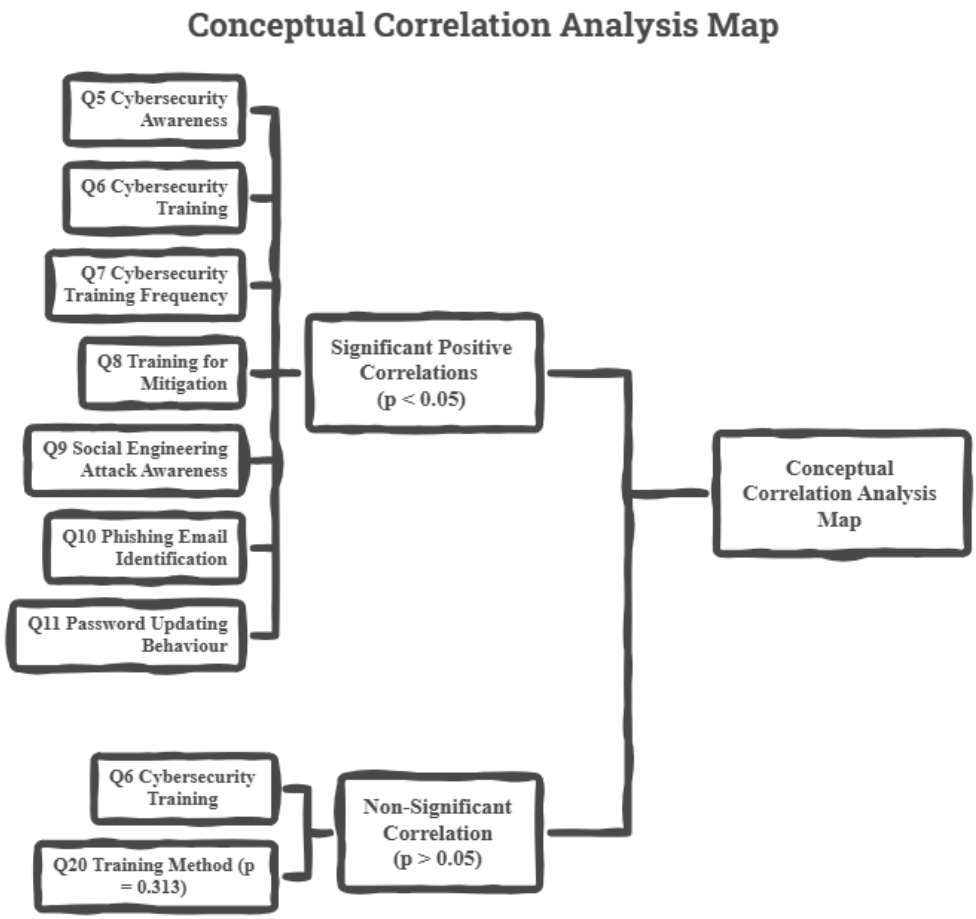

Figure 8. *Correlation analysis of key variables.*

Correlation Analysis: From the SPSS analysis, the correlation or p-value for cybersecurity awareness (Q5) with all other factors, such as Cybersecurity training (Q6), Cybersecurity training frequency (Q7), Training for mitigation (Q8), Social engineering attacks (Q9), Phishing email identification (Q10), and Updating passwords (Q11), ranges from 0.00 to 0.002, all less than 0.05 ($p<0.05$). Therefore, these values are significant, and hence, cybersecurity awareness has a significant and positive correlation with Cybersecurity training (Q6), Cybersecurity training frequency (Q7), Training for mitigation (Q8), Social engineering attacks (Q9), Phishing email identification (Q10), and Updating passwords (Q11). On the contrary, the p-value for the association between Cybersecurity training (Q6) and Training method (Q20) is 0.313, which is greater than 0.05 ($p>0.05$). Therefore, this value is insignificant, and there is no significant correlation between these two variables. The correlation analysis, as shown in the analysis result and as depicted in Figure 8, revealed that there were positive correlations between: (1) Cybersecurity training and awareness, (2) Clarity of organisational policies and secure behaviour and (3) Organisational culture supports vigilance to social engineering by employees. This finding demonstrates that organisational attributes have an important impact on human security performance.

T-Test Results and Regression Analysis: A t-test was conducted in this study to test the hypotheses developed. Based on the results of this analysis, it is possible to determine whether organisational culture, training, or organisational policies help to increase cybersecurity awareness among people. Additionally, the results help determine whether password updates and Phishing email identification help reduce the risk of cyberattacks. However, to conduct this statistical test, Cybersecurity awareness (Q5) and cyber-attack (Q15) have been selected as the dependent variables. At the same time, Cybersecurity training (Q6), Phishing email identification (Q10), Updating passwords (Q11), Organisational cybersecurity policies and procedures (Q13), and Organisational culture (Q14) have been used as independent variables. According to the results, the p-values for all variables considered are 0.000, which is less than 0.05 ($p<0.05$). Hence, these values are significant at the 0.05 level. The independent samples t-tests revealed significant differences ($p < 0.05$) in cybersecurity awareness across demographic groups, including educational attainment and work experience. Those with higher education and greater work experience exhibited better awareness and adherence to cybersecurity practices. This underscores the importance of designing training programmes tailored to each employee's profile.

According to the regression analysis and the T-test, as shown in Table 1, three main factors contributed to the level of cybersecurity awareness: Cybersecurity Training, Clarity of Organisational Policy, and Organisational Culture. The variables 'training' and 'clarity of organisational policy' showed significant positive effects, whereas the third factor, organisational culture', had a moderate effect. In addition, the model indicates that both individual security behaviours and organisational governance factors contribute to cybersecurity awareness. This suggests that organisational factors do not have an equal impact on awareness levels.

Table 1. *Regression Model Summary.*

Predictor Variable	B	SE	β	t	p
Cybersecurity training (Q6)	-0.220	0.052	-0.258	-4.231	<.001
Phishing email identification (Q10)	0.191	0.064	0.202	2.963	.003
Updating passwords (Q11)	0.126	0.059	0.138	2.130	.034
Organisational cybersecurity policies	0.228	0.068	0.231	3.367	.001
Organisational culture (Q14)	0.126	0.066	0.131	1.917	.057
Constant	1.148				0.265
	4.330	<.001			

Model Summary:
Residual SS = 143.994 (df = 205), Total SS = 224.278 (df = 211)
Dependent Variable: Cybersecurity Awareness (Q5)
Independent Variables: Q6, Q10, Q11, Q13, Q14

Summary of Key Patterns: Across the analyses performed, three common themes have emerged: (1) Training increases awareness, yet recognition of complex social engineering techniques remains

limited. (2) Clear, easily accessible policies promote security behaviour. (3) The organisation's culture, particularly management's focus on cybersecurity, increases vigilance and adherence to policies. This evidence highlights the socio-technical aspects of cybersecurity within the public sector.

4.3. Research Discussion

The research findings presented here contribute to an organised understanding of cybersecurity awareness and social engineering vulnerabilities experienced by public-sector workers in Saudi Arabia. It has been found that human-related vulnerabilities remain a major issue for the Kingdom, even after considerable investments in cybersecurity infrastructure. This finding is consistent with global evidence suggesting that most cyber incidents are linked to human error. This study has considered the application of behavioural theories and engineering principles to interpret cybersecurity vulnerabilities from a sociotechnical perspective.

Public sector employees in Saudi Arabia hold varied perceptions of cybersecurity threats, influenced by factors such as age, gender equality, and education [2, 30]. The research emphasises the need for customised awareness programs and resource-heavy training to reduce cyber risks. A positive correlation exists among gender balance, educational diversity, knowledge sharing, and compliance with cybersecurity protocols [31]. The study highlights that cybersecurity training plays a crucial role in promoting cybersecurity awareness among employees. Employees who have received structured training have shown greater awareness of social engineering tactics and have exhibited more security behaviours than their counterparts. These findings are consistent with the principles of both the NIST SATE and CSAT models, which advocate systematic and effective training. Nonetheless, the descriptive analysis indicates a lack of awareness of certain complex forms of social engineering attacks, including pretexting and baiting. Organisational policy clarity emerged as another strong predictor of awareness. Employees who reported easy access to cybersecurity policies and clear procedural guidance exhibited higher compliance and vigilance. This reinforces the relevance of the HAIS-Q model, which highlights the importance of knowledge and attitudes in shaping behaviour. The findings also underscore the engineering principle that clear procedural documentation reduces system variability and enhances reliability. Most participants display high cybersecurity awareness, thanks to ongoing training and e-learning efforts [22]. Nonetheless, gaps in training leave organisations vulnerable to social engineering tactics such as phishing, baiting, and tailgating [10]. Phishing remains a significant threat, with many employees lacking the skills to identify malicious emails and messages [32-34]. Effective training should focus on recognising urgency signals and understanding the risks of identity theft. Organisational culture significantly affects cybersecurity awareness and preparedness, highlighting the need for better policies and targeted training to protect sensitive data and combat malware [7, 35].

The impact of organisational culture was found to be moderately significant yet considerable in shaping awareness levels. A culture that promotes cybersecurity by highlighting its importance and reinforcing associated attitudes through communication helps ensure safe behaviour and increases resistance to social engineering. Such findings align well with the theoretical foundation of TPB by emphasising the importance of subjective norms and PBC. The results demonstrate the predictive significance of the combination of three organisational factors (training, policy, and culture). Together, they form a significant predictive model for cybersecurity awareness. Nevertheless, one predictor had no impact on the outcome, indicating that organisational predictors do not always prove influential. The conclusion is that human factor risks must be considered in a context-specific manner. Cybersecurity is crucial to daily operations, enhancing threat awareness and response capabilities. However, inconsistent training and limited participatory practices hamper progress. Organisations need to integrate cybersecurity into everyday routines, promote regular reporting, and foster a shared sense of responsibility to minimise vulnerabilities.

Overall, the research shows that cybersecurity awareness levels in Saudi public organisations are increasing, yet social engineering threats remain relevant due to behavioural, cognitive and organisational factors. The solution will require a combination of approaches aligned with engineering and organisational perspectives on cybersecurity management

5. Conclusion, Recommendation and Future Research

This study presents an empirical analysis of cybersecurity awareness and susceptibility to social engineering among government employees in Saudi Arabia. Although cybersecurity awareness is fairly high, significant vulnerabilities persist among public-sector workers, leaving them susceptible to social engineering cyberattacks. It found a diverse workforce with varying levels of cybersecurity understanding, revealing both strengths and areas for improvement in threat detection. While many participants demonstrated high awareness, a notable number lacked confidence in identifying phishing, indicating a need for targeted training. The findings show that cybersecurity training, policies, and organisational support play a crucial role in shaping cybersecurity awareness and behaviour. The study is important to the cybersecurity engineering domain because it incorporates behavioural theories, including protection motivation theory (PMT) and the theory of planned behaviour (TPB), to analyse human vulnerabilities within a socio-technical system. The findings will be vital in designing training programmes and other policies that could contribute to national cybersecurity. Nonetheless, inconsistent training delivery and limited policy communication pose ongoing challenges. The study achieved all five goals: assessing

awareness, identifying gaps, evaluating training programmes, analysing cultural factors, and proposing practical improvements.

Future research must adopt a longitudinal approach to assess changes in awareness and actions before and after the introduction of training programmes. Qualitative methods, such as interviews or focus groups, could provide a deeper understanding of employees' thoughts and motivating factors. Increasing the sample size and using probability sampling would improve the generalisability of the findings. Future research should test the efficacy of different training techniques, specifically simulated attacks and scenario-based training. Applying new technologies and advances in information security, such as artificial intelligence, to deliver adaptive training could be a focus area. Lastly, future research must consider the interactions between organisational culture, leadership, and human factors that may contribute to cybersecurity.

Abbreviations

CSAT	Cybersecurity Awareness Training
HAISQ	Human Aspects of Information Security Questionnaire
IT	Information Technology
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
PMT	Protection Motivation Theory
SAT	Security Awareness Training and Education
SPSS	Statistical Package for the Social Sciences
TPB	Theory of Planned Behaviour

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] K. Khando, M. S. Islam, and S. Gao, "The Emerging Technologies of Digital Payments and Associated Challenges: a Systematic Literature Review," Future Internet, vol. 15, no. 1, p. 21, Dec. 2022, https://doi.org/10.3390/fi15010021

[2] S. Burns and L. Roberts, "Applying the Theory of Planned Behaviour to predicting online safety behaviour," Crime Prevention and Community Safety, vol. 15, no. 1, pp. 48–64, Feb. 2013, https://doi.org/10.1057/cpcs.2012.13

[3] Laith Alzubaidi et al., "A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications," Journal of Big Data, vol. 10, no. 1, Apr. 2023, https://doi.org/10.1186/s40537-023-00727-2

[4] K. M. Anderson, P. W. Wilson, P. M. Odell, and W. B. Kannel, "An updated coronary risk profile. A statement for health professionals.," Circulation, vol. 83, no. 1, pp. 356–362, Jan. 1991, https://doi.org/10.1161/01.cir.83.1.356

[5] D. P. Zipes et al., "ACC/AHA/ESC 2006 Guidelines for Management of Patients with Ventricular Arrhythmias and the Prevention of Sudden Cardiac Death," Journal of the American College of Cardiology, vol. 48, no. 5, pp. e247–e346, Sep. 2006, https://doi.org/10.1016/j.jacc.2006.07.010

[6] S. Lazarus, M. Button, and A. Adogame, "Advantageous Comparison: Using Twitter Responses to Understand Similarities between Nigerian Cybercriminals ('Yahoo Boys') and Politicians ('Yahoo men')," Heliyon, p. e11142, Oct. 2022, https://doi.org/10.1016/j.heliyon.2022.e11142

[7] R. Hoheisel, G. van Capelleveen, D. K. Sarmah, and M. Junger, "The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains," Computers & Security, vol. 128, p. 103158, May 2023, https://doi.org/10.1016/j.cose.2023.103158

[8] V. Chang, L. Golightly, Q. A. Xu, T. Boonmee, and B. S. Liu, "Cybersecurity for children: an investigation into the application of social media," Enterprise Information Systems, vol. 17, no. 11, Mar. 2023, https://doi.org/10.1080/17517575.2023.2188122

[9] M. Dabas, D. Schwartz, D. Beeckman, and A. Gefen, "Application of artificial intelligence methodologies to chronic wound care and management: A scoping review," Advances in Wound Care, Apr. 2022, https://doi.org/10.1089/wound.2021.0144

[10] A. Visvizi, O. Troisi, and M. Grimaldi, "Mapping and Conceptualizing Big Data and Its Value Across Issues and Domains," Emerald Publishing Limited eBooks, pp. 15–25, Jan. 2023, https://doi.org/10.1108/978-1-80382-551-920231002

[11] S. Elo and H. Kyngäs, "The Qualitative Content Analysis Process," Journal of Advanced Nursing, vol. 62, no. 1, pp. 107–115, Mar. 2008, https://doi.org/10.1111/j.1365-2648.2007.04569.x

[12] Md. A. Uddin, M. S. Alam, A. A. Mamun, T.-U.-Z. Khan, and A. Akter, "A Study of the Adoption and Implementation of Enterprise Resource Planning (ERP): Identification of Moderators and Mediator," Journal of Open Innovation: Technology, Market, and Complexity, vol. 6, no. 1, p. 2, Dec. 2019, https://doi.org/10.3390/joitmc6010002

[13] A. L. Imoize, O. Adedeji, N. Tandiya, and S. Shetty, "6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap," Sensors, vol. 21, no. 5, p. 1709, Mar. 2021, https://doi.org/10.3390/s21051709

[14] J. U. Pedreira Junior, E. P. Galindo, A. H. Batista, C. S. Pitombo, and A. N. Rodrigues da Silva, "The panorama of public officials' meeting trips after the COVID-19 pandemic: Impact level, recovery, and prospects," Frontiers in Future Transportation, vol. 3, Oct. 2022, https://doi.org/10.3389/ffutr.2022.972133

[15] T. Cai and Z. Hong, "Exploring the structure of the digital economy through blockchain technology and mitigating adverse environmental effects with the aid of artificial neural networks," Frontiers in environmental science, vol. 12, Mar. 2024, https://doi.org/10.3389/fenvs.2024.1315812

[16] R. Issa et al., "Human migration on a heating planet: A scoping review," PLOS climate, vol. 2, no. 5, pp. e0000214, May 2023, https://doi.org/10.1371/journal.pclm.0000214

[17] Dr. Farhat Saba, D. Apollo, and S. Mehmood, "The Role, Impact, and Usage of Information Technology in Higher Education Institutions (HEIs) in Pakistan," vol. 6, no. 6, Jan. 2022, https://doi.org/10.24088/ijbea-2021-66005

[18] S. M. A. Fredeluces, N. P. Garcia, and L. A. Quines, "Extent of Utilization of Paperless Technology: basis for a Proposed Intervention Program," European Journal of Education Studies, vol. 10, no. 7, Jun. 2023, https://doi.org/10.46827/ejes.v10i7.4903

[19] M. M. Queiroz and S. Fosso Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," International Journal of Information Management, vol. 46, no. 1, pp. 70–82, Jun. 2019, https://doi.org/10.1016/j.ijinfomgt.2018.11.021

[20] A. Alammari, O. Sohaib, and S. Younes, "Developing and evaluating cybersecurity competencies for students in computing programs," PeerJ Computer Science, vol. 8, p. e827, Jan. 2022, https://doi.org/10.7717/peerj-cs.827

[21] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, vol. 23, no. 16, p. 7273, Jan. 2023, https://doi.org/10.3390/s23167273

[22] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," Heliyon, vol. 7, no. 1, p. e06016, Jan. 2021, https://doi.org/10.1016/j.heliyon.2021.e06016

[23] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," PeerJ Computer Science, vol. 7, p. e703, Sep. 2021, https://doi.org/10.7717/peerj-cs.703

[24] N. M. Alzahrani and F. A. Alfouzan, "Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review," Sensors, vol. 22, no. 7, p. 2792, Apr. 2022, https://doi.org/10.3390/s22072792

[25] H. K. Mohajan, "Quantitative research: A successful investigation in natural and social sciences," Journal of Economic Development, Environment and People, vol. 9, no. 4, pp. 50–79, Dec. 2020, https://doi.org/10.26458/jedep.v9i4.679

[26] K. A. Tamminen and Z. A. Poucher, "Research philosophies," The Routledge International Encyclopedia of Sport and Exercise Psychology, vol. 1, no. 2, pp. 535–549, Apr. 2020, https://doi.org/10.4324/9781315187259-39

[27] C. Okoli, "Inductive, Abductive and Deductive Theorizing," SSRN Electronic Journal, vol. 1, no. 1, pp. 1–8, 2021, https://doi.org/10.2139/ssrn.3774317

[28] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy, "The online survey as a qualitative research tool," International Journal of Social Research Methodology, vol. 24, no. 6, pp. 641–654, 2021, https://doi.org/10.1080/13645579.2020.1805550

[29] J. Kropko and R. Kubinec, "Interpretation and identification of within-unit and cross-sectional variation in panel data models," PLOS ONE, vol. 15, no. 4, p. e0231349, Apr. 2020, https://doi.org/10.1371/journal.pone.0231349

[30] J. Akati and M. Conrad, "Anti-Tailgating Solution Using Biometric Authentication, Motion Sensors and Image Recognition," IEEE Xplore, Oct. 01, 2021. https://ieeexplore.ieee.org/abstract/document/9730243

[31] E. Bakkalbasioglu, "How to Access Elites When Textbook Methods Fail? Challenges of Purposive Sampling and Advantages of Using Interviewees as 'Fixers,'" The Qualitative Report, vol. 25, no. 3, Mar. 2020, https://doi.org/10.46743/2160-3715/2020.3976

[32] D. Majumdar, "Rise in cyber threats make companies go for unified security command," The Economic Times, Jul. 2024. https://m.economictimes.com/jobs/hr-policies-trends/rise-in-cyber-threats-make-companies-go-for-unified-security-command/articleshow/111396990.cms

[33] Remco Spithoven and A. Drenth, "Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality," Journal of Cybersecurity, vol. 10, no. 1, Jan. 2024, https://doi.org/10.1093/cybsec/tyae010

[34] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications, vol. 58, no. 1, p. 102726, May 2021, https://doi.org/10.1016/j.jisa.2020.102726

[35] B. Mufor, A. Marnewick, and S. Von Solms, "The Development of Cybersecurity Awareness Measurement Model in the Water Sector." Available: https://papers.academic-conferences.org/index.php/iccws/article/download/43/28/66