https://doi.org/10.33472/AFJBS.6.6.2024.2503-2514

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Cybersecurity and Its Privacy Awareness in An Era of Digital Transformation

Dr. Shahin A[1], Dr Nafisa Idris M[2]

[1]Assistant Professor, JBAS College for Women, Teynampet, Chennai-18.
Email: [1]shahin@jbascollege.edu.in
[2]Assistant Professor, Guru Nanak College (Autonomous), Velachery,Chennai - 42.
Email: [2]nafisaidris.m@gurunanakcollege.edu.in

Article Info

Volume 6, Issue 6, June 2024

Received: 09 April 2024

Accepted: 15 May 2024

Published: 10 June 2024

doi: 10.33472/AFJBS.6.6.2024.2503-2514

ABSTRACT:

Digital technologies have been evolving over many years, but the pandemic provided an unprecedented acceleration. It acted as a catalyst for digital transformation in various ways. In the aftermath of the pandemic, there is a noticeable transformation in the way businesses harness information technology. Companies are increasingly utilizing technology not just for their routine activities but also to expedite processes, reduce expenses, and boost overall productivity. Information security and data protection, dynamic fields, are continually challenged and influenced by advancements in digital age technologies and innovative business practices. The aim of this article is to evaluate cyber awareness and its security among users in an era of digital transformation. The sample size of 100 was determined through random sampling. The study was analysed using the SPSS software to derive results in relation to the specified objectives and hypotheses. The study finds a strong link between socio-economic variables and cybersecurity awareness. Targeted campaigns are crucial for effective cybersecurity education. Top threats include malware and phishing, emphasizing the need for preventive measures and comprehensive training.

Keywords: Digital Transformation, Cybersecurity, Privacy, Awareness, Protection

1. Introduction

The widespread adoption of digital technologies to improve or even establish entirely new business models, customer experiences, and operational processes has resulted in a fundamental shift in how organisation function **(World Economic Forum, 2021)[1].** Although this transformation has been ongoing for several years, the pandemic brought about an unprecedented escalation. In many respects, the pandemic served as a driving force for virtual transformation. Virtually every industry experienced a newfound reliance on virtual work technologies. Individuals who had never engaged in remote work suddenly found themselves working from laptops at their recreation room tables. Pubs and restaurants had to quickly adaptby implementing digital ordering services **(McKinsey & Company, 2021)[2].**

Theoretical Background

1.1 Digital Transformation

Digital transformation involves a comprehensive reworking of business operations, daily activities, procedures, capacities, and business frameworks to maximize the benefits of cutting-edge technologies and their ongoing influence on society. This approach adopts a forward-thinking stance regarding future revolutions **(Westerman et al., 2014)[3].** In simple term, it requires the alteration of social norms, firms, eco-systemic, revenue models and operations by incorporating modern technologies and intelligent processes **(Ross et al., 2018)[4].**

1.2 Technological Catalysts: Driving Digital Transformation InModern Business

Modern businesses are leveraging several key technologies to drive digital transformation. Social media plays a pivotal role in customer interactions, allowing businesses to monitor feedback and trends while encouraging satisfied customers to contribute to cost- effective marketing **(Westerman et al., 2014)[3].** Cloud computing is essential for scalable digital frameworks, enabling the swift deployment of solutions and fostering integration and collaboration **(Ross et al., 2018)[4]**. The rise in remote work and mobile device usage has stimulated digital transformation, facilitated collaboration and enhanced tasks through video conferencing and applications for monitoring in real-time on mobile devices. Data processing guides informed decision-making by understanding customer behavior and preferences **(Westerman et al., 2014)[3]**. The Internet of Things connects devices, offering alternate to manage physical products and experiences, while Artificial Intelligence optimizes processes, streamlines operations, and enhances adaptability, already making a substantial impact on various industries, from self-guided cars to chatbots **(Ross et al., 2018)[4].** These technologies collectively empower businesses to adapt to changing consumer behaviours, improve customerexperiences, and stay at the forefront of innovation[5].

1.3 Cybersecurity and Privacy

Cybersecurity and privacy awareness pertain to the comprehension, awareness, and consciousness that people and firms possess concerning the challenges, uncertainty and protective measures related to information security and privacy. This entails acknowledging the significance of protecting digital assets, personal information and personal data from unlawful access, exposure, alteration, or devastation.

1.4 Threats and Challenges of Cybersecurity and Privacy

Cybersecurity and privacy face a myriad of threats and issues that pose significant risks to individuals, organizations, and societies at large. Malware, such as viruses and ransomware, threatens data integrity and operational continuity, while phishing exploits human vulnerability by deceiving users into disclosing sensitive information. Data breaches, fueled by unauthorized access, compromise privacy and lead to identity theft. Insider threats, arising from malicious or unwitting individuals within organizations, pose substantial risks to data security.

Inadequate security measures, IoT vulnerabilities, and weak authentication expose systems to exploitation, emphasizing the importance of robust protective mechanisms. User awareness gaps contribute to susceptibility, as uninformed individuals may fall victim to social engineering attacks. Supply chain vulnerabilities and regulatory compliance challenges add layers of complexity, requiring vigilant oversight.

Encryption lapses, especially in data transmission and storage, heighten the risk of unauthorized access. As technology advances, emerging threats like quantum computing vulnerabilities loom on the horizon. Addressing these issues demands a holistic approach involving robust cybersecurity frameworks, ongoing education, and compliance with evolving regulations. Proactive measures, including strong authentication and encryption practices, are essential to mitigating these threats and safeguarding the digital landscape.

1.5 Navigating Challenges in the Digital Era

Information Security and Data Protection face evolving challenges in the digital age, driven by technological advancements and changing business practices. Social computing introduces risks through Social Networking Sites, potentially exposing personal data to unauthorized users. Cloud computing, while not inherently violating data protection principles, poses challenges in cross-border data transfers. Guidelines aligning with GDPR e-privacy requirements aim to mitigate these risks. Internet of Things (IoT) introduces privacy concerns, as connected devices may compromise confidentiality and security. Unique identification codes for objects may lead to sensitive information exposure, while inadequate security measures and default passwords create vulnerabilities. Big Data (BD) and Big Data Analytics (BDA) present privacy challenges, as the massive volume of collected data can result in inaccurate conclusions or trends about individuals, contradicting GDPR principles of minimizing personal data processing.

As technology advances, addressing these challenges becomes crucial to ensure the protection of user data, emphasizing the need for robust security measures and compliance withevolving data protection regulations[6].

1.6 Cybersecurity Solutions for Digital Resilience

In the digital age, safeguarding information is paramount, ensuring the protection of personal data and upholding privacy as a fundamental human right. FCA and ISO 27001 compliant cybersecurity solutions, including Cranberry Cloud Hosted Desktop and Cranberry Desktop. These solutions feature multi-factor authentication, regular vulnerability testing, and robust data encryption. Protect information by implementing data backups with unique credentials and staying vigilant with phishing simulations. Adopt multi-factor authentication, advanced email filtering, and keep systems updated to patch vulnerabilities. Establish and enforce a comprehensive cybersecurity policy, including disaster recovery plans. Understand digital transformation risks and prioritize security to enhance overall cyber resilience[7].

1.7 Policies and Regulatory Frameworks Governing Cybersecurity

Policies and regulatory frameworks governing cybersecurity are essentially sets of rules and

guidelines established by governments and organizations to manage and safeguard digital information and technology systems. In the fast-paced and interconnected world of the internet, these frameworks act as a vital place in defining the standards practices that individuals, businesses, and governmental bodies must adhere to ensure the security of digital assets.

These policies typically address various aspects of cybersecurity, including data protection, network security, incident response, and the overall safeguarding of sensitive information. They serve as a roadmap, outlining the measures and procedures that entities should implement to mitigate risks, prevent unauthorized access, and respond effectively to cyber threats.

Moreover, regulatory frameworks often carry legal implications, stipulating the consequences for non-compliance. They evolve in response to the dynamic nature of cyber threats, reflecting ongoing efforts to stay ahead of potential risks and vulnerabilities. Overall, these policies and frameworks provide a structured approach to maintaining the integrity, confidentiality, and availability of digital information in an increasingly interconnected and digitalized environment[8].

2. Review of Literature

Mohsin and Asthana (2023)[9] investigate the intersection of cybersecurity and privacy in the rapidly evolving cyberspace. It delves into the challenges posed by data protection concerns, examines the impact of cybersecurity policies on privacy, and emphasizes the global nature of cyberspace governance. In today's tech-driven world, where artificial intelligence replaces manual intelligence, internet privacy remains a contentious legal issue. The legal community must develop robust policies to protect against cyber threats and reevaluate online privacy in the face of society's increasing computerization.

Moti et.al (2022)[10] discovered that internet users in Israel, Slovenia, Poland, and Turkey demonstrate sufficient awareness of cyber threats but tend to adopt fewer preventive measures. The study found that greater cyber knowledge is associated with increased awareness, irrespective of the country or gender. While awareness is linked to the use of protective tools, it does not necessarily correlate with the disclosure of information. The study highlights country-specific variations influencing the dynamics among consciousness, information, and behaviours, providing insights for targeted cybersecurity awareness programs.

Alqahtani (2022)[11] explores the influence of software program and electronic mail security on overall cybersecurity consciousness. Findings reveal students in developing countries possess good knowledge of cybersecurity, demonstrating awareness of software updates and email security, highlighting a positive level of consciousness among university students regarding cyber threats.

Hicham and Lhacen (2020)[12] investigates the influence of the pandemic on the process of implementing digital transformation. The findings indicate the effect of pandemic on the perception of digital transformation in Morocco. Both the public and private sectors have takenadvantage of the lockdown to make advance progress in terms of digital transformation.

Sambada and Bhayani (2018)[13] found that consumers, while concerned about online privacy, often disclose personal information for personalized content benefits. Lack of trust leads to fabricated details or privacy tools use. Consumers avoid marketing for privacy but engage in personalized ads when feeling control over social media data.

Nikhita and Ugander (2014)[14] focussed into the obstacles encountered by cybersecurity in the context of emerging technologies. It also examined into the latest developments in cybersecurity techniques, ethical considerations, and the evolving trends shaping the landscape of cybersecurity. The escalating incidence of cybercrimes has prompted numerous governments and organizations to implement preventive measures. Despite these efforts, cybersecurity remains a major concern for many.

3. Statement of the Problem

In contemporary society, our dependence on technology has reached unprecedented levels, influencing crucial aspects such as power, industries, law and order, and safety. Consequently, the significance of cybersecurity becomes paramount, as it is essential for safeguarding data sources and Information technology infrastructure from potential misuse. This encompasses the protection of sensitive data, official records, personally identifiable information, protected health information, personal details, and intellectual property.

4. Need of the Study

Studying cybersecurity in the digital age is crucial due to rising cyber threats, data protection concerns, and evolving regulations. As businesses embrace digital transformation, understanding these risks is vital for implementing effective security measures, ensuring compliance, and fostering a secure environment, ultimately contributing to the responsible useof technology in today's dynamic technological landscape.

5. Objectives

- Examine theoretical background of cybersecurity and privacy within the context of digital transformation era.
- Assess the level of user awareness regarding cybersecurity and privacy in the current era of digital transformation.
- Investigate how threaten factors of cybersecurity and its privacy influence users' awareness level in an era of digital transformation.
- Propose effective measures to address issues related to cybersecurity and privacy in the era of digital transformation.

6. Hypotheses

- There is no significant association between the demographic variables of the users and their awareness of cybersecurity and its privacy in digital era.
- There is no correlation between the cybersecurity threats and its privacy with respect to the user's awareness in an era of digital transformation.

7. Research Methodology

Research methodology involves a systematic and hypothetical investigation of the methods applied within the research. It incorporates the proposed analysis of the methods and values related to a specific branch of information. The current study takes on an exploratory approach, aiming to raise awareness among technology users regarding cybersecurity and privacy amidst the ongoing digital transformation era.

7.1 Data Collection

In this study, a mixed-methods approach was employed to comprehensively explore cybersecurity and privacy awareness during the era of digital transformation. The primary method of data collection involved the use of surveys distributed to a diverse sample of technology users. The survey instrument was designed to elicit quantitative data on users' perceptions, knowledge, and practices related to cybersecurity and privacy. Furthermore, a thorough review of relevant literature, government publications, and industry reports constituted the secondary method of data collection, offering valuable context and insights. This dual approach aimed to triangulate findings and provide a comprehensive understanding of cybersecurity and privacy awareness in an era of digitalization.

7.2 Sampling Size

The sample unit refers to the sum of observations utilized in estimating parameters for a particular population. In this case, a sample of 100 has been randomly selected for analysis.

7.3 Questionnaire Structure

The structure of questionnaire comprises three parts. The first part addresses socio- economic details of technology users, the second focuses on awareness of cybersecurity and privacy, and the final part explores awareness of cybersecurity and privacy issues in an era of digitalization. The study was analyzed using random sampling with statistical tools by SPSS software to ascertain results in relation to the given objectives and hypotheses.

8. Analysis and Interpretation

I. H0: There is no correlation between the demographic variables and their awareness oncybersecurity and its privacy in digital era.

To study the correlation between the demographic variables of the users and their awareness were tested using the chi-square analysis.

TABLE 9.1: DEMOGRAPHIC VARIABLES AND CHI-SQUARE TEST

Particulars		**Unaware**	**Aware**	**Neutral**	**Total**
Gender	**Male Count**	**16**	**24**	**15**	**55**
	Percent within male	29	43	28	100
	Female Count	**13**	**16**	**16**	**45**
	Percent within male	29	35	36	100
	Total Count	**29**	**40**	**31**	**100**
	Percent within awareness level	28.8	39.5	31	100
	Chi-Square	**Val 4.001^{NS}**	**df -2**	**Sig .000**	
	Below 20 yrs Count	**12**	**0**	**0**	**12**
	Percent within Below 20 yrs	100	0	0	100
	21 – 30 yrs Count	**29**	**13**	**0**	**42**

Age	Percent within 21 – 30 yrs	69	31	0	100
	31 – 50 yrs Count	**0**	**29**	**1**	**30**
	Percent within 31 – 50 yrs	0	97	3	100
	Above 50 yrs Count	**0**	**3**	**13**	**16**
	Percent within Above 50 yrs	0	20	80	100
	Total Count	**41**	**45**	**14**	**100**
	Percent within awareness level	41.3	45.3	13.6	100
	Chi-Square	**Val 716.131 [a]**	**df - 6**	**Sig .000**	
Marital status	**Married Count**	**3**	**30**	**26**	**59**
	Percent within	5	51	44	100
	Unmarried Count	**41**	**0**	**0**	**41**
	Percent within	100	0	0	100
	Total Count	**44**	**30**	**26**	**100**
	Percent within awareness level	44	30	26	100
	Chi-Square	**Val 439.256 [a]**	**df - 2**	**Sig .000**	
Educational Qualification	**No Formal Education Count**	**10**	**0**	**0**	**10**
	Percent within No Formal Education	100	0	0	100
	School/Diploma Count	**15**	**0**	**0**	**15**
	Percent within School/Diploma	100	0	0	100
	UG/PG Count	**4**	**32**	**4**	**40**
	Percent within UG/PG	10	81	9	100
	Professional/Ph.D. Count	**0**	**6**	**29**	**35**
	Percent within Professional/Ph.D.	0	17	83	100
	Total Count	**29**	**38**	**33**	**100**
	Percent within awareness level	29	38	33	100
	Chi-Square	**Val 718.360 [a]**	**df - 6**	**Sig .000**	
Occupation	**Student Count**	**10**	**0**	**0**	**10**
	Percent within Student	100	0	0	100
	Business/Professional Count	**1**	**18**	**11**	**30**
	Percent within Business/Professional	4	60	36	100
	Salaried Count	**5**	**17**	**21**	**43**
	Percent within Salaried	11	39	50	100
	Home maker /Retired Count	**0**	**0**	**17**	**17**
	Percent within Home maker /Retired	0	0	100	100
	Total Count	**16**	**35**	**49**	**100**
	Percent within awareness level	16	35	49	100
	Chi-Square	**Val 520.217 [a]**	**df - 6**	**Sig .000**	
	Below Rs.30000 Count	**15**	**0**	**0**	**15**
	Percent within Below Rs.30000	100	0	0	100
	Rs.30001 – Rs.50000 Count	**13**	**16**	**16**	**45**
	Percent within Rs.30001 – Rs.50000	29	35	36	100

Monthly Income	**Above Rs.50001 Count**	**0**	**29**	**1**	**30**
	Percent within Above Rs.50001	0	97	3	100
	Total Count	**28**	**45**	**17**	**100**
	Percent within awareness level	**28**	**45**	**17**	100
	Chi-Square	**Val 539.488** [a]	**df - 4**	**Sig .000**	

(Source: Primary data)

Note: [a] **refers Significant at 5 % levelNote: NS denotes Not Significant**

The provided data presents a demographic variable based on categorized by awareness levels (unaware, aware, and neutral). The Pearson Chi-Square values and associated significance levels (Sig.) indicate the degree of association between the variables.

Gender: The awareness levels vary significantly between males and females (Chi- Square = 4.001, Sig. = .000). Awareness percentages within each gender category highlight diverse levels of understanding.

Age: Age groups exhibit a strong association with awareness levels (Chi-Square = 716.131, Sig. = .000). Notably, those below 20 years are uniformly unaware, while awareness increases with age.

Marital Status: There is a correlation between marital status and awareness (Chi- Square = 439.256, Sig. = .000). Unmarried individuals show higher awareness percentages compared to married ones.

Educational Qualification: Educational qualifications are significantly associated with awareness levels (Chi-Square = 718.369, Sig. = .000). Higher education levels correspond to higher awareness.

Occupation: Occupation and awareness levels are significantly associated (Chi-Square = 520.217, Sig. = .000). Students exhibit lower awareness compared to business professionalsand salaried individuals.

Monthly Income: Monthly income levels show a significant association with awareness (Chi-Square = 539.488, Sig. = .000). Higher income brackets correlate with increased awareness.

In summary, the data underscores that awareness levels are influenced by demographic factors, emphasizing the importance of targeted awareness campaigns tailored to specific demographic groups.

II. H0: There is no association between the cybersecurity threats and its privacy with respect to the user's awareness in an era of digital transformation.

An analysis of the respondents' responses was conducted to interpret the factors at play. Factor analysis proves to be a valuable method for discerning hidden or primary factors amidst numerous important variables. In the factor analysis, variables were categorizing the diverse factors influencing cybersecurity and its privacy in relation to user awareness during the era of digital transformation. The collected responses underwent factor analysis, and the results underwent scrutiny through the KMO and Bartlett's test of sphericity.

TABLE 9.2 RELIABILITY STATISTICS

Cronbach's Alpha	No. of Items
.845	13

Source: Computed

The data in Table No. 9.2 clearly indicates that the cronbach's value is 0.845, surpassing the recommended threshold of 0.6. This leads to the conclusion that the provided data can be deemed reliable for conducting further analysis on user awareness levels.

TABLE NO. 9.3 KMO AND BARTLETT'S TEST

KMO measure of sampling adequacy		.810
Bartlett's Test of Sphericity	App. Chi-Square	101.866
	df	110
	Sig	.000

Source: Computed

The observed KMO value of 0.810 exceeds the suggested threshold 0.5, indicating the size of the sample deemed adequate. Additionally, the Barlett's test measure of 0.000 is below 0.01, signifying significance at the 1 percent level. Consequently, both tests confirm the fulfillment of necessary circumstances for doing factor analysis and subsequent outcome are detailed in the following schedule.

TABLE 9.4: TOTAL VARIANCE EXPLAINED

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sum of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
C1	1.739	7.560	39.256	1.739	7.560	39.256	3.340	14.523	30.742
C2	1.317	5.725	44.981	1.317	5.725	44.981	2.553	11.099	41.842
C3	1.227	5.336	50.317	1.227	5.336	50.317	1.949	8.475	50.317

Source: Computed

The findings from Table No. 9.4 indicate that, based on Eigenvalues, a factor analysis was computed to the provided data, resulting from extraction of three factors. The factors identified are related to Preventive Measures Awareness, Human Factor and Training Awareness, and Technological Consideration & Incident Response Awareness.

The Preventive Measures Awareness factors encompass Phishing Awareness, Weak Authentication Awareness, Encryption Awareness, Security Measures Awareness (including firewalls, intrusion detection/prevention systems, secure configurations), and Malware Awareness. **The Human and Training Awareness factors** include Insider Threats Awareness, Regulatory Compliance Awareness, Overall Cybersecurity and Privacy Awareness, User Awareness, and **The Technological Considerations & Incident Response Awareness factors** consist of IoT Vulnerabilities Awareness, Ransomware Awareness, Data Breaches Awareness, and Supply Chain Attacks Awareness. The number of items and their respective loading are detailed in given below schedule.

TABLE 9.5: ROTATED COMPONENT MATRIX

Cybersecurity issues and its Privacy	**Component**		
	Preventive Measures	**Human Factor& Training**	**Technological Consideration & Incident Response**
Malware awareness	0.896		
Phishing awareness	0.885		
Inadequate Security Measures Awareness	0.873		
Lack of Encryption awareness	0.867		
Weak Authentication awareness	0.859		
Insider Threats Awareness		0.740	
Regulatory Compliance Challenges		0.734	
Overall Cybersecurity and Privacy Awareness		0.726	
User Awareness		0.705	
IoT Vulnerabilities Awareness			0.644
Ransomware Awareness			0.628
Data Breaches Awareness			0.615
Supply Chain Attacks Awareness			0.603

Source: Computed

From the table no. 9.5, three key factors are identified. Preventive measures awareness, ranging from 0.859 to 0.896, contribute 50.25% to user awareness. Human awareness factors, ranging from 0.705 to 0.740, contribute 30.25%, while technological and incident response factors, ranging from 0.603 to 0.644, contribute 19.50%. Overall, preventive measures awareness emerges as the most influential factor in users' cybersecurity awareness during the digital transformation era.

9. FINDINGS

Findings of the study provide general insights and trends that are commonly observed in research related to cybersecurity and privacy awareness in the era of digital transformation**.** The finding reveals the correlation among awareness levels and demographic variables. Tailoring awareness campaigns to specific demographic characteristics is crucial for effective cybersecurity education and fostering a vigilant digital community. The study also reveals the significance of cybersecurity threats and awareness factors. Malware, phishing, and inadequate security measures top the list, highlighting the importance of preventive measures and education. Human factors like insider threats and regulatory compliance also weigh heavily, underscoring the need for comprehensive training in cybersecurity and privacy practices.

Further, the findings of the study highlight a rise in complex cyber threats with digital expansion. Individuals increasingly recognize the pivotal role of privacy in the digital era, integrating cybersecurity into digital strategies. Emphasizing a comprehensive approach, the research underscores the challenge of balancing robust security with user convenience. Addressing the evolving regulatory landscape is crucial, emphasizing ongoing research for adaptive strategies in the dynamic digital transformation era.

10. Measures Building Cybersecurity Resilience

To enhance cybersecurity and protect privacy, organizations should prioritize employee training to build a vigilant workforce. Strong password policies and multi-factor authentication bolster access security, while regular software updates and firewalls strengthen network defenses. Encryption for personal information mutually transfer and at rest, along with secure communication protocols, adds an extra layer of protection. Access control measures, limiting system and data access, are vital. Establishing an incident response plan, regular security audits, vulnerability assessments, and robust backup systems contribute to a resilient defense. Implementing reputable antivirus and anti-malware software, securing mobile devices with encryption and remote wipe capabilities, is crucial. For privacy, integrate considerations into system development, comply with data protection laws, inform users, and collaborate for threat intelligence. Continuous monitoring with automated tools ensures real-time threat detection, creating a comprehensive approach for a secure cybersecurity and its privacy.

11. Limitations

- One limitation of this study is the potential for capturing cybersecurity and privacy awareness at a specific moment but not accounting for the rapidly evolving nature of digital threats.
- Additionally, the study's focus on general trends may overlook nuances specific to certainindustries or regions.
- The reliance on self-reported awareness levels introduces a subjective element that may not fully reflect actual behaviors.
- Lastly, the study's scope may not encompass emerging technologies or threats that have surfaced after the data collection period, limiting the comprehensive understanding of thecurrent cybersecurity landscape.

12. Conclusion and Scope for Future Research

In conclusion, the synergy between cybersecurity and privacy awareness is vital in the digital transformation era, demanding a holistic approach. As technology shapes our lives, fortifying digital security and nurturing privacy consciousness is paramount. Further research can focus on adaptive cybersecurity frameworks, understanding psychological aspects of privacy, and exploring regulatory responses. Investigating emerging technologies like AI and blockchain for enhanced security is essential. Continuous research is crucial to anticipate evolving cyber threats. By delving into these areas, researchers contribute to an ongoing dialogue, addressing cybersecurity and privacy concerns in the ever-evolving landscape of digital transformation.

13. Reference

1. World Economic Forum. (2021). "The Great Reset: Building Future-Resilient Societies and Industries." https://www.weforum.org/great-reset/
2. McKinsey & Company. (2021). "How COVID-19 has pushed companies over the technology tipping point-and transformed business forever." https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-covid-19.
3. Westerman, G., Bonnet, D., & McAfee, A. (2014). "Leading Digital: Turning Technology into Business Transformation." Harvard Business Review.
4. Ross, J. W., Beath, C., & Mocker, M. (2018). "Designed for Digital: How to Architect Your Business for Sustained Success." Harvard Business Review Press.
5. https://yourstory.com/mystory/digital-transformation-new-era-business-simplification
6. https://www.aimspress.com/article/doi/10.3934/mbe.2020286?viewType=HTML
7. https://tivarri.com/blog/cybersecurity-in-an-era-of-digital-transformation/
8. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
9. Kamshad Mohsin and Dr. K. B. Asthana - "Information Privacy in Cyberspace: A Study", Dogo Rangsang Research Journal, UGC Care Group I Journal, ISSN: 2347-7180 Vol-13, Issue-4, No. 1., Pg. 176 – 186.
10. Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetinorcid Icon & Hamdullah Nejat Basim, (2022) "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", Journal of Computer Information Systems, Volume 62, 2022 - Issue 1, Pg. 82-97.
11. Mohammed A. Alqahtani (2022) Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis, Computational Intelligence and Neuroscience, Vols. 2007 to 2022; Published online 2022 Mar 18. DoI: 10.1155/2022/6775980.
12. Hicham Nachit and Lhacen Belhcen (2020) Digital Transformation in Times of Covid-19 Pandemic: The Case of Morocco, SRN-Electronic-Journal-1556-5068, Pg.1-10.
13. Jagdish Sambada and Dr. Sanjay Bhayani (2018) International Journal of Management Studies, ISSN(Print) 2249-0302 ISSN (Online)2231-252, Vol.–V, Issue –3(9).
14. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies