Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

DIGITAL TRANSFORMATION AND CYBER SECURITY CHALLENGES IN THE INFORMATION AGE

[1]Sarabjit Kaur
Assistant professor,
Department of Commerce,
Chandigarh Business School of Administration,
CGC, Landran Mohali, Punjab, India
Kaur1992srb@gmail.com
[2]Dr. Aruna. V
Assistant Professor,
Department of MBA,
St. Joseph's Institute of Technology, OMR, Chennai-600119
arunav@stjosephstechnology.ac.in
[3]Dr. A.Valarmathi
Director/ Professor,
Department of Management
Vivekananda Institute of Management Studies,
Coimbatore, Tamilnadu, India
dravalarmathi@gmail.com
[4]Dr.A.Geetha
Professor and Head Department of Business Administration,
Bharath Institute of Higher Education and Research,
173-AgaramRoad, Selaiyur, Chennai -73
geethaganesh2015@gmil.com
[5]Dr.Nitin Kumar Srivastava
Assistant Professor,
School of Computer Science & Engineering
IILM University Gurugram, Golf Course Road 122011, Haryana
nitink.srivastava@iilm.edu
[6]Dr. P. Dhanasekaran
Guest Faculty,
Department of Extension And Career Guidance
Bharathiar University, Coimbatore – 641 046
dhanasekar593@gmail.com

ABSTRACT

Digital transformation, one of the themes of the Information Age, is forming the basis of industries, rewarding innovation and fueling economic advancement. However, this advancement becomes faster and engulfs technology and with these new advancements comes a lot of virtual insecurity such as data leakage, privacy violation and increased virtual dangers. Digital transformation was discussed in this article in relation to cyber security in the context of interactions through interconnected systems. On the basis of existing theory, this work assesses the measures that organisations have to implement in order to address these threats where digitalization is implemented. The research also looks at a number of case studies and polices that have already been studied in prior educational work to show the effects that will be analyzed in the following sections on policy and governance, as well as future improvements in

technology. The nature of cyber threats is evolving at an incredibly fast pace, making it impossible to implement changes that wouldn't demand constant investments in training, tools, and processes. As for the restriction of resources, the identification and prevention of breaches are also delayed during incident response. In order to counter these problems, organisations may turn to the use of a third-party cyber security services and products including cyber security-as-a-Service; incorporate automation to enable them achieve greater performances yet minimize workload; as well as engage in security culture campaigns that aim at reaching all organisational workforce. Lack of resources may be a major detriment in the ongoing fight against cyber threats, but better prioritization and alliance can flatten the negative effects of having scarce resources in one's arsenal.

Keywords: *Digital transformation, cybersecurity, information age, data breaches, interconnected systems, governance.*

Introduction

The research underscores the need for continuous monitoring, regular audits, and compliance with evolving regulations to mitigate risks. By methodically addressing these issues, companies may safeguard their digital transformation efforts while securing sensitive data and systems. While it aims at innovation and efficiency it at the same time leads companies to suffer from cyber threats. This is because this phenomenon must work in harmony, and only if their dynamics are understood adequately, growth and security are truly achievable. Damaraju, A. (2024) provides a detailed look on how security of the cloud systems can be addressed while undergoing digital transformation. Analyzing the wide list of inputs, Damaraju notices such serious threats as insecure clouds' configurations, weak cryptographic protection, and the invisibility of cloud infrastructures. The study stresses the shared responsibility model that results in ambiguity concerning security commitment between cloud providers and clients. The author also lays down several approaches to deal with these issues such as information monitoring through the use of AI technologies and the use of multi-form authentication mechanisms and there should be the encryption of such data. The focus is thereby placed on the full qualification of a cloud-native security technique, which comprises server less security services and containerization for improving business continuity. The paper also demonstrates the importance of mapping security responsibilities among IT teams and cloud service providers. It is also wise to carry out frequent security assessments, and it is legal to use conformity standards like SOC 2 and ISO 27001 to achieve secure cloud space. Determinedly, cloud security has its issues but Damaraju agrees that if a business uses a strategic and pre-emptive approach, it may help them create safer cloud adoption strategies. Thakur (2024) presents a systematic analysis of cyber security risks and the strategies that organizations could adopt in cyberspace. In the current paper, options to raise staff awareness and training levels as a way of strengthening human aspects of cyber security are of great prominence. The work identifies the signification of a collective approach and adherence to laws in preventing transnational cybercrime.

Literature review and research Agenda

Thakur, although digital transformation comes with a good deal of risks, the implementation of a digital security system can help organisations address their concerns adequately. In another study, Moller (2023) explained cyber security trends, approaches, and best practices based on digital transformation. The book reiterates that the combination of cloud computing, IoT, AI, and block chain increases system susceptibility. The document logically divides several threats: insufficient security of IoT devices, supply chain attacks, and cloud misconfiguration.

Procedures are described with the highest detail, ranging from security policies, regular staff training, and even development of incident handling procedures. GDPR and ISO 27001 are expected standards which should be met in order to manage risks ad ensure continuity of trust. Examples of such solutions are provided through presentations of best practices concerning cyber security issues, based on case studies. Moller agreed that cyber security issues are not going to disappear, but both technology and knowledge may help alleviate the risks associated with digital transformation. Stewart (2023) analysed the unique security challenges posed by digital transformation initiatives in modern businesses. The report highlights how the increasing adoption of technologies such as IoT, cloud computing, and AI extends the attack surface, leaving organisations more susceptible to cyber assaults. Stewart emphasizes that discordant security policies and insufficient integration of cybersecurity measures in transformation initiatives are common issues. Furthermore, human issues such as employee negligence, insufficient training, and insider threats also contribute to security breaches. Shaikh et al. (2024) analyze the intersection of digital transformation and cybersecurity, emphasizing the vulnerabilities that arise in a cohesive digital landscape. The authors analyze how reliance on emerging technologies, such as AI, block chain, and 5G, generates new opportunities for cyber-attacks. Identified hazards include phishing and data breaches, compounded by the rising popularity of connected devices and cloud-based services. The authors advocate for a holistic cybersecurity strategy to alleviate these concerns. The text emphasizes the need of continuous education and training for personnel, since human error remains a significant risk. Moreover, the authors emphasize the need for collaboration among stakeholders, including governmental bodies, business entities, and technology providers, to formulate a unified strategy for cybersecurity. The article concludes by endorsing legal frameworks that adapt to technological advancements, foster innovation, and protect data privacy and system integrity

Theoretical Framework

This research uses the Technology-Organization-Environment (TOE) paradigm to analyze the impact of technical, organisational, and environmental aspects on the adoption and risk mitigation in digital transformation. Chowdhry (2020) analysed the transformational effects of digitalization on enterprises, emphasizing cybersecurity vulnerabilities and measures for their mitigation. The editors provide a thorough analysis of the evolution of cyber risks in conjunction with technical progress. Their discourse focusses on prominent cyber-attacks to highlight weaknesses in essential systems and underscore the need of regulatory compliance in promoting safe corporate settings. The authors provide a paradigm for safe digital transformation, highlighting risk management, threat intelligence, and advanced technology. The subjects addressed include the function of block chain in augmenting transaction security, AI-based methodologies for anticipatory threat identification, and the incorporation of cybersecurity into cloud-centric operations. Case studies of successful digital transitions emphasize best practices like as stakeholder participation, strong governance, and flexible security protocols. The book discusses the significance of corporate culture in improving cybersecurity resilience, contending that organisations should cultivate a security-first mentality among workers. The editors conclude that although digital transformation is a corporate need, success relies on implementing effective cybersecurity protections into every phase of the process.

Technology-Organization-Environment (TOE) Framework

The Technology-Organization-Environment (TOE) framework, developed by Tornatzky and Fleischer in 1990, provides a comprehensive lens to understand how organizations adopt and

implement new technologies. It emphasizes three dimensions—technological, organizational, and environmental—that collectively influence the adoption process. The TOE framework has gained widespread recognition in the study of digital transformation, cybersecurity, and innovation management due to its holistic nature.

1. **Technological Dimension**: The technological dimension focuses on the attributes and capabilities of the technology being adopted. It includes factors like relative advantage, compatibility, complexity, trialability, and observability. Relative advantage is the perceived advantages of implementing a new technology in comparison to current processes or instruments. It underscores how technology promotes efficiency, lowers expenses, improves performance, or offers distinctive possibilities. In digital transformation, technologies like cloud computing, artificial intelligence, and the Internet of Things exhibit distinct relative benefits, including scalability, real-time data analytics, and improved client interaction. Organisations are more inclined to embrace technologies when their benefits correspond with strategic objectives, such as enhancing operational efficiency or achieving competitive market positioning.

Compatibility, conversely, emphasizes the degree to which a new technology assimilates with established systems, values, and processes inside an organisation. Elevated compatibility reduces opposition to adoption and mitigates interruptions. Organisations with existing IT infrastructures may choose solutions that interact smoothly with their legacy systems to avoid expensive overhauls. Compatibility also extends to cultural alignment—technologies must suit the organization's operating style and human skillsets to achieve adoption success. Relative advantage and compatibility serve as crucial determinants of technology adoption, affecting the speed and efficacy with which organisations undertake digital transformation. Addressing these aspects facilitates seamless transitions and optimises advantages. Complexity denotes the perceived challenge in comprehending, executing, and using a novel technology. Technologies seen as too complicated may encounter opposition, especially if organisations lack the necessary skills or resources for effective implementation. Adopting block chain or AI might appear overwhelming owing to technological intricacy, steep learning curves, and the requirement for specialized expertise. The impression of complexity often corresponds with increased costs, elevated resource requirements, and extended implementation schedules, making it a substantial obstacle to adoption. Organisations must mitigate complexity by streamlining technological interfaces, offering extensive training, and guaranteeing strong technical support. Intuitive designs, comprehensive documentation, and modular implementation methodologies help alleviate issues. Minimizing perceived complexity enhances user trust, facilitating expedited adoption and incorporation into processes. Mitigating complexity not only promotes seamless adoption but also guarantees that the organisation can fully use the technology's capabilities to foster innovation and competitive advantage

Trialability and Observability

Trialability denotes the extent to which a technology may be evaluated or experimented with prior to comprehensive implementation. Organizations are more willing to accept technology that provide trial periods, pilot programs, or prototypes. Trialability decreases uncertainty by enabling stakeholders to assess the technology’s functioning, identify possible concerns, and quantify its value versus goals. For instance, cloud services providing limited free trials allow enterprises to examine scalability and dependability without immediate cash commitment. Observability, conversely, relates to the extent to which the advantages of the technology are apparent to others. Technologies that provide unequivocal benefits, such as enhanced efficiency

or revenue augmentation, are more prone to adoption. Success stories, testimonials, and case studies are essential for improving observability, since they provide concrete proof of the technology's effectiveness. By emphasizingtrialability and observability, organisations may enhance trust in technology adoption, mitigate perceived risks, and cultivate stakeholder support. Collectively, these elements facilitate a more seamless shift from experimentation to comprehensive deployment.

Dimensions and Assets, Executive Endorsement

The dimensions and resources of an organisation significantly influence its capacity to embrace and integrate new technology. Larger firms frequently have the financial and human capacity required to invest in innovative technologies, training programs, and infrastructure changes. They may also designate resources for risk management and problem-solving throughout deployment. Conversely, smaller organisations may have constraints in cash and experience, hindering their ability to adopt complicated technology. Nonetheless, smaller businesses might use their agility to implement new ideas more rapidly than bigger rivals. Leadership support is another essential component that strongly impacts technology adoption. Leaders that advocate for innovation may facilitate organisational change by endorsing a vision that corresponds with digital transformation objectives. Their participation in resource distribution, decision-making, and promoting a culture of adaptation guarantees seamless transitions. Executive backing of cybersecurity measures often results in more effective implementations and increased staff compliance. Effective leadership bridges comprehension gaps and mitigates opposition to change, so assuring sustained success in technology adoption.

Organisational culture comprises the collective values, attitudes, and practices inside a company, profoundly influencing technology adoption. A culture that fosters creativity, perpetual learning, and adaptation cultivates an atmosphere suitable to digital transformation. Organisations characterized by inflexible or risk-averse cultures may have difficulties in assimilating new technology owing to resistance or apprehension over failure. Organisations that foster interdepartmental cooperation and engage employees in decision-making are more likely to successfully embrace new technology. Facilitating training and promoting feedback fosters employee confidence and dedication to the process. Conversely, a lack of receptivity to change might inhibit advancement, regardless of technical competence. To cultivate a supportive culture, organisations must synchronize their digital transformation objectives with employee values, emphasize honest communication, and incentivize creativity. In doing so, they guarantee that all stakeholders are engaged in the change process.

Applications of the TOE Framework

The TOE framework has been extensively applied in research and practice to analyze various technological adoptions, including cloud computing, big data, AI, block chain, and cybersecurity measures. Its strength lies in offering a structured approach to assess both internal and external factors that shape technology implementation.

Recognizing Cybersecurity Threats in Digital Transformation

Digital transformation incorporates sophisticated technology and integrated systems to enhance efficiency and foster creativity. Nonetheless, these improvements render organisations vulnerable to considerable cybersecurity threats.

Market Dynamics and Regulatory Obligations

Market dynamics denote the evolving factors within an industry, including consumer preferences, technical advancements, and economic fluctuations. These factors significantly impact organizations' choices to embrace new technology in their digital transformation efforts. The increasing need for personalized customer experiences has compelled organisations to employ AI and data analytics to improve engagement and loyalty. Likewise, transitions towards sustainability and environmentally conscious behaviours compel enterprises to adopt eco-friendly technology. Market dynamics influence pricing strategies, supply chain efficiency, and product development cycles, necessitating organisational agility. Organisations that do not adjust to these transformations jeopardize their position relative to more inventive rivals. Consequently, being cognizant of market developments is crucial for using digital transformation as a competitive edge. Regulatory mandates have a significant influence on technology adoption. Regulatory authorities and industry organisations establish policies to guarantee data security, safeguard consumer rights, and promote ethical standards in technology utilization. Compliance with regulations such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) requires strong cybersecurity and data governance systems. Failure to adhere to these standards may lead to substantial penalties, reputational harm, and erosion of consumer confidence. Therefore, organisations must include regulatory mandates into their technological plans, reconciling innovation with compliance to legal norms. Ensuring compliance enhances credibility and fortifies stakeholder relationships.

Competitive Pressure

Competitive pressure serves as a crucial catalyst for digital change. Organisations use new technologies to align with or exceed their competitors' capabilities, aiming to sustain market relevance and leadership. For instance, when rivals employ AI-driven solutions to streamline supply chains or deliver greater customer experiences, other organisations are pushed to follow suit to stay competitive. This pressure influences product development, operational efficiency, and marketing tactics. Organisations that embrace novel technology may disrupt sectors, compelling rivals to react swiftly. The emergence of digital payment systems such as PayPal and Square compelled conventional banking institutions to adopt digital offerings. Nonetheless, using technology only to surpass rivals without a defined plan may result in wasteful resource allocation and worse results. Organisations must evaluate their distinct capabilities and synchronize technology adoption with their long-term objectives to react successfully. Competitor-driven change underscores the need of benchmarking and industry study. By analyzing rivals' strategy and technical progress, organisations may pinpoint deficiencies, capitalize on possibilities, and formulate proactive measures, so assuring continuous growth and resilience in fluctuating marketplaces.

Effective Strategies for Secure Implementation

To achieve secure digital transformation, organizations must adopt comprehensive cybersecurity strategies:

1. Data Breaches: Data breaches represent a critical danger in the digital era, happening when sensitive information is accessed without proper authorization. These breaches may jeopardise personal information, financial records, trade secrets, and other vital assets, resulting in significant financial and reputational repercussions. The growing convergence of cloud storage, big data analytics, and linked technologies amplifies the danger of data breaches. Cybercriminals use inadequate access restrictions, unpatched software, or misconfigured systems to breach

networks. Upon entry, they may extract sensitive information for purposes of identity theft, extortion, or sale on the dark web. Organisations must use stringent data security protocols, such as encryption, multi-factor authentication, and periodic vulnerability assessments, to alleviate this risk.

2. Cloud Vulnerabilities: Cloud computing has emerged as a fundamental element of digital transformation, providing scalability, cost-effectiveness, and adaptability. Nonetheless, it also presents weaknesses specific to its design. Misconfigurations, inadequate API security, and shared infrastructure vulnerabilities may render cloud systems vulnerable to unauthorized access and data breaches. Improperly designed storage services or unsecured cloud credentials may render critical data publicly accessible. Moreover, when organisations depend on external cloud providers, they jeopardize their control over data protection. Addressing cloud risks requires rigorous access restrictions, frequent audits, and a collaborative responsibility between the organisation and the cloud service provider. Implementing cloud-native security technologies and frameworks such as Zero Trust may significantly bolster protection.

3. Risks Associated with the Internet of Things (IoT): IoT devices, ranging from industrial sensors to consumer electronics, are rapidly incorporated into organizational networks. While they boost productivity and data collecting, their often-inadequate security measures offer major hazards. Numerous IoT devices are devoid of encryption, routine upgrades, or robust authentication protocols, rendering them vulnerable to cyber attacks. Once infiltrated, attackers may utilize IoT devices as access points to bigger networks or use them in Distributed Denial of Service (DDoS) operations. To counter these dangers, enterprises must enforce device-level security, segregate IoT traffic, and demand updates and fixes for linked devices.

4. Social Engineering: Social engineering attacks use human psychology to get unauthorized access to systems or data. Methods like phishing, luring, and pretexting manipulate people' trust or ignorance. Phishing emails often mimic authentic organisations to deceive recipients into disclosing confidential information or engaging with harmful links. Such assaults are especially successful in evading technical barriers, focusing instead on human mistake. Countering social engineering requires extensive staff training, effective email filtration systems, and awareness initiatives to recognize and evade manipulative strategies.

5. Supply Chain attacks: The growing dependence on third-party suppliers has become supply chain attacks a significant cybersecurity issue for organisations. Attackers target less-secure suppliers to penetrate bigger corporations indirectly. Malicious software upgrades from a third-party vendor may jeopardise an organization’s systems. Moreover, inadequate assessment of suppliers' security protocols may result in vulnerabilities across the supply chain. Organisations should create rigorous vendor management rules, perform frequent audits, and establish contractual obligations for cybersecurity compliance to minimise these hazards. Transparency and cooperation throughout the supply chain augment protection against these dangers.

1. Resilient Security Frameworks: Data Encryption and Backup: Establishing a comprehensive security framework is crucial for protecting organisational assets from advancing cyber threats. A complete framework comprises many defensive layers, including firewalls, intrusion detection systems, and secures network topologies, aimed at thwarting unauthorized access and reducing vulnerabilities. Data encryption is an essential element of this architecture, guaranteeing the safe transmission and storage of sensitive information. Advanced Encryption Standards (AES) safeguard data from interception, making it unintelligible without the appropriate decryption

keys. Routine data backups enhance encryption by offering protection against data loss resulting from breaches, ransomware incidents, or system malfunctions. Organisations protect business continuity in worst-case circumstances by keeping backups in safe, remote locations and verifying their integrity.

2. Employee Training: Multi-Factor Authentication (MFA): Human mistake is a primary contributor to cybersecurity breaches, making staff training a crucial technique for safeguarding organisational systems. Training programs must emphasize the identification of phishing efforts, the avoidance of harmful links, and the adherence to safe password protocols. Consistent, immersive lessons that replicate actual assaults enhance awareness and prepare workers to serve as the first line of defense. Multi-Factor Authentication (MFA) enhances access restrictions by necessitating users to provide several verification methods, such passwords, biometric information, or security tokens. Implementing MFA enables organisations to substantially reduce the risk of unauthorized access, even if a single authentication element is breached.

3. Ongoing Surveillance and Threat Identification: Supplier Oversight: Proactive cybersecurity relies on ongoing surveillance and threat identification. Security Information and Event Management (SIEM) solutions provide real-time insights into network operations, detecting and addressing abnormalities prior to their escalation into breaches. Automated threat detection systems backed by artificial intelligence may further boost speed and accuracy in detecting possible threats. Vendor management is essential, since third-party suppliers often bring vulnerabilities into an organization's ecosystem. Implementing rigorous security criteria, performing frequent audits, and ensuring transparency in suppliers' operations guarantee compliance with the organization’s cybersecurity standards. By creating collaborative partnerships, firms may limit risks while preserving supply chain efficiency.

4. Incident Response Strategies: Regardless of precautionary measures, no organisation is impervious to cyber-attacks. Incident response plans (IRPs) are crucial for mitigating harm and facilitating rapid recovery. These plans delineate the procedures to follow during a security breach, including threat identification, containment of its proliferation, eradication of the fundamental cause, and restoration of regular operations. Effective Incident Response Plans delineate explicit roles and responsibilities, guaranteeing that all team members comprehend their duties throughout a crisis. Routine simulations and tabletop exercises evaluate the plan's efficacy, pinpointing deficiencies that need rectification. A well implemented IRP not only alleviates the immediate consequences of cyber disasters but also fosters resilience against future threats, hence preserving organisational stability and confidence.

Statement of the Problem

The unusually fast-digitization process across many industries has impacted company functioning, increased effectiveness, and inspired innovation. This has also brought about complex security challenges to organisational stability, data, and customer trust. As organisations implement new technology solutions such as cloud computing, or the Internet of Things, or artificial intelligence, they create more interconnectivity in their digital environment, making them more vulnerable to an attack. One of the biggest problems is that companies increase exposure due to the ongoing digital transformation. In addition, IoT devices and reliance upon third parties for products and services only increase cyber security risks, due to inadequate security measures of those outside organisations, which introduce risks throughout the supply chain. Freeware is developed and launched in record times and sometimes, cyber security is not

given the appropriate consideration that it deserves. Businesses, especially SMES, face challenges in providing adequate resource and talent for protection of the systems. The gap between the increasing speed of technology advancement and the slow capability of organizations to protect themselves creates increased risk in organizations that operate in industries that are heavily governed such as the banking, healthcare, and energy industries. However, the lack of comprehensive laws and legal systems and also the lack of international cooperation produce significant gaps to deal with international cyber threats.

Research Objectives

1. To identify cybersecurity risks in digital transformation.
2. To evaluate effective strategies for secure implementation.
3. To analyze implications for policy and governance.

Analysis, Findings and Results

Many organisations face challenges of developing an organisational culture that is sensitive to security because employee errors are still the leading cause of the breaches. It is then on this premise that the mix between the opportunities afforded by digital transformation and the utility of effective cyber security measures presents the best difficulty on the part of the company to achieve. These complexities render organisational advancement, process sustainability and stakeholder confidence exposed to high risk especially in a more digital environment to achieve the study, 150 participants participated using convenience sampling and were drawn from management positions in numerous sectors. The reason for choosing convenience sampling was that it is easily achievable to find participants through professional connections, social media, and conferences. The data were collected through structured questionnaires which make it easy to do both quantitative as well as qualitative analysis. This approach enables a simultaneous consideration of data characteristics and exploratory investigation of textual content.

Table 1
Descriptive statistics

S.No	Factors	N	Mean	SD
1	Increasing Attack Surface	150	3.23	.779
2	Complexity of Emerging Technologies	150	3.49	1.217
3	Regulatory and Compliance Issues	150	3.30	1.276
4	Sophistication of Threat Actors	150	3.21	1.123
5	Resource Constraints	150	3.12	0.765

The descriptive statistics table provides insights into key factors related to cybersecurity challenges during digital transformation. Increasing Attack Surface (Mean = 3.23, SD = 0.779): This factor indicates a moderate level of agreement

among respondents regarding the growing exposure to cybersecurity risks due to an expanding attack surface.The relatively low standard deviation suggests that responses were fairly consistent. Complexity of Emerging Technologies (Mean = 3.49, SD = 1.217) Respondents rated this as a significant challenge, with the highest mean value among all factors.However, the higher standard deviation indicates diverse opinions, reflecting varying experiences with emerging technologies.Regulatory and Compliance Issues (Mean = 3.30, SD = 1.276)Regulatory challenges are another prominent concern, with respondents indicating a moderate to high impact.The high standard deviation suggests varied levels of impact based on organizational or regional contexts.Sophistication of Threat Actors (Mean = 3.21, SD = 1.123) this factor also shows a moderate level of concern about increasingly advanced cyber threats.The standard deviation indicates moderate variability in perceptions, possibly influenced by organizational preparedness. Resource Constraints (Mean = 3.12, SD = 0.765) Resource limitations are perceived as a moderate issue, with the lowest mean among all factors.The low standard deviation indicates consistent views across respondents.

Table 1 reveals the results of descriptive statistics of factors of digital transformation in the study area. The study results reveal that the mean values are whole statements are >3. Increasing Attack Surface: The rapid digital transformation across industries has significantly broadened the attack surface for cyber threats. The widespread adoption of cloud services adds another layer of complexity; while cloud infrastructure offers scalability and cost-efficiency, misconfigurations, inadequate access controls, and vulnerabilities in third-party integrations pose significant risks. Additionally, the rise of hybrid work models has intensified the challenge. Employees working remotely often use personal devices and unsecured networks, increasing the risk of data breaches, malware infections, and phishing attacks. Organizations must adopt robust endpoint protection, enforce strict access management protocols, and implement continuous monitoring to mitigate these risks. Failure to secure the expanding attack surface can lead to significant financial, operational, and reputational damages. Complexity of Emerging Technologies: Emerging technologies such as artificial intelligence (AI), machine learning (ML), block chain, and 5G have revolutionized industries but have also introduced new cybersecurity challenges. AI and ML, while enhancing threat detection and response capabilities, can be attackers to create advanced phishing campaigns, automate attacks, and bypass traditional defenses. Block chain, often touted for its security, may have vulnerabilities in smart contracts and centralized implementations. Meanwhile, 5G networks offer unprecedented speed and connectivity but can amplify the reach and sophistication of cyber-attacks. The rapid evolution of these technologies often outpaces the development of security protocols, leaving gaps in protection. Organizations must integrate security considerations into the design and deployment of these technologies. Investing in advanced cyber security tools and upskilling teams to address these challenges is critical to leveraging emerging technologies securely. Regulatory and Compliance Issues: As digital transformation accelerates, organizations must navigate an increasingly complex regulatory landscape. Cross-border operations further complicate compliance, requiring adherence to varied international regulations. Emerging technologies like AI and block chain often operate in gray areas of regulation, creating uncertainty about compliance requirements. Additionally, the pace of regulatory changes often lags behind technological advancements, leaving organizations unsure of their obligations. Compliance is not merely about avoiding penalties; it is also crucial for building customer trust and safeguarding sensitive data. Implementing a robust governance framework, conducting regular audits, and collaborating with legal experts are essential for ensuring compliance. Organizations that proactively adapt to regulatory changes and integrate them into their cybersecurity strategies will gain a competitive

edge in the market. Sophistication of Threat Actors: Threat actors are becoming increasingly sophisticated, leveraging advanced tools and strategies to exploit vulnerabilities in digital ecosystems. State-sponsored hackers, organized cybercriminal groups, and even rogue insiders are using AI, ML, and zero-day exploits to conduct highly targeted attacks. These actors are often well-funded and operate collaboratively, exchanging tools and knowledge on the dark web. Advanced persistent threats (APTs) further complicate the security landscape, as they remain undetected for long periods while infiltrating critical systems. The growing sophistication of these attackers necessitates a shift from reactive to proactive cybersecurity measures. Organizations must adopt threat intelligence, behavior-based detection, and zero-trust architectures to counter these advanced threats effectively. Resource Constraints: Despite the growing cybersecurity challenges, many organizations face significant resource constraints that hinder their ability to protect against threats. Limited budgets often result in outdated technologies and inadequate security infrastructure. Small and medium-sized enterprises (SMEs) are particularly vulnerable due to their lack of dedicated IT and cybersecurity teams. Even larger organizations struggle to find skilled cybersecurity professionals, as the demand for expertise far exceeds the supply.

Table 2
Results of F-test for Digital transformation and cyber security challenges in the information Age

Age(In years)	Up to 30	31-40	41-50	Above 50
N	57	32	41	20
Mean	3.68	3.51	3.24	2.39
SD	0.654	0.543	0.487	0.231
F	5.076			
p	0.006			

Table 2 illustrated the results of the F-test on digital transformation and cybersecurity issues in the information age. The computed F and p-values for digital transformation and cybersecurity issues in the information age across different age are 5.076 and 0.006, respectively. The p-value is below 0.01, indicating that the study demonstrated a substantial disparity across age groups concerning digital transformation and cybersecurity issues in the information age. Nowicka et al. (2024) investigated the challenges of managing organisational security during digital transformation. The authors highlight the increasing complexity of security systems as organisations use cloud services, artificial intelligence, and Internet of Things technologies. They identify common vulnerabilities, such as inadequate cloud configurations, ineffective identity management, and insufficient employee training. The report highlights the need for companies to have a comprehensive security management plan. This involves the execution of zero-trust designs, automation of threat detection, and enforcement of rigorous access protocols. The authors underscore the need of aligning cybersecurity measures with organisational goals to avoid obstructing innovation. The major focus is on the impact of leadership in enhancing security protocols. Executives must prioritise cybersecurity, provide enough resources, and foster interdepartmental collaboration to effectively minimize threats. The analysis underscores the need of complying with international regulations and standards, such as GDPR and ISO 27001,

to ensure data security and enhance customer trust. The authors contend that companies must continuously adapt their security protocols to proactively counter evolving cyber threats.

Discussion

The research proposed a structure to enhance security awareness, including regular training sessions, phishing simulation exercises, and involvement from leadership. It also analyses opportunities created by advancements in AI and block chain for enhancing cybersecurity procedures. However, the authors note that challenges such as budgetary constraints and rapid technological advancement may hinder acceptance. The chapter concludes by emphasizing the need for businesses to integrate cybersecurity awareness into their overarching digital transformation plan to ensure enduring resilience. Taherdoost et al. (2021) examined the dual role of cybersecurity and information security awareness in facilitating successful digital transformation. The authors emphasize the increasing need for organisations to prioritise cybersecurity education as assaults get more sophisticated. They assert that insufficient comprehension among employees often results in violations, even when robust technology safeguards are implemented. Tagarev and Stoianov's (2019) investigated the relationship among digital transformation, cybersecurity, and organisational resilience. The authors illustrate how the integration of digital technology creates both opportunities and vulnerabilities. They emphasize the need of fostering resilience against cyber threats via a combination of proactive strategies and adaptive technologies. Key topics include the role of public-private partnerships in enhancing cybersecurity, the impact of law on resilience strategies, and the use of AI for predictive threat assessment. The authors examine the concept of cyber hygiene, advocating for regular updates, assessments, and staff training. Case studies from several sectors demonstrate how businesses have successfully used resilience frameworks to mitigate risks. The authors contend that a cohesive strategy, combining technology, policy, and awareness, is essential for maintaining the benefits of digital transformation while mitigating risks. Spremic and Simunic (2018) analyzed the cybersecurity issues intrinsic to the digital economy and their implications for organisations. The authors assert that as organisations use digital technology to enhance efficiency and competitiveness, they become susceptible to a rapidly evolving danger landscape. The principal challenges are securing e-commerce platforms, protecting customer data, and ensuring the integrity of financial transactions. The authors emphasize the significance of governmental regulations and standards in formulating cybersecurity policy, underscoring compliance as an essential condition. They promote a combination of technology strategies—such as firewalls, encryption, and intrusion detection systems—and organisational approaches, including employee training and risk management frameworks. The report concludes by urging businesses to adopt a balanced approach that aligns security investments with business goals, so ensuring resilience while promoting innovation.

Implication of the study

The incorporation of cyber security into digital transformation dramatically transforms the businesses, sectors, and society. On the organisational level, issues of cyber security prospective define resource allocation, functioning protocols, and staff education. To protect their data assets, businesses have no option other than to spend heavily in technologies like encryption, unintake detection systems, two factor authentications and more. Also, creating a security-aware culture is crucial because people can be still a valuable source of numerous risks. These changes increase the robustness and ensure that business entities occupy strategic positions in competitive market systems. The use of cyber security at the industrial level enhances the integration process in

emulation standard and collaboration.

Conclusion

The study findings clearly indicate that complexity of emerging technologies is viewed as the main threat, which is agreed by the second threat, namely regulatory and compliance concerns. Though the attack surface grows, threat actors become more sophisticated, and resources remain limited, it is rated slightly lower. Such variations in standard deviations imply the difference of challenge perceptions due to organizational characteristics or respondent roles.Digital integration with cyber security is essential for maintaining the constant innovation pace in the Information age. It became increasingly evident that successful risk mitigation and developmental improvement require integrated approaches and solid processes. Some businesses including banking, healthcare, and energy, which deal with confidential information, need to employ a common set of security to improve compatibility and meet the legal requirements. By conducting work in cooperation with other institutions, more integrated systems may be developed, thus improving the general protection mechanisms against cyber threats. From society's perspective, cyber security is crucial because people trust software and hardware systems. With consumers shopping, speaking, and transacting online, robust security guarantees the protection of consumer information and a safeguard against fraud and scam. Also, the government needs to change legal regulations because new cyber threats create certain problems; thus, it is necessary to encourage people to use the Internet safely. The essence of integrating cyber security on the international level affects diplomatic relations and economic security. Introducing the cooperation at the international level is the primary step coping with the transnational cybercriminal activity, which endangered global business and communication systems. Hence, cyber security is not only the technological requirement to be incorporated into digital transformation but also a business continuity and growth necessity in the contemporary globalized world.

Reference

1. Chowdhry, D. G., Verma, R., &Mathur, M. (Eds.). (2020). *The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security*. CRC Press.
2. Damaraju, A. (2024). Cloud Security Challenges and Solutions in the Era of Digital Transformation. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 387-413.
3. Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 1-70). Cham: Springer Nature Switzerland.
4. Nowicka, J., Ciekanowski, Z., Kudins, J., &Dąbrowski, P. J. (2024). Managing organizational security in the era of digital transformation.
5. Shaikh, M., Datir, a. P., &Birajdar, A. S. (2024). Cyber Security in the Age of Digital Transformation. *Cyber Security in The Age Of Digital Transformation*.
6. Spremić, M., &Šimunic, A. (2018, July). Cyber security challenges in digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.
7. Stewart, H. (2023). Digital transformation security challenges. *Journal of Computer Information Systems*, *63*(4), 919-936.
8. Tagarev, T., &Stoianov, N. (2019). Digital Transformation, Cyber Security and Resilience. Information & Security: An International Journal, 43(1), 1-398.
9. Taherdoost, H., Madanchian, M., &Ebrahimi, M. (2021). Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities

and Challenges. *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, 99-117.

10. Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1-20.