International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(22s) 2026 pp. 573-589
https://doi.org/10.70917/ijcisim-2026-5463
Article

Strengthening Digital Security Resilience: A Framework Based on Cybersecurity, Data Privacy, and Cyber Governance

Dr. V. Mallika Vedantham

MA., Ph.D., UGC-NET, Assistant Professor of Public Administration, Tara Government College (Autonomous), Sangareddy
Mail Id: mallikavvdl@gmail.com

Abstract: Digital Security Resilience (DSR) shines a spotlight on its importance as the digital technologies continue to evolve and grow, providing organizations with additional opportunities to address cyber threats, data breach and privacy concerns. The current study explores how important the practice of Cyber security (CSP), Data privacy protection (DPP), Cyber Governance Framework (CGF) and Cyber security Awareness (CSA) are for Digital Security Resilience (DSR) in India. The quantitative approach was taken, where the data collected from 486 respondents which include students, IT professionals, academicians, research scientist and employees from different sectors and adopted both Protection Motivation Theory and Socio-Technical Systems Theory. The proposed relationships were tested with the software Partial Least Squares Structural Equation Modeling (PLS-SEM) version 3 (SmartPLS). The findings reveal the Cybersecurity Awareness's effects on Digital Security Resilience, with Cybersecurity Practices and Data Privacy Protection coming next. But the effect of Cyber Governance Framework was not statistically significant. However, this accounts for 41.9% of the variance of Digital Security Resilience; it emphasises the critical need to meld technology, privacy and consciousness into all elements of digital systems, which have strong implications for policy makers and organisations as they strive to develop digital economies.
Keywords: Cybersecurity; Data Privacy; Cyber Governance; Digital Security; Digital Security Resilience; Cybersecurity Awareness; Cybersecurity Practices; Cyber Resilience

1. Introduction

Digital technologies are a game-changer, changing how people, communities and governments are making, sharing and using information. In addition, threats such as cyber-attacks, privacy problems, etc. have emerged with the advent of innovations and economic growth that can be attributed to the use of cloud computing, artificial intelligence, big data, Internet of Things (IoT) and digital platforms (von Solms & van Niekerk, 2013; Tsai et al., 2016). In the context of an evolving business environment and the digital transformation, cybersecurity has emerged as one of the most important aspects to ensure business continuity, protect critical information resources and maintain trust in digital ecosystems (Seshanna et al., 2025). To resist cyberattacks, data breaches, phishing and identity theft, and to recover from them, the mechanisms used in cybersecurity need to be resilient (Bada et al., 2019). As a result, Digital Security Resilience (DSR) has been increasingly gaining attention both within the research and practice communities as a key competency to maintain secure and trustworthy digital environments.

India is an interesting place to study digital security resilience. India is one of the world's fastest growing digitally advanced economies, with online shopping and e-commerce, digital banking, digital governance initiatives, and even internet connectivity, rapidly shaping up the Indian digital landscape (Sharma, 2023). At the same time, with a growing reliance on digitisation, information security, cybercrime and privacy issues have risen to a higher level of cybersecurity issues. The impact of digital security resilience has been studied separately in several fields including

cybersecurity practices, privacy concerns, and governance mechanisms, however, the factors influencing Digital Security Resilience are not fully comprehended, especially in new and emerging digital economies (Martin & Murphy, 2017; Parsons et al., 2014). The literature so far has mainly dealt with technological aspects and thus given relatively little attention to the interaction between the dimensions of behaviour, organisation and governance.

There are a number of research lacunae in the literature. First, in general, cybersecurity practices, data privacy protection, and cybersecurity awareness have been studied separately, but their overall effect on digital resilience is not that well explored in the empirical literature. Second, Guidelines around Cyber Governance as institutional mechanisms are predominant and always recognised as being necessary but empirical knowledge about the effectiveness of enhancing cyber-resilience with the help of cyber governance frameworks is still lacking and theoretically underdeveloped (von Solms & van Niekerk, 2013). Third, much of the research to date has focused solely on the technological aspects of resilience building and neglected to consider the role of human behavior and cybersecurity culture in resilience outcomes (Parsons et al., 2017). Fourthly, although emerging economies are increasingly becoming important, there is limited empirical evidence of the cyber resilience of some of these economies, like India. Lastly, very few studies have taken a holistic view of theory incorporating at the same time the cognitively, technically, organizationally, and institutionally related aspects.

In order to overcome these gaps, an integrated framework is proposed and its influence on Digital Security Resilience validated in terms of Cybersecurity Practices (CSP), Data Privacy Protection (DPP), Cyber Governance Framework (CGF), and Cybersecurity Awareness (CSA) thereby. The study's conceptualization of resilience is derived from Protection Motivation Theory (PMT; Rogers, 1975, 1983), Socio-Technical Systems (STS; Trist & Bamforth, 1951), cybersecurity culture perspectives, and cyber governance perspectives, and believes resilience is a multi-faceted result of the interplay between technological protection, behavioral ability, and organizational mechanisms.

The novelty of this research is in three important aspects. Digital Security Resilience is not just a technological phenomenon, but is understood as the outcome of various mechanisms, comprising the cognitive, technical and governance aspects. Second, the link between behavioral, organizational and institutional views is combined in a coherent framework and found to be testable. Third, this study enriches the cyber resilience literature with evidence from India giving it a more international character than has been found in much previous works, which were mainly oriented towards the western world.

This study would add to the body of literature in various ways. Theoretically, it builds on Protection Motivation Theory and Socio-Tech models that identify how the interplay of Awareness, Privacy mechanisms, Governance structures and Cyber security Practice will help build Resilience. It provides empirical evidence for a digital economy which is rapidly undergoing digital transformation. The findings of the study provide inputs to policy makers and cybersecurity practitioners. The interdependency of technological, behavioural and organizational mechanisms is explained in this study, contributing to an understanding of digital security resilience in the current complex cyber landscape.

2. Literature Review

To develop the study hypotheses and conceptual framework, an extensive review of the cybersecurity, information systems, and digital resilience literature was undertaken. Despite the extensive body of scholarly work in the past few years on cybersecurity and data privacy, the combination of cybersecurity best practices and data privacy protection into a single framework explaining Digital Security Resilience (DSR) is relatively under explored, especially in emerging digital economies (Nafees & Kumar, 2023). Nowadays, the focus on cyber resilience is shifting from a technological infrastructure towards mechanisms that have behavioral, organizational, and governance dimensions (Bada et al., 2019; von Solms & van Niekerk, 2013). Moreover, there are mixed evidence on the role of governance mechanisms in improving the cyber resilience. Thus, in order to be able to investigate the direct antecedents of Digital Security Resilience and develop hypotheses, the present review examines the previous theoretical and empirical evidence.

2.1 Cybersecurity Practices and Digital Security Resilience

Cybersecurity is one of the most important tools used to safeguard an organization's information assets and ensure operational continuity. Cybersecurity practices include preventive and corrective measures such as risk assessment, threat detection, access control, vulnerability management and incident response procedures (NIST, 2018). Good cybersecurity practices help minimize the impact an organization can have from cyber threats and increase the resilience of an organization against disruption. The studies recently indicate that proactive security measures can significantly enhance the resilience and business continuity in digital environment (Shameli-Sendi et al., 2016).

With digital technologies becoming more fundamental to everyday life, so do the threats they face that can be very sophisticated and require constant monitoring and adaptation. Companies by taking up cybersecurity measures can detect vulnerabilities, reduce risks and can even operate in a secure way. Digital Security Resilience shall be improved by strengthening preparedness and recovery capacities, hence good cybersecurity practices. Thus:

H1: Cybersecurity Practices positively influence Digital Security Resilience.

2.2 Data Privacy Protection and Digital Security Resilience

The security of data and the protection of privacy are crucial in a secure digital world. Data Privacy refers to the procedures and guidelines that are meant to secure personal and sensitive data from unauthorized access, misuse and disclosure (Martin & Murphy, 2017). With the emergence of numerous digital platforms, cloud computing, and online services, privacy and information leakage issues are becoming more prevalent. Strong privacy protections reduce risks of cyber-attacks, and heighten users' confidence in digital systems. Implementing robust privacy controls can help mitigate the risks associated with data and maintain the integrity of the organization's operations (Ewoh et al., 2025). Previous research indicates that privacy protection plays a key role in the digital trust and resilience of organizations, by reducing the likelihood and consequences of cyber incidents (Acquisti et al., 2015). Thus, institutions that have strong data protection systems are more likely to have high Digital Security Resilience. Thus:

H2: Data Privacy Protection positively influences Digital Security Resilience.

2.3 Cyber Governance Framework and Digital Security Resilience

Cyber governance is the policies, standards, regulatory mechanisms and accountability structures that define cybersecurity activities in organisations (von Solms & van Niekerk, 2013). Strategic decision making, compliance with regulatory requirements, risk management, resource allocation and strategic decision making for cybersecurity all benefit from effective governance frameworks. Governance mechanisms are now being acknowledged as key elements of cybersecurity management and digital transformation.

Klimburg (2017) stated that coordination and clear responsibilities for security would increase the resilience when it comes to cyber governance. Governance systems tend to focus more on adherence to policies and good governance practices than on operational security skills. As such, they are effective only if governance mechanisms are linked with technological and human resources. Although governance structures are becoming more relevant, there are few empirical studies on their role in cyber resilience. The conceptual relationships among these constructs are shown in Figure 1. Therefore, it is proposed that:

H3: Cyber Governance Framework positively influences Digital Security Resilience.

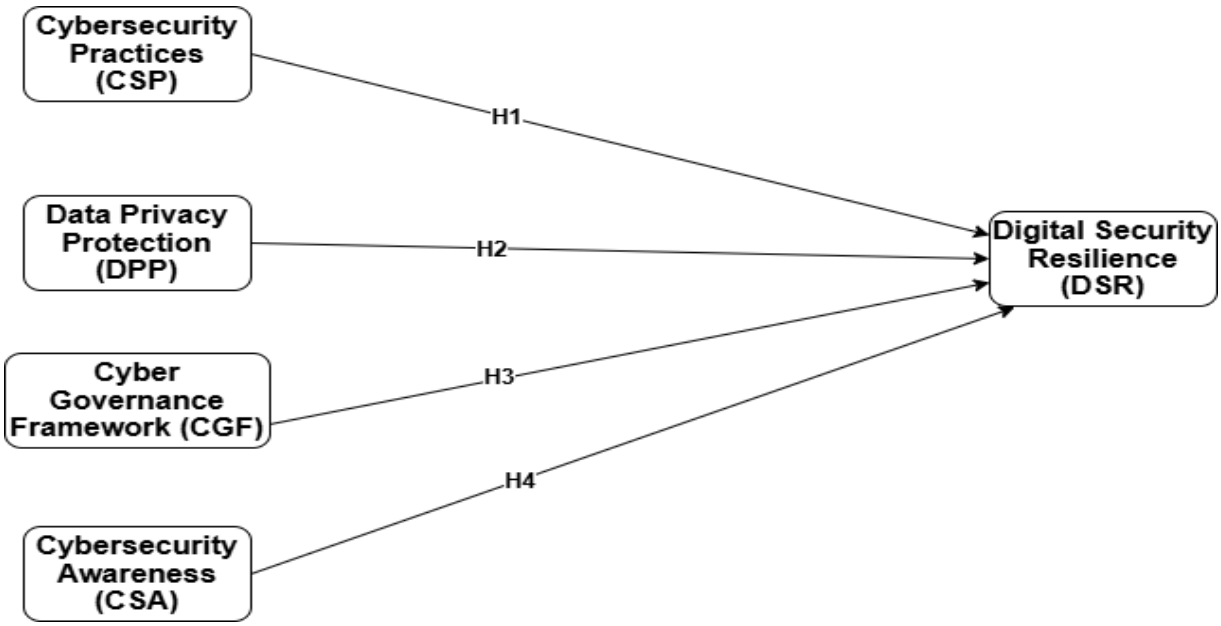

Figure 1. Conceptual framework

Source: Author's own work

2.4 Cybersecurity Awareness and Digital Security Resilience

The human aspect of cybersecurity is now a pivotal one that is more widely acknowledged in this field. Cybersecurity awareness is people's understanding of cyber threats, vulnerabilities, and safe online practices (Parsons et al., 2014). Lack of awareness is one of the biggest reasons for having a cyber security incident and awareness is a critical component of cyber resilience.

By raising awareness about security, people can identify phishing attacks, malware, social engineering schemes, and other potential cyber threats. Earlier research has shown that awareness programmes are important in ensuring safe behaviour and making it harder to gain successful cyberattacks (Bada et al., 2019). Moreover, increased awareness facilitates threat identification and increases response capacity, which boosts cyber resilience. Cybersecurity awareness is expected to be a key component in improving Digital Security Resilience, alongside technological solutions, as cyber resilience requires human action as well as technology. Thus:

H4: Cybersecurity Awareness positively influences Digital Security Resilience.

3. Theory-Based Framework

The current study proposes a theoretically informed framework to explain the concept of Digital Security Resilience (DSR) which is a combined effect of Cybersecurity Practices (CSP), Data Privacy Protection (DPP), Cyber Governance Framework (CGF), and Cybersecurity Awareness (CSA). The framework is mainly based on Protection Motivation Theory (PMT) (Rogers, 1975; Rogers, 1983), Socio-Technical Systems Theory (Trist & Bamforth, 1951) and Cybersecurity Culture perspectives. New cybersecurity studies highlight the importance of cognitive, behavioral, and organizational mechanisms for digital resilience, which will not be just the technology itself, but also how people think, behave, and act of the organization as a whole in order to prevent, withstand, and recover from cyber disruptions (Bada et al., 2019). Thus, Digital Security Resilience is considered to be the result of a multidimensional process, in which the components of technology-based protection, privacy protection, governance and awareness contribute to increasing the resilience to cyber-attacks.

3.1 Protection Motivation Theory (PMT)

The primary theoretical framework for the understanding of protective behavior against threats is Protection Motivation Theory (PMT) proposed by Rogers (1975) and later by Rogers (1983). PMT outlines two cognitive appraisal processes as threat appraisal and coping appraisal that involve individuals' actions when deciding on protective measures. Threat appraisal refers to the assessment of threat severity and threat vulnerability, coping appraisal refers to response efficacy, self-efficacy and perceived effectiveness of coping mechanisms.

Within the framework of cybersecurity, Cybersecurity Awareness is equivalent to threat appraisal as people with a higher awareness are better able to recognize cyber threats and the repercussions of a cyber-attack. Coping mechanisms are: Cybersecurity Practices and Data Privacy Protection, each offering practical and technical answers to tackle cyber risks. Those individuals and organizations that detect cyber threats and have effective protective capability are more likely to develop Digital Security Resilience. Recent research has shown that PMT offers a strong theoretical grounding for understanding cybersecurity behavior (Ifinedo, 2012; Tsai et al., 2016) and information security compliance (Tsai et al., 2016). The present framework continues with PMT by making Digital Security Resilience the last line of defense in cognitive and behavioral reactions to cyber threats.

3.2 Socio-Technical Systems Theory

Socio-Technical Systems Theory (STST) states that the outcomes of an organization are the result of how technological systems and social systems relate to one another (Trist & Bamforth, 1951). The theory explains that for ensuring effective performance in an organisation, there should be an integration of human capabilities, organizational structures, and technological resources.

This vision defines Cybersecurity Practices as the technological aspect and Cybersecurity Awareness as the human aspect of the socio-technical system within the present framework. Organizational mechanisms for coordination and control include Data Privacy Protection and Cyber Governance Framework. Digital Security Resilience, according to STST, is a symbiotic combination of technical security and human capabilities. Hence, resilience is not only about technological infrastructure but it is a product of the interplay between technology, people and governance mechanisms. Few recent studies on cyber resilience also highlight the need for socio-technical integration to boost organizational resilience against cyber threats (Bada et al., 2019).

3.3 Cybersecurity Culture Perspective

Cybersecurity culture is the collective psychology, attitudes, values and practices that shape and influence cybersecurity-related behaviors in organizations (Parsons et al., 2017). Given that many cyber incidents stem from behavioural vulnerabilities and not technological ones, human factors have come under increasing focus as one of the most critical factors in the success of cybersecurity.

From the proposed perspective, Cybersecurity Awareness is a cultural and cognitive mechanism that helps foster secure behaviours and mitigate risks associated with humans. People with more phishing awareness, malware awareness, social engineering awareness, and secure online practices are more likely to be a part of the organizational resilience. Similarly, Cybersecurity Practices and Data Privacy Protection help foster a security culture through practices and mechanisms that promote safe digital behavior. Hence, cybersecurity culture views indicate that resilience is a matter of both formal technologies as well as behavioral norms and shared awareness.

3.4 Cyber Governance Perspective

The institutional and regulatory aspect of cybersecurity is Cyber Governance Framework (CGF). According to von Solms & van Niekerk (2013), cyber governance is a framework of policies, standards, accountability mechanisms and strategic guidelines that guide the activities of Cyber Security in an organization. Cyber security readiness and risk management depends upon the regulatory frameworks.

However governance mechanisms may not directly lead to resilience if they are poorly implemented and lack technological and human capacities. Hence, Cyber Governance Framework is not considered as a standalone enabler of resilience but rather as a support mechanism to security practices and awareness. This is because governance structures can have less direct impacts than operational and behavioural factors, this is the perspective.

3.5 Integrating Theoretical Perspectives

A combination of Protection Motivation Theory, Socio-Technical Systems Theory, Cybersecurity Culture perspectives and Cyber Governance perspectives will yield a complete explanation of Digital Security Resilience. In the present framework, in contrast to cybersecurity being a purely technological phenomenon, the concept of resilience is defined as a multi-dimensional phenomenon arising from the interplay among cognitive, behavioral, organizational and technological mechanisms. The mental or cognitive part of threat appraisal and security culture is Cybersecurity Awareness. Coping mechanisms and technological responses to cybersecurity challenges are evident in Cybersecurity Practices and Data Privacy Protection. Cyber Governance Framework is an institutional structure which enables coordination and strategic cyber security management. These mechanisms, when combined, create the ability for individuals and organisations to anticipate, withstand, recover from and adapt to cyber threats to enhance Digital Security Resilience.

In the context of this, the present model assumes that Cybersecurity Practices, Data Privacy Protection, Cyber Governance Framework, and Cybersecurity Awareness positively influence Digital Security Resilience. The study covers all four aspects of cyber resilience, namely behavioral, technological, organizational and institutional, thus giving a comprehensive description of the phenomenon and adding to the literature on cybersecurity and digital resilience in the emerging digital economies.

4. Research Methodology

4.1 Research Design and Data Collection

The present study was a quantitative research method with the intention of studying the influence of Cybersecurity Practices (CSP), Data Privacy Protection (DPP), Cyber Governance Framework (CGF), Cybersecurity Awareness (CSA) on Digital Security Resilience (DSR). The conceptual framework and hypotheses were formulated in light of theory and empirical work in the fields of cyber security, data privacy, information systems and cyber governance. Based on this, the study was conducted with four independent variables (Cybersecurity Practices, Data Privacy Protection, Cyber Governance Framework, Cybersecurity Awareness), and one dependent variable (Digital Security Resilience). Purposive sampling technique was used since the subjects required to be familiar with digital technologies, online platforms, cyber security issues and digital information systems. The target population comprised university students, IT, academicians, researchers, Government employees, employees in the private sector who usually interact with digital platforms and are exposed to cybersecurity-related practices. The respondents were chosen to reflect the diversity and enhance the representativeness of the sample from various educational and professional backgrounds.

A total of 486 valid data were obtained from respondents from different organizations across the different higher educational institutions and professional fields in India. The responses were screened meticulously before analysis to remove that of those questionnaires which were incomplete, and inconsistencies, thus enhancing accuracy and reliability of the data. The sample size is suitable for the requirements of Structural Equation Modeling (SEM) because previous studies have recommended that more than 200 observations is enough for PLS-SEM analysis (Hair et al., 2019). Primary data collection was conducted by structured questionnaire, which was mostly completed by Google Forms and professional and academic online networks. Prior to the main survey, a pilot study was conducted to determine the clarity, reliability and appropriateness of the measurement items. Some minor changes were made to enhance the questionnaire based on the feedback that was received at the pilot phase. There were two sections to the questionnaire. Data on the respondents' demographics were collected in the first section and the second section

collected data on the study constructs of Cybersecurity Practices, Data Privacy Protection, Cyber Governance Framework, Cybersecurity Awareness, and Digital Security Resilience.

There were 26 indicators initially in the measurement model. Six items measured Cybersecurity Practices (CSP1 – CSP6), six items measured Data Privacy Protection (DPP1 – DPP6), six items represented Cyber Governance Framework (CGF1 – CGF6), six items measured Cybersecurity Awareness (CSA1 – CSA6), and six items captured Digital Security Resilience (CR1 – CR6). In the assessment of the Measurement Model in SmartPLS 3, some signs with an outer loading less than the recommended value of 0.70 were eliminated in order to strengthen the model and ensure a level of consistency in the model signs. In particular, the following were not included in further analysis: CSP3 and CSP6, DPP6, CGF1, CSA1, CSA2, CSA6 and CR4–CR6. These were then left in the final model for subsequent statistical analysis: CSP1, CSP2, CSP4, CSP5, DPP1–DPP5, CGF2–CGF5, CSA3–CSA5, and CR1–CR3. All items were scored by a five-point likert scale from Strongly Disagree (1) to Strongly Agree (5). The scale format was adopted and modified to suit the purpose and context of the present study from existing studies that had previously been validated.

The collected data had been analyzed using SmartPLS 3 software. Descriptive statistics, reliability assessment, convergent validity, discriminant validity, and collinearity assessment were conducted along with evaluating the structural model. Moreover, in order to test the significance of hypothesized relationships among the variables, the bootstrapping procedure with 5,000 resamples was employed. It was found that Cybersecurity Practices, Data Privacy Protection and Cybersecurity Awareness are significant positive factors whereas Cyber Governance Framework is insignificant.

Table 1. Demographic Statistics

Category	**Frequency (n)**	**Percentage (%)**
Gender		
Male	292	60.1
Female	194	39.9
Age		
18–25 years	198	40.7
26–35 years	176	36.2
Above 35 years	112	23.1
Educational Qualification		
Undergraduate	146	30.0
Postgraduate	218	44.9
Doctorate	74	15.2
Others	48	9.9
Occupation		
Students	172	35.4
IT Professionals	118	24.3
Academicians/Researchers	82	16.9
Government Employees	56	11.5
Private Sector Employees	58	11.9

Experience with Digital Platforms		
Less than 3 years	124	25.5
3–5 years	173	35.6
More than 5 years	189	38.9
Primary Use of Digital Services		
Online Banking and Payments	156	32.1
E-commerce Platforms	104	21.4
Educational and Research Platforms	126	25.9
Professional/Organizational Systems	100	20.6

Note: n = frequency.

Source(s): Authors' own compilation based on survey data.

Table 1 presents the demographic characteristics of the respondents. Among the 486 respondents, 60.1% were male and 39.9% were female. Approximately 40.7% of the respondents belonged to the 18–25 years age category, followed by 36.2% between 26–35 years and 23.1% above 35 years of age. As far as education is concerned, 44.9% of the respondents were post graduates, 30.0% were under graduates, 15.2% were doctoral scholars and 9.9% were others. The students group (35.4%) was the largest group followed by IT professionals (24.3%), academicians and researchers (16.9%), private sector employees (11.9%) and government employees (11.5%) in terms of occupation. In addition, 38.9% of respondents stated that they had over 5 years of experience with digital platforms. Regarding the main purpose of digital service use, online banking and payment systems were used most (32.1%), followed by educational and research platforms (25.9%), e-commerce platforms (21.4%) and professional or organizational systems (20.6%). The demographic profile shows that the sample is representative of digitally active individuals with good exposure to cybersecurity and digital technologies, which makes it suitable for the purpose of investigating the determinants of Digital Security Resilience.

5. Data Analysis Technique

The present study used Partial Least Squares Structural Equation Modeling (PLS-SEM) in the use of software SmartPLS to analyze the relationship between Cyber Governance Framework (CGF), Cybersecurity Awareness (CSA), Cybersecurity Practices (CSP), Data Privacy Protection (DPP), and Digital Security Resilience (DSR). The popularity of PLS-SEM in management and information systems research is due to its ability to be applied in predictive analysis, complex models, and latent variable estimation (Hair et al., 2019). Unlike the covariance-based structural equation modeling, PLS-SEM does not require strong multivariate normal distributional assumption and is suitable for exploratory and prediction studies (Hair et al., 2022). Considering the goal of the present study, which is investigating the impact of cybersecurity-related dimensions on digital security resilience, PLS-SEM is the most suitable method for analysis.

Data analysis included two-step procedure. In the first phase the measurement model was evaluated to check the reliability of the indicators, internal consistency reliability, convergent validity and discriminant validity. The second stage involved the evaluation of the structural model, which was used to test the hypothesized relationships among the constructs.

5.1 Measurement Model Assessment

The measurement model was evaluated following the recommendations of Hair et al. (2019). During the measurement model assessment, several indicators exhibiting outer loadings below the recommended threshold value of 0.70 were excluded from the final model to improve reliability and validity. Specifically, CGF1, CSA1, CSA2,

CSA6, CSP3, CSP6, and DPP6 were removed. After eliminating these indicators, all retained items demonstrated satisfactory loading values exceeding the recommended threshold of 0.70, thereby confirming indicator reliability.

The values reported for the indicators on the Cyber Governance Framework (CGF) ranged from 0.708 to 0.811. Likewise, the values of the indicators of Cybersecurity Awareness (CSA) ranged from 0.755 to 0.886. The loading values for Cybersecurity Practices (CSP) ranged from 0.705 – 0.830 while the loading values for Data Privacy Protection (DPP) ranged from 0.703 – 0.870. Additionally, the loading values for the indicators of Digital Security Resilience (DSR) ranged from 0.842 to 0.884, which were fairly high. All indicators were found to be above the minimum value of the indicator reliability, 0.70, which means that the indicators were considered acceptable (Hair et al., 2022).

The internal consistency reliability was tested with Cronbach's alpha, rho_A, and Composite Reliability (CR). The results showed Cronbach's alpha values varying from 0.758 to 0.854 which is above the minimum value of 0.70 recommended by Nunnally and Bernstein (1994). Similarly, the rho_A values ranged from 0.759 to 0.858, and the composite reliability values ranged from 0.846 to 0.896, indicating good internal consistency reliability in the measurement items (Dijkstra & Henseler, 2015). Average Variance Extracted (AVE) was used to evaluate the convergent validity. The range of the AVE value was between 0.580 and 0.743, which is higher than the threshold value recommended by Fornell and Larcker (1981), which is 0.5. So as far as convergent validity was concerned, all constructs were validated. Two measures were used to assess the discriminant validity: Fornell-Larcker criterion and Heterotrait-Monotrait ratio (HTMT). The Fornell-Larcker criterion was used to check discriminant validity, and the square root of the average variance extrapolated (AVE) for each construct was greater than the correlations between the constructs, indicating discriminant validity (Fornell & Larcker, 1981). Furthermore, the values of the HTMT were between 0.564 and 0.783, which were lower than the recommended value of 0.85 proposed by Henseler et al. (2015). Therefore, there was sufficient discriminant validity among the constructs. The results of measuring models showed that the overall measurement model had good psychometric properties, meaning that the constructs were appropriate for further analysis of the structural model.

The results of indicator loadings, reliability and convergent validity are shown in Table 2 while the results of discriminant validity by Fornell-Larcker criterion and HTMT ratio are shown in Tables 3 and 4, respectively.

Table 2. Factor Loadings, Reliability, and Convergent Validity

Construct	Code	Loading	Alpha	rho_A	CR	AVE
Cyber Governance Framework (CGF)	CGF2	0.708	0.758	0.759	0.846	0.580
	CGF3	0.766				
	CGF4	0.811				
	CGF5	0.758				
Cybersecurity Awareness (CSA)	CSA3	0.755	0.780	0.796	0.873	0.696
	CSA4	0.856				
	CSA5	0.886				
Cybersecurity Practices (CSP)	CSP1	0.738	0.784	0.806	0.859	0.604
	CSP2	0.705				
	CSP4	0.830				
	CSP5	0.828				
Data Privacy Protection (DPP)	DPP1	0.772	0.854	0.858	0.896	0.634

	DPP2	0.846				
	DPP3	0.870				
	DPP4	0.778				
	DPP5	0.703				
Digital Security Resilience (DSR)	CR1	0.884	0.826	0.828	0.896	0.743
	CR2	0.859				
	CR3	0.842				

Note: α = Cronbach's Alpha; ρA = Dijkstra–Henseler's rho_A; CR = Composite Reliability; AVE = Average Variance Extracted.

Source(s): Authors' own calculations using SmartPLS.

Table 3. Discriminant Validity Assessment Using Fornell–Larcker Criterion

Constructs	CGF	CSA	CSP	DPP	DSR
CGF	0.762				
CSA	0.517	0.834			
CSP	0.473	0.467	0.777		
DPP	0.593	0.473	0.665	0.796	
DSR	0.450	0.564	0.505	0.515	0.862

Note: Diagonal values represent the square root of the Average Variance Extracted (AVE). CGF = Cyber Governance Framework; CSA = Cybersecurity Awareness; CSP = Cybersecurity Practices; DPP = Data Privacy Protection; DSR = Digital Security Resilience.

Source(s): Authors' own calculations using SmartPLS.

Table 4. Heterotrait-Monotrait Ratio (HTMT)

Constructs	CGF	CSA	CSP	DPP	DSR
CGF	-				
CSA	0.673	-			
CSP	0.596	0.583	-		
DPP	0.724	0.570	0.783	-	
DSR	0.564	0.699	0.610	0.610	-

Note: HTMT = Heterotrait–Monotrait Ratio; CGF = Cyber Governance Framework; CSA = Cybersecurity Awareness; CSP = Cybersecurity Practices; DPP = Data Privacy Protection; DSR = Digital Security Resilience.

Source(s): Authors' own calculations using SmartPLS.

5.1.1 Collinearity Assessment

The Variance Inflation Factor (VIF) was used for the collinearity between indicators. Hair et al. (2022) said VIF < 5.0 is no indication of multicollinearity, whereas Kock (2015) said that the more conservative indicator of VIF value < 3.3 is no sign of multicollinearity. The findings indicated that all of the VIF values were within the range 1.256 to 2.793, which were below the recommended VIF value range of 10. The result showed that all the VIF value

obtained were within the range of 1.256-2.793 which were far below the recommended range of VIF value 10. So, a concern about collinearity was not observed as the indicators were not correlated with each other, and they were appropriate for further analysis. Table 5 shows the results of the collinearity assessment.

Table 5. Collinearity Assessment (VIF)

Indicator	VIF
CGF2	1.256
CGF3	1.606
CGF4	1.649
CGF5	1.570
CR1	2.069
CR2	1.915
CR3	1.736
CSA3	1.390
CSA4	1.861
CSA5	1.968
CSP1	1.616
CSP2	1.477
CSP4	1.756
CSP5	1.748
DPP1	1.675
DPP2	2.628
DPP3	2.793
DPP4	1.877
DPP5	1.453

Note: VIF = Variance Inflation Factor.

Source(s): Authors' own calculations using SmartPLS.

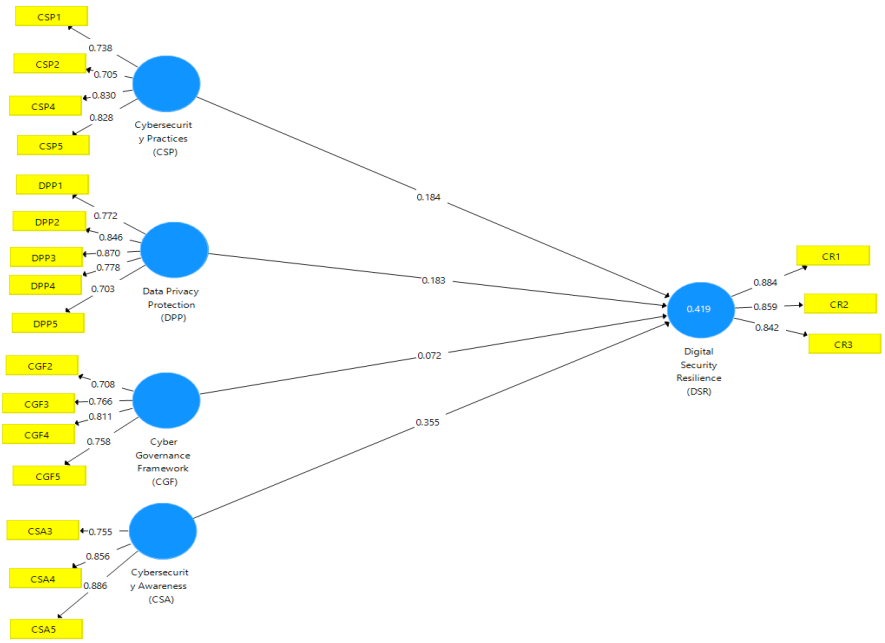

Figure 2: Structural Model Results of the PLS-SEM Analysis

5.2 Structural Model Assessment

The reliability and validity of the measurement model were tested prior to evaluation of the structural model, which was tested using the bootstrapping procedure in SmartPLS 3 with 5,000 bootstraps to examine the proposed hypotheses.

H1 suggested that Digital Security Resilience (DSR) is positively affected by Cybersecurity Practices (CSP). The results revealed a significant positive relationship between Cybersecurity Practices and Digital Security Resilience ($\beta = 0.184$, $t = 4.212$, $p < 0.001$). The p-value is less than the recommended value of 0.05 which means that H1 is accepted. The results indicate that good cybersecurity practices enhance an organisation's ability to resist and recover from cyber threats and disruptions.

H2 said, Data Privacy Protection (DPP) has a positive impact on Digital Security Resilience. The results revealed that there was a significant positive correlation between Data Privacy Protection and Digital Security Resilience with $\beta = 0.183$, $t = 3.590$, $p < 0.001$. Therefore, H2 is recommended. This result indicates that data protection is a key component of digital resilience because it minimises vulnerabilities and risks associated with data breaches or unauthorised access.

H3 suggested that Cyber Governance Framework (CGF) has a positive impact on Digital Security Resilience. The results, however, showed a positive (but insignificant) relationship of Cyber Governance Framework to Digital Security Resilience ($\beta = 0.072$, $t = 1.614$, $p = 0.107$). The value of the p is greater than recommended value of 0.05, hence H3 is rejected. This discovery indicates that governance frameworks and regulatory frameworks alone could not ensure digital resilience without the help of effective cybersecurity measures and awareness campaigns.

H4 said, Cybersecurity Awareness (CSA) has a positive impact on Digital Security Resilience. The result indicated that there was a significant high correlation between Cybersecurity Awareness and Digital Security Resilience ($\beta = 0.355$, $t = 7.776$, $p < 0.001$). So, H4 is supported. The findings indicate that increase in awareness of cyber threats and secure digital practice will enable better prevention of cyber incidents and enhance the resilience of the organization.

Overall, Cybersecurity Awareness had the most significant effect on Digital Security Resilience, while Cybersecurity Practices and Data Privacy Protection were the next most significant. The role of awareness and knowledge in improving cyber risk resilience and building a secure digital environment is highlighted. The complete results of the structural modelling assessment are given in Table 6 and Figure 2.

Table 6. Structural Model Assessment

Hypothesis	Predictor	Outcome	β	Std. Dev	t-value	p-value	Decision
H1	Cybersecurity Practices (CSP)	Digital Security Resilience (DSR)	0.184	0.044	4.212	0.000	Supported
H2	Data Privacy Protection (DPP)	Digital Security Resilience (DSR)	0.183	0.051	3.59	0.000	Supported
H3	Cyber Governance Framework (CGF)	Digital Security Resilience (DSR)	0.072	0.045	1.614	0.107	Not Supported
H4	Cybersecurity Awareness (CSA)	Digital Security Resilience (DSR)	0.355	0.046	7.776	0.000	Supported

Note: β = beta coefficient; Std. Dev = standard deviation; t = t-statistic; p = probability value. Relationships are considered significant at $p < 0.05$.

Source(s): Authors' own calculations using SmartPLS.

Figure 3. Bootstrapping Results of the Structural Model

6. Discussion

In the current study, the four variables namely, Cybersecurity Practices, Data Privacy Protection, Cyber Governance Framework, Cybersecurity Awareness have been examined for their effect on Digital Security Resilience among digitally active people in India. The findings contribute to the growing amount of research that investigates cybersecurity and digital resilience in the interconnected world, providing empirical insights into technological, organizational, and human factors that affect cyber resilience.

Cybersecurity Awareness was the most important indicator of Digital Security Resilience. This is consistent with the earlier research which has underscored the importance of human behavior as one of the most critical factors in achieving success in cybersecurity (Parsons et al., 2017). The results show that the more aware people are of phishing attacks, malware, social engineering methods and safe online behavior, the more well-prepared they will be when it comes time to detect threats and respond effectively if a cyber incident occurs. Recent research also suggests that awareness and security culture are also becoming an important component of cyber resilience as human error continues to be one of the major causes of cyber security breaches (Bada et al., 2019). Thus, digital resilience seems to rely on both technical skills and user knowledge and readiness in digital ecosystems.

Additionally, Cybersecurity Practices had a significant positive impact on Digital Security Resilience. These results align with past studies which have shown improvements in an organization's ability to resist and recover from a cyberattack as a result of proactive security measures such as threat detection systems, risk assessments and incident response protocols (NIST, 2018). Implementing good cyber security practices will help to ensure continuity of operations and reduce cyber risks. The resilience of the organisation depends upon it investment in cybersecurity defence and protection.The outcome of the study indicates that cybersecurity should become a part of continuous process in the organisation strategy.

It is recommended to emphasize programmes on awareness creation, cyber security training and development of cyber security culture as these have turned out to be the most important in determining Digital Security Resilience (Haney et al., 2022). Ongoing education about phishing, password maintenance, social engineering and safe digital practices can significantly diminish vulnerabilities induced by humans and improve the resilience (Bada et al., 2019). In addition, the need for organizations to take proactive measures, including conducting risk assessments, monitoring threats, managing vulnerabilities, and developing incident response plans, to ensure the continuity of operations (NIST, 2018) is paramount.

Positive impact of data privacy protection calls for policy makers and organisations to strengthen data privacy laws and have a policy by design, that will build digital trust and minimise the risks of unauthorised access and data breaches (Martin & Murphy, 2017). The overall results show that a multi-faceted approach to digital security resilience is needed that includes technological security measures, cybersecurity awareness, privacy protection measures and governance capabilities. This comprehensive approach is necessary for creating safe, robust and reliable digital environments in ever-evolving digital landscapes.

To the contrary, Cyber Governance Framework was not statistically significant with respect to Digital Security Resilience. While cyber governance mechanisms create policy, standards and regulatory frameworks, their direct role in fostering cyber resilience seems to be limited. This finding partially validates previous arguments that have indicated a linkage between cyber security awareness, operational capabilities, and governance frameworks in order to achieve cyber security effectiveness (von Solms & van Niekerk, 2013). While many organizations focus on regulatory compliance, implementation, security culture, and preparedness of their employees are typically less focused. Thus, governance systems can be viewed as enablers of resilience but not necessarily as drivers of resilience. Since the relationship between the insignificant values in this study, cyber governance should be linked to technological and behavioral aspects to achieve meaningful security results.

Overall, Cybersecurity Awareness and Cybersecurity Practices and Data Privacy Protection had the most significant impact on Digital Security Resilience. This discovery underscores the significance of adopting a human-

centric approach to cybersecurity and further emphasizes that it is not possible to create digital resilience through investment in technology alone. Instead, a holistic approach is needed, including privacy protection measures, effective security protocols, and awareness campaigns. The results also show that cybersecurity problem is multi-dimensional and as such, the technological, organizational and behavioral approach should be combined to solve the problem.

Finally, the coefficient of determination $R^2 = 0.419$ means that together, Cybersecurity Practices, Data Privacy Protection, Cyber Governance Framework and Cybersecurity Awareness explain 41.9% of the variance in Digital Security Resilience, which is a moderate amount of variance. The result of the study reveals that even though the present proposed model

included major factors that influence digital resilience, for further comprehending concept of digital resilience, other important other aspects like the adoption of artificial intelligence, perception of cyber risk, organizational culture, digital trust, and technological readiness have to be considered.

The overall results show that the notion of Digital Security Resilience mostly relies on knowledge on cybersecurity, good practices, and data privacy protection. In view of this, organisations would be well advised to build up their cybersecurity expertise and user employee awareness of cyber threats hand in hand with governance and compliance. This comprehensive approach plays a vital role in creating secure, trustworthy, and resilient digital environments.

7. Theoretical and Practical Implications

The present study extends the previous cybersecurity studies around Digital Security Resilience by suggesting that it is not a cybersecurity product, but rather a multi-faceted concept comprising the dimensions of cybersecurity practices, data privacy protection, governance mechanisms and cybersecurity awareness. Findings corroborate Protection Motivation Theory (PMT) (Rogers, 1975) as a theory of protective behavior that assumes that threat appraisal and coping appraisal predict protective behavior and resilience outcomes. In particular, cybersecurity awareness acts as a threat appraisal and cybersecurity practices and data privacy protection serve as coping mechanisms that facilitate the efficacy of the cybersecurity responses and increase cyber threat resilience (Tsai et al., 2016). The study extends PMT by making cognitive, behavioral, and technological mechanisms work together to drive Digital Security Resilience as the outcome.

Significantly, the negligible correlation between Cyber Governance Framework (CGF) and Digital Security Resilience further sheds light on the pre-existing notions of cyber governance.Importantly, the near-zero correlation between Cyber Governance Framework (CGF) and Digital Security Resilience further polishes the previously existing notions about Cyber Governance. While governance aspects are widely seen as important pillars of cybersecurity management, the findings indicated that a policy and/or regulatory framework is inadequate to enhance cyber-resilience without having operation capabilities and cybersecurity awareness to back them up (von Solms & van Niekerk, 2013). Moreover, the outcomes align with socio-technical viewpoints that acknowledge resilience arises not only as technological arrangement but also as the dynamics between the human competences and the technology. Cybersecurity awareness is a strong enabler, indicating that behavioral factors and the aspect of cybersecurity culture, deserve importance in explaining the resilience outcomes (Parsons et al., 2014).

Practically, the results hold implications for organizations and policy makers. It is recommended to emphasize programmes on awareness creation, cyber security training and development of cyber security culture as these have turned out to be the most important in determining Digital Security Resilience (Haney et al., 2022). To enhance resilience and reduce vulnerability, more educative and awareness programmes on phishing, password maintenance, social engineering and safe digital practices have to be organised (Bada et al., 2019). In addition, the need for organizations to take proactive measures, including conducting risk assessments, monitoring threats, managing vulnerabilities, and developing incident response plans, to ensure the continuity of operations (NIST, 2018) is paramount.

Positive impact of data privacy protection calls for policy makers and organisations to strengthen data privacy laws and have a policy by design, that will build digital trust and minimise the risks of unauthorised access and data breaches (Martin & Murphy, 2017). The overall results indicate that there is a need for holistic and multi pronged approach that embraces technological security measures, cybersecurity awareness, privacy protection measures and governance capabilities. This comprehensive approach is necessary for creating safe, robust and reliable digital environments in ever-evolving digital landscapes.

8. Conclusion

This present study aimed at empirically examining the influence of Cybersecurity Practices (CSP), Data Privacy Protection (DPP), Cyber Governance Framework (CGF) and Cybersecurity Awareness (CSA) on Digital Security Resilience (DSR) and to investigate the determinants of DSR. The findings offer a full picture of the relationship between the technological, behavioural and governance aspects, which can help increase cyber resilience. The study is based on the Protection Motivation Theory and socio-technical lenses to better understand digital resilience in the era of digitalisation.

The strongest predictor of Digital Security Resilience was Cybersecurity Awareness ($\beta = 0.355$, $p < 0.001$), highlighting the importance of human factors and security awareness in reducing cyber risks. The result echoes with earlier research that indicated awareness and security culture are critical factors shaping cyber resilience, with human vulnerabilities still being one of the main factors that lead to cybersecurity incidents (Parsons et al., 2014). Raising awareness of cyber threats and how to prevent and combat them, such as phishing attacks, as well as the importance of online security, makes it easier for everyone to prevent and respond to cyber incidents, and be more cyber resilient.

Digital Security Resilience ($\beta = 0.184$, $p < 0.001$) had a significant positive impact on Cybersecurity Practices, signifying that the proactive security measures that include risk assessment, threat monitoring, and incident response capabilities enhance the capability to resist and bounce back from cyber disruptions (NIST, 2018). Likewise, the impact of Data Privacy Protection on Digital Security Resilience was positive and significant ($\beta = 0.183$, $p < 0.001$), which further affirmed that robust privacy measures and the management of sensitive data lead to greater resilience and security in the digital landscape (Martin & Murphy, 2017). The results support the concept of building resilience through the combination of technological protection and privacy-enhancing measures, and not through standalone security measures.

Surprisingly, Cyber Governance Framework did not have any statistically significant effect on Digital Security Resilience ($\beta = 0.072$, $p = 0.107$). The finding indicates that, without the support of effective implementation, cybersecurity practices and awareness capabilities, regulatory structures and governance mechanisms are not enough to guarantee resilience. The finding aligns with the previous arguments that governance mechanisms are mostly enabling and that their effectiveness is related to their interaction with technological and behavioural aspects (von Solms & van Niekerk, 2013).

Taken as a whole, the findings support the conclusion that Digital Security Resilience is a multiple dimensional construct with cybersecurity awareness as its main dimension, followed by cybersecurity practices and data privacy protection. The structural model accounted for 41.9% of the variance in Digital Security Resilience, suggesting moderate explanatory power, and underscoring the need for cognitive, technological and organizational aspects to be considered when developing resilience (Hair et al., 2022). The results indicate that compliance-focused security measures are not the most effective approach and that a more comprehensive strategy is needed, focusing on awareness, privacy and proactive security measures within organizations and policies. This collaborative solution is crucial for building safe, trustworthy, and robust digital ecosystems that can effectively mitigate the new digital transformation challenges and threats.

9. Limitations and Future Research Directions

In the present study, the causal relationships between Cybersecurity Practices, Data Privacy Protection, Cyber Governance Framework, Cybersecurity Awareness, and Digital Security Resilience is difficult to conclude as the

study used cross-sectional research design. As cyber security is a dynamic contemporary topic which changes according to rapid strides in technology, the future studies must be based on longitudinal or experimental designs to understand the cyber security resilience mechanisms. Secondly, the study was based on the Indian context and the conclusions of the study may not be applicable to other countries that possess varied digital infrastructure and regulatory frameworks.Thirdly, in order to gain an in depth understanding of the Digital Resilience Mechanism, other variables like AI adoption, Organisation culture can be explored.

REFERENCES

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. doi:https://doi.org/10.1126/science.aaa1465.
2. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* In *Cyber Security for Sustainable Society* (pp. 118–131). Springer. doi:10.48550/arXiv.1901.02672.
3. Ewoh, P., Vartiainen, T., & Mantere, T. (2025). Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review. *Journal of Medical Internet Research*, *27*(1), e75584. https://doi.org/10.2196/75584.
4. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. doi:https://doi.org/10.1177/002224378101800104.
5. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.
6. Haney, J., Jacobs, J., Furman, S., & Barrientos, F. (2022). *Federal cybersecurity awareness programs :* national institute of standards technology. https://doi.org/10.6028/nist.ir.8420b
7. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. doi:https://doi.org/10.1007/s11747-014-0403-8.
8. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. doi:https://doi.org/10.1016/j.cose.2011.10.007.
9. Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10. doi:https://doi.org/10.4018/IJEC.2015100101.
10. Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155. doi:https://doi.org/10.1007/s11747-016-0495-4.
11. Nafees, M., & Kumar, M. M. (2023). *CYBERSECURITY AND DATA PRIVACY LAW: NAVIGATING THE LEGAL LANDSCAPE*. noble science. doi:https://doi.org/10.52458/9789388996747.nsp2023.eb.ch-20.
12. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.
13. 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. doi:https://doi.org/10.1016/j.cose.2013.12.003.
14. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. doi:https://doi.org/10.1080/00223980.1975.9915803.
15. Seshanna, S. V., Gopalakrishnan, G., Anute, N., Deepthi Reddy, K., Sharma, M., Selvakumar, P., & Manjunath, T. C. (2025). *Digital Transformation and Cybersecurity* (pp. 1–30). igi global scientific. doi:https://doi.org/10.4018/979-8-3373-3171-3.ch001.
16. Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment methods. *Computers & Security, 57*, 14–30. doi:https://doi.org/10.1016/j.cose.2015.11.001.
17. Sharma, M. (2023). Digital governance of E-commerce in India. *VIDHIGYA: The Journal of Legal Awareness*, *18*(1and2), 126–138. doi:https://doi.org/10.5958/0974-4533.2023.00011.8.
18. Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations, 4*(1), 3–38. doi:https://doi.org/10.1177/001872675100400101.
19. Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors from a protection motivation theory perspective. *Computers & Security, 59*, 138–150. doi:https://doi.org/10.1016/j.cose.2016.02.009.
20. von Solms, B., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. doi:https://doi.org/10.1016/j.cose.2013.04.004.