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

Cyber security and digital transformation issues in the information age

Vilas Nair
Assistant Professor, SCMS School of Technology and Management,
Prathap Nagar Muttom, Aluva, Ernakulam, Kerala-683106
vilasnair@scmsgroup.org

Dr. M. Sivasankari
Assistant Professor, Department of Corporate Secretary Ship and Accounting & Finance,
SRM Institute of Science and Technology, Kattankulathur, Chennai.- 626126
sivasankari.m88@gmail.com

Dr.Priyanka Jayaraj
Associate professor, Department of B.Com IT,
Sri Ramakrishna College of Arts and Science , Coimbatore
priyankajayaraj@srcas.ac.in

Dr.V.Seedha Devi
Associate Professor, Department of Information Technology,
Jaya Engineering College, Thiruninravur , Chennai
seethaitjec@gmail.com

Dr. Aruna. V
Assistant Professor, Department of MBA,
St. Joseph's Institute of Technology, OMR, Chennai-600119
arunav@stjosephstechnology.ac.in

Dr. Priyanka Bhatt
Associate Professor, GTU-School of Management Studies,
Gujarat Technological University, Ahmedabad, Gujarat
bhattpriyanka273@gmail.com

Abstract

The Information Age has transformed worldwide connections and commercial operations via digital transformation, however it also presents intricate cybersecurity issues. Digital transformation fosters creativity, efficiency, and data-driven decision-making across sectors.. These vulnerabilities arise from insufficient security frameworks, advancing cyber threats, and the emergence of sophisticated cyber-attacks. The interdependent characteristics of contemporary systems exacerbate the possible consequences of breaches, jeopardizing data privacy, operational continuity, and customer confidence. Moreover, adherence to changing legal frameworks like

GDPR and CCPA poses a considerable problem for organisations balancing the conflicting demands of modernization and security. Cybersecurity must be prioritized strategically, necessitating organisations to implement proactive measures like zero-trust architectures, constant threat monitoring, and comprehensive incident response plans. The integration of cybersecurity and digital transformation is crucial for developing resilient ecosystems that use technology while maintaining security. Organisations may manage risks and capitalize on the advantages of digital transformation by prioritizing staff training, using sophisticated threat detection technology, and integrating security into the foundation of digital initiatives. This abstract emphasizes the critical need to tackle cybersecurity concerns as essential to the success of digital transformation efforts in the Information Age.

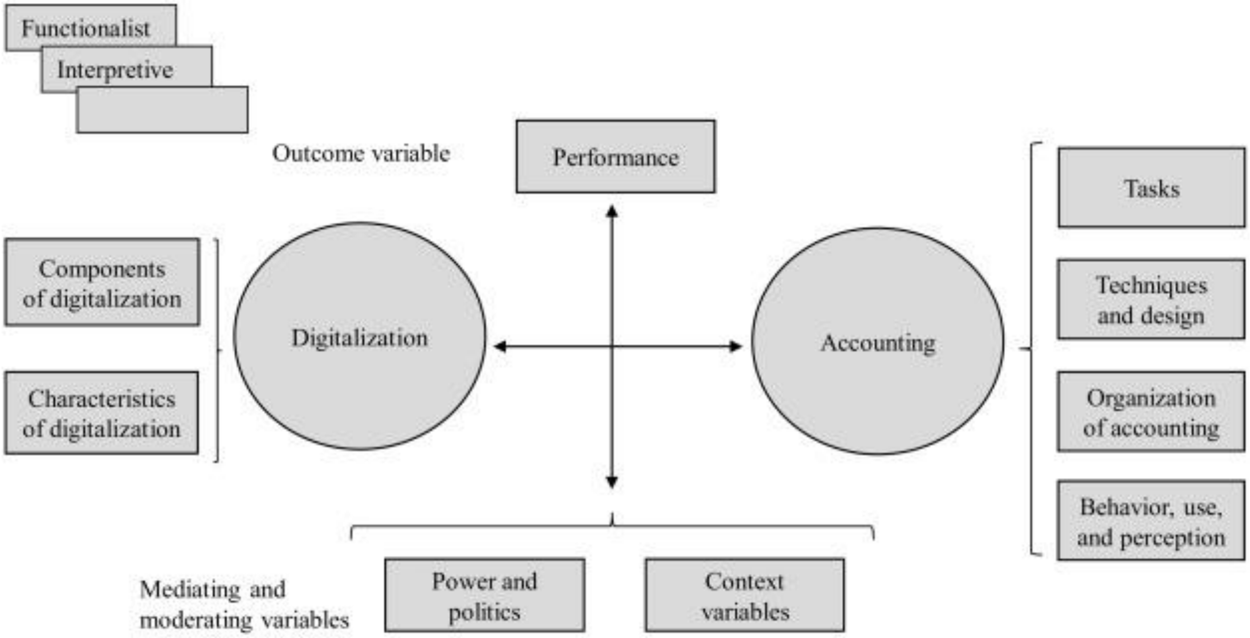
Keywords: Cybersecurity, Digital Transformation, Information Age, Data Privacy, Cyber Threats, Zero-Trust Architecture, Regulatory Compliance, Risk Mitigation, Advanced Technologies, Organizational Resilience

Introduction

The emergence of the Information Age has revolutionized the interactions and operations of people, organisations, and society. Digital transformation, propelled by technological developments has yielded unparalleled advantages across several industries, including healthcare, education, finance, and commerce. As digital systems become more intricate and linked, they simultaneously increase their susceptibility to cyber assaults. Cybersecurity has emerged as a paramount issue, prompting organisations and governments to spend significantly in safeguarding their digital infrastructure and data assets. This paper examines the convergence of cybersecurity and digital transformation, assessing their consequences and recommending solutions to manage related risks. Möller (2023) asserts that cybersecurity transcends a purely technical problem, including a holistic concern that overlaps with organisational strategies, policies, and culture. These technologies have transformed sectors, providing avenues for innovation and efficiency. Nonetheless, they also broaden the attack surface for cyber threats, making effective cybersecurity measures essential. The author recognizes developing hazards, including as advanced malware and insider threats, exacerbated by the growing complexity of networked systems. The chapter primarily emphasizes the incorporation of cybersecurity inside the digital transformation process. The report advocates for proactive strategies that integrate security into the design and execution of digital activities. The chapter emphasizes optimal practices, including the implementation of a risk-based strategy, the execution of frequent threat evaluations, and the use of sophisticated technology like as block chain and quantum cryptography. It underscores the need of connecting cybersecurity strategy with business goals to guarantee resilience and reliability. A notable element addressed is the human role in cybersecurity. The report emphasizes that staff, sometimes seen as the weakest link, are essential in maintaining security. Organisations must provide resources to training programs to improve cyber awareness and cultivate a culture of alertness. The author examines the significance of leadership in advancing cybersecurity measures, endorsing a top-down strategy to prioritise and deploy resources efficiently. This chapter analyses frameworks such as GDPR and ISO standards that assist organisations in developing comprehensive security measures. Moreover, the author examines ethical quandaries in cybersecurity, including the equilibrium between privacy and surveillance, as well as the judicious use of AI in monitoring systems. The chapter finishes with a prospective outlook, underscoring the need for ongoing innovation in cybersecurity to address emerging threats. Möller advocates for cooperation among stakeholders, including governments, academia, and business, to establish a safe digital environment. Integrating cybersecurity into digital transformation enables organisations to protect their assets and secure a competitive advantage in a more interconnected environment.

Garcia-Perez (2023 highlighted the hazards engendered by these improvements, especially regarding cybersecurity. The authors assert that resilience in healthcare systems depends on the capacity to foresee, address, and recuperate from cyber threats while maintaining continuity of treatment. These technologies improve patient care while also increasing the vulnerability to attackers. The research delineates prevalent cyber dangers, including data breache, assaults, and the exploitation of vulnerabilities in IoT-enabled medical equipment, which may interrupt essential operations and jeopardize patient safety. They advocate for the incorporation of cybersecurity inside the digital transformation process to protect sensitive health information and guarantee system dependability. Essential suggestions include the deployment of sophisticated threat detection systems, zero-trust frameworks, and encryption technologies. The authors emphasize the significance of proactive strategies, including routine security audits and ongoing surveillance of network activity. The research highlights the human element as a crucial aspect of cybersecurity resilience. Healthcare personnel often become targets of phishing and social engineering assaults, making employee awareness and training essential. Establishing a security culture inside healthcare organisations is prioritized to reduce risks linked to human error. A major element addressed is regulatory compliance. The authors underscore the significance of frameworks such as GDPR and HIPAA in guaranteeing comprehensive data protection and accountability. They also tackle the ethical dilemmas of reconciling data privacy with the practical requirements of healthcare systems, especially with data sharing and AI-driven diagnoses. This entails the incorporation of cybersecurity protocols, allocation of resources for staff training, compliance with legal requirements, and the promotion of a security-conscious culture. The research highlights the need of cooperation among politicians, healthcare professionals, and technological innovators to tackle increasing cyber dangers. Aligning cybersecurity with digital transformation enables healthcare institutions to bolster resilience, safeguard patient data, and uphold trust within a progressively digital healthcare environment.

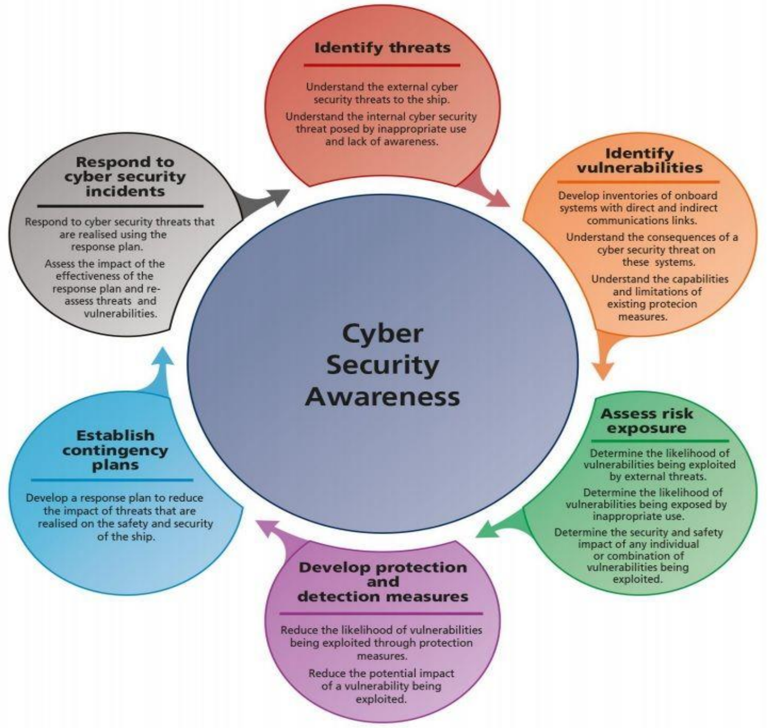
Figure: 1


Functionalist
Interpretive
Outcome variable
Performance
Components of digitalization
Characteristics of digitalization
Digitalization
Accounting
Tasks
Techniques and design
Organization of accounting
Behavior, use, and perception
Mediating and moderating variables
Power and politics
Context variables

Background of the Study

The worldwide transition to digitalization has been propelled by the growing dependence on data and connection. Organisations use digital technologies to augment operational efficiency, refine decision-making, and provide new services. Nonetheless, this rapid acceptance presents considerable obstacles. Studies indicate that the financial impact of cybercrime is anticipated to ascend to billions of dollars each year, representing a significant risk to economic stability and community confidence. The current literature highlights the need for comprehensive cybersecurity frameworks to facilitate digital transformation efforts; nonetheless, a gap persists in comprehending the successful integration of security into the fundamental aspects of digital strategy. Saeed et al. (2023) examine the complex interplay between digital transformation and cybersecurity, emphasizing the difficulties organisations have in sustaining resilience despite rapid technical progress. The report published in Sensors highlights that digital transformation, propelled by advancements such as IoT, big data, AI, and cloud computing, has become essential for organisational competitiveness. The extensive use of these technologies has considerably increased cybersecurity threats, jeopardizing corporate continuity and resilience. The article delineates significant cybersecurity issues associated with digital transformation. This encompasses the expanding attack surface resulting from networked devices, vulnerabilities inside IoT ecosystems, and the intricacies of protecting cloud-based platforms. Emerging risks, like ransomware, phishing, and advanced persistent attacks (APTs), are also emphasized. The authors indicate that small and medium-sized firms (SMEs) are more susceptible due to their frequent deficiency in resources and skills necessary for implementing effective cybersecurity measures. Saeed et al. accentuate that cybersecurity is an essential facilitator of company resilience. They contend that organisations must implement a proactive strategy to tackle these difficulties. The research presents many suggestions, starting with the incorporation of cybersecurity in the first phases of digital transformation efforts. This entails doing thorough risk assessments, implementing zero-trust architectures, and using sophisticated security technologies like as block chain and AI-based threat detection systems. The significance of staff awareness and training is another important theme of the text. Moreover, cultivating a security-first organisational culture is considered vital for maintaining resilience. The document examines the significance of governance and regulatory adherence in improving cybersecurity. Compliance with international standards, including ISO 27001 and GDPR, is recommended to guarantee strong data security and accountability. The authors examine the ethical ramifications of cybersecurity, highlighting the need of reconciling privacy with security protocols, especially in surveillance and data monitoring frameworks. They promote inter- sectoral cooperation and the exchange of information to successfully address complex cyber threats. By tackling the cybersecurity problems linked to digital transformation, enterprises can bolster their resilience, safeguard essential assets, and preserve confidence in a more digital economy. The research offers significant insights for organisations seeking to synchronize their digital initiatives with strong security regimes.

Figure: 2



Cyber Security Awareness
Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond to cyber security incidents

Understand the external cyber security threats to the ship.

Understand the internal cyber security threat posed by inappropriate use and lack of awareness.

Develop inventories of onboard systems with direct and indirect communications links.

Understand the consequences of a cyber security threat on these systems.

Understand the capabilities and limitations of existing protecion measures.

Determine the likelihood of vulnerabilities being exploited by external threats.

Determine the likelihood of vulnerabilities being exposed by inappropriate use.

Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

Reduce the likelihood of vulnerabilities being exploited through protection measures.

Reduce the potential impact of a vulnerability being exploited.

Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.

Respond to cyber security threats that are realised using the response plan.

Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Literature review and research Agenda

Özsungur (2021) investigates how cybersecurity and business management techniques might be used to support effective digital transformation. To protect digital assets, ensure continuity, and foster stakeholder confidence, organisations must align cybersecurity strategy with business objectives. The author outlines the main problems that organisations face, including the rapid evolution of cyber threats, a lack of awareness, and the misalignment of cybersecurity efforts with strategic goals. The researcher advocates for a holistic approach to cybersecurity, integrating it into the operational, tactical, and strategic levels of business management. In order to mitigate cybersecurity risks, the chapter highlights the need of putting frameworks like risk management, governance models, and compliance systems into place. Human factors are given a lot of attention, particularly leadership and employee awareness. A security-focused culture and training initiatives are essential for reducing the risks brought on by human error.. Saeed et al. (2024). However, there are risks associated with growing digitization that might seriously affect critical infrastructure. The authors outline important risks, such as cyber-attacks targeting oil pipelines, power grids, and renewable energy facilities. These risks might result in financial losses, operational disruptions, and even threats to national security. These challenges are exacerbated by the complexity of interconnected energy networks and the lack of standardization in cybersecurity procedures. In order to lessen these vulnerabilities, the report recommends using a risk-based approach to cybersecurity. To secure sensitive data, it is advised to use real-time monitoring systems, zero-trust architecture, and robust encryption techniques. The authors stress how important it is to teach employees and foster a security-conscious culture inside energy organisations. Saeed et al. By incorporating these strategies into digital transformation initiatives, the energy sector will be able to ensure sustainability, safety, and reliability. Digital transformation, driven by advancements in AI, IoT, and cloud computing, has become a vital component of modern civilizations, as highlighted by Tagarev et al. (2021). However, it also poses serious cybersecurity risks that might compromise critical infrastructure, disrupt services, and threaten societal order. The concept of social resilience—which is the ability to anticipate, withstand, and recover from cyber events—is emphasized by the editors. They argue that in order to achieve resilience, cybersecurity must be included into digital transformation programs at the organisational and national levels. The use of risk management frameworks, advanced threat detection technologies, and collaboration between the public and private sectors to strengthen security are among the main issues. The book looks at moral and legal conundrums, such as how to balance security and privacy and how to abuse monitoring technologies. International standards and regulatory frameworks are seen as essential tools for ensuring adherence and protecting sensitive information. The editors advocate for a holistic approach to cybersecurity that incorporates social, strategic, and technical elements. Communities may strengthen resilience, protect critical infrastructure, and foster trust in an increasingly interconnected world by coordinating digital change with strict security measures.

Research Gap

Numerous unresolved enquiries exist on the interplay between security and the evolution of technology in the Information Age. The socio-technical challenges, including the ethical, cultural, and policy implications of rapid digitalisation, have not been as extensively addressed in the literature as technological advancements. There is a paucity of empirical research on the resilience of firms transitioning to cloud-based and AI-driven systems, particularly in relation to managing cybersecurity threats throughout this transition. Moreover, there is no evidence that the existing regulatory frameworks effectively mitigate emerging dangers such as ransomware and quantum computing attacks. The methodology of the present research mostly relies on theoretical models or simulations, without sufficient real-world case studies or longitudinal analyses to assess the temporal evolution of cyber risks. Moreover, there are deficiencies in our understanding of how cybersecurity practices influence non-technical sectors and small to medium-sized enterprises (SMEs), who face distinct challenges throughout digital transformation. Interdisciplinary approaches that amalgamate technological innovation with socioeconomic and psychological research are essential to bridge these gaps.

Significance of the Study

The study is significant since it addresses a crucial global challenge—facilitating secure digital transition. The findings augment the current knowledge on cybersecurity and provide pragmatic advice for policymakers, business leaders, and technology specialists. This research underlines the need of adopting proactive techniques for risk management via an analysis of the correlation between digital transformation and cybersecurity. The research underscores the need for collaboration among stakeholders to create resilient digital ecosystems that foster innovation while safeguarding data integrity and privacy. Sandhu (2021) analyses the evolving dynamics of cybersecurity in the context of digital transformation, evaluating the advantages and challenges that emerge from this paradigm shift. These technologies has substantial potential to revolutionize sectors, improve efficiency, and foster innovation. However, they also provide a new spectrum of cybersecurity concerns. These include data breaches, ransomware attacks, insider threats, and vulnerabilities inside networked systems. Sandhu highlights that alleviating these risks is crucial for the success of digital transformation initiatives. The chapter primarily examines the duality of cybersecurity in digital transformation, seen as both a challenge and an enabler. Insufficient cybersecurity may impede the adoption of digital technologies by eroding trust and exposing companies to operational disruptions. In contrast, robust cybersecurity measures may foster innovation, enhance customer confidence, and provide a competitive edge. Sandhu underscores the need for organisations to adopt a proactive approach by integrating cybersecurity into the design and implementation of digital initiatives. This include using AI for prompt threat detection, instituting zero-trust security frameworks, and employing encryption to protect vital information. Human factors are seen as a crucial component of cybersecurity. Sandhu notes that people often constitute the most susceptible element of security systems due to ignorance or negligence. Organisations must focus employee training and foster a culture of cybersecurity to mitigate risks. The chapter examines legal and ethical considerations, emphasising the need of complying with frameworks like GDPR and ISO standards to protect data privacy and uphold ethical conduct. Moreover, Sandhu underscores the need of collaboration among governments, companies, and academia in mitigating cyber dangers and developing innovative security solutions. By addressing challenges and using opportunities presented by advancing technology, businesses may achieve a secure, resilient, and innovative digital future.

Research Statement

Digital transformation offers several advantages, although it also exposes organisations to various cyber threats. Furthermore, a consistent gap occurs between the pace of technological progress and the implementation of adequate security protocols. This study seeks to examine effective strategies for integrating cybersecurity into digital transformation efforts, therefore reducing risks and enhancing organisational resilience. Mijwil et al. (2023) highlighted the growing reliance of public services on digital technology and the need for robust governance structures to effectively address cybersecurity risks. However, the digitization of governmental organisations increases their susceptibility to cyber-attacks. Widespread dangers like as data breaches, cyber-attacks, and weaknesses inside critical infrastructure may interrupt essential services and erode public trust. The study mainly investigates cybersecurity governance, which is described as a systematic approach to managing cybersecurity risks. Governance frameworks are essential for ensuring accountability, strategy coherence, and effective resource allocation. The authors assert that cybersecurity governance must be integrated into the overarching strategy of digital transformation to protect sensitive information, guarantee service continuity, and foster trust in digital systems. The report highlights essential components of effective cybersecurity governance, such as risk management, policy development, and compliance supervision. They emphasize the need of regulatory frameworks, such as GDPR, to ensure data security and privacy. An essential aspect discussed is the role of leadership in cybersecurity governance. The study underscores the need for lawmakers and public administration to prioritise cybersecurity. Leadership must enable the execution of governance principles and provide resources to bolster resilience against cyber threats. They assert that governance frameworks must balance the need for security with transparency and inclusivity. The authors promote a proactive and collaborative approach to cybersecurity governance in public services. Governments, technology providers, and stakeholders must cooperate to develop resilient systems capable of withstanding cyber-attacks. Incorporating cybersecurity governance into the digital transformation process enhances operational efficiency in public services, safeguards citizen data, and sustains trust in the digital environment. This study provides critical insights for policymakers and practitioners seeking to navigate the complexities of cybersecurity in the digital age.

Research Methodology

This study uses a qualitative research methodology, using convenience sampling to collect data from professionals and businesses engaged in digital transformation. Convenience sampling enables the inclusion of readily accessible individuals who are willing to provide ideas based on their experiences. Data will be collected using semi-structured interviews, questionnaires, and case studies to provide an in-depth understanding of the challenges and strategies related to cybersecurity in the context of digital transformation.

Analysis, findings and Results

Factors influence cybersecurity and digital transformation issues in the Information Age

Rapid Technological Advancements: The fast pace of technological progress creates challenges in maintaining secure systems, as organizations struggle to adapt to new innovations while protecting sensitive data. Emerging technologies like AI, IoT, and block chain introduce vulnerabilities, often outpacing the development of effective cybersecurity measures. This dynamic environment demands agile strategies to mitigate risks.

Legacy Systems: Legacy systems pose significant cybersecurity risks due to outdated software, limited vendor support, and incompatibility with modern security protocols. These systems are particularly vulnerable to attacks, yet many organizations rely on them for critical operations, making secure integration or replacement a pressing but complex issue requiring careful planning and investment.

Integration Challenges: Integrating new technologies with existing systems often leads to compatibility issues and security vulnerabilities. Complex configurations, disparate architectures, and lack of standardization can expose networks to sophisticated cyber-attacks. Organizations must address these challenges by adopting robust integration strategies and ensuring security protocols are maintained throughout the digital transformation process.

Sophisticated Threats: Cyber threats are becoming increasingly sophisticated, leveraging advanced tools such as AI and automation to exploit vulnerabilities. These threats often bypass traditional defenses, targeting critical systems with precision. As attackers evolve, organizations face escalating challenges in detecting, preventing, and responding to these dynamic and multifaceted cyber risks effectively.

Skilled Workforce Shortage:. This gap hinders organizations' abilities to implement and maintain robust defenses, especially as advanced technologies demand specialized expertise. Bridging this talent deficit requires investments in education, training, and workforce development initiatives to meet growing demands.

Cybersecurity Culture: A lack of cybersecurity awareness and culture within organizations contributes to vulnerabilities. Employees often underestimate risks or fail to follow security protocols, increasing exposure to threats. Building a strong cybersecurity culture requires consistent training, leadership support, and policies promoting proactive security behaviors across all organizational levels.

Budget Constraints: Limited budgets hinder the implementation of comprehensive cybersecurity measures, especially for small and medium enterprises (SMEs). Organizations may struggle to invest in advanced tools, training, or system upgrades, leaving them exposed to evolving threats. Balancing cost constraints with the need for robust cybersecurity is a persistent and critical challenge.

Table 1
Descriptive statistics

S.No	Factors	N	Mean	SD
1	Rapid Technological Advancements:	200	**3.19**	.908
2	Legacy Systems	200	3.20	1.289
3	Integration Challenges	200	3.31	1.276
4	Sophisticated Threats	200	3.0	0.865
5	Skilled Workforce Shortage:	200	3.26	1.143
6	Cybersecurity Culture	200	2.97	0.876
7	Budget Constraints	200	2.85	0.754

Rapid Technological Advancements (Mean = 3.19, SD = 0.908): This factor reflects a moderate influence, with a relatively low variability. Organizations recognize the role of advancing technologies but manage them with some consistency. **Legacy Systems (Mean = 3.20, SD = 1.289)** Legacy systems also score moderately, indicating they remain a significant concern for cybersecurity. The high standard deviation suggests variability in how organizations perceive and experience challenges with outdated systems. **Integration Challenges (Mean = 3.31, SD = 1.276):** Integration challenges rank slightly higher among concerns. The relatively high variability indicates that while some organizations manage integrations effectively, others face significant issues, likely due to differences in resources or expertise. **Sophisticated Threats (Mean = 3.00, SD = 0.865):** This factor has a neutral mean, suggesting that while advanced threats are recognized, their perceived impact varies less across respondents. The lower SD reflects a more consistent acknowledgment of this issue. **Skilled Workforce Shortage (Mean = 3.26, SD = 1.143)**: The shortage of skilled professionals is a moderately significant challenge. Its variability indicates differences in the availability of cybersecurity talent across organizations or regions. **Cybersecurity Culture (Mean = 2.97, SD = 0.876)**: This factor scores slightly below neutral, suggesting that a strong cybersecurity culture may not be uniformly present in organizations. The relatively low SD shows consistency in perceptions. **Budget Constraints (Mean = 2.85, SD = 0.754):** Budget constraints rank as the least significant issue, with the lowest mean and variability. This suggests that while budget limitations exist, they are less prominent compared to other factors.

Implications

The study's conclusions include both theoretical and practical significance. The study theoretically enhances the academic debate on cybersecurity and digital transformation by providing novel insights into their integration. The report offered practical guidelines for organisations aiming to improve their cybersecurity stance while advancing digital innovation. Policymakers may use the data to design legislation and standards that facilitate safe digital transition. The report emphasizes the need of cultivating a culture of security awareness inside organisations to guarantee sustained resilience against cyber-attacks.

Recommendations and Suggestions

1. Organizations should implement a zero-trust model to minimize vulnerabilities by ensuring that all users and devices are authenticated and authorized.
2. Regular training programs should be conducted to enhance employees' awareness of cybersecurity best practices and emerging threats.
3. Organizations should use AI and machine learning for real-time threat detection and response.
4. Establishing clear protocols for responding to cyber incidents can minimize downtime and data loss.
5. Governments, private enterprises, and academia should collaborate to share knowledge and resources for tackling cyber threats effectively.

Conclusion

The data suggests that integration challenges (Mean = 3.31) and skilled workforce shortage (Mean = 3.26) are perceived as the most critical issues influencing cybersecurity and digital transformation. On the other hand, budget constraints (Mean = 2.85) and cybersecurity culture (Mean = 2.97) are relatively less pressing concerns. The variety in reactions to elements like legacy systems and integration obstacles indicates that organisations encounter these issues differently, possibly owing to differences in technical maturity, resource allocation, and strategic goals. These observations underscore the need for customized solutions to tackle individual difficulties, especially in workforce development and system integration, while fostering a proactive and resilient cybersecurity culture. The intersection of cybersecurity and digital transformation poses both a difficulty and an opportunity in the Information Age. Although digitalization fosters innovation and efficiency, it also exposes organisations to considerable cyber dangers that need proactive management. This research emphasizes the need of incorporating cybersecurity into digital plans to develop resilient systems that can endure shifting threats. Organisations can manage the intricacies of the digital world and ensure sustainable development by implementing rigorous security measures, promoting cooperation, and prioritizing staff training.

Reference

1. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. Technovation, 121, 102583.

2. Hai, T.N.; Van, Q.N.; Thi Tuyet, M.N. Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. Emerg. Sci. J. 2021, 5, 21–36. [Google Scholar] [CrossRef]
3. Hasan, M.F.; Al-Ramadan, N.S. Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. Soc. Sci. Humanit. J. 2021, 5, 2312–2323. [Google Scholar]
4. Joveda, N.; Khan, M.T.; Pathak, A.; Chattogram, B. Cyber laundering: A threat to banking industries in Bangladesh: In quest of effective legal framework and cyber security of financial information. Int. J. Econ. Financ. 2019, 11, 54–65
5. Matt, C.; Hess, T.; Benlian, A. Digital transformation strategies. Bus. Inf. Syst. Eng. 2015, 57, 339–343.
6. Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. Mesopotamian journal of cybersecurity, 2023, 1-6.
7. Möller, D. Cybersecurity in Digital Transformation: Scope and Applications; Springer: Berlin/Heidelberg, Germany, 2020. [Google Scholar]
8. 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.
9. Özsungur, F. (2021). Business management and strategy in cybersecurity for digital transformation. In Handbook of Research on Advancing Cybersecurity for Digital Transformation (pp. 144-162). IGI Global.
10. Rodrigues, A.R.D.; Ferreira, F.A.; Teixeira, F.J.; Zopounidis, C. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Res. Int. Bus. Financ. **2022**, 60, 101616
11. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
12. Saeed, S., Gull, H., Aldossary, M. M., Altamimi, A. F., Alshahrani, M. S., Saqib, M., ... & Almuhaideb, A. M. (2024). Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications. Information, 15(12), 764.
13. Sandhu, K. (2021). Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges. Handbook of Research on Advancing Cybersecurity for Digital Transformation, 1-17.
14. Tagarev, T., Atanassov, K. T., Kharchenko, V., & Kacprzyk, J. (Eds.). (2021). Digital transformation, Cyber security and resilience of modern societies (pp. 117-136). Heidelberg: Springer.
15. Uddin, M.H.; Ali, M.H.; Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Manag. **2020**, 22, 239–309