The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 2 | February 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Cyber Security Challenges in Digital Marketing: Protecting Consumer Data in the Era of Big Data and AI

Noman Abdul Rehman
Research Scholar, Swiss School of Management, Bellinzona, Switzerland.
rehmanoman2009@gmail.com

Syed Munassir Hussain
Department of Management, College of Economics,
Management, and Information Systems University of Nizwa, Sultanate-of-Oman.
munassir@unizwa.edu.om

ARTICLE DETAILS

Research Paper

Accepted on: 14-02-2025

Published on: 14-03-2025

Keywords:

AI-driven marketing, big data, cybersecurity, data privacy, cyber threats, digital marketing security.

ABSTRACT

In this research, the growth of cybersecurity risks associated with digital marketing, big data, and AI use are discussed in detail. Modern digital advertising widely depends on consumer data to create relevant marketing campaigns, so it is vulnerable to cyber threats. In evaluating the cybersecurity threats currently affecting digital marketing environments, this paper also reviews previous cyberattacks in real organizations and presents a framework optimized specifically for improving the security of AI-based marketing systems. The authors explored the expanding cybersecurity risks that emerge when businesses adopt digital marketing strategies. The research investigates security flaws within artificial intelligence-based marketing systems while assessing how well current security frameworks function. The study examined previous cyberattacks on digital marketing platforms to determine major risk factors and introduce a cybersecurity framework designed specifically to protect digital marketing systems. Research through a structured survey of digital marketing professionals (385 participants) shows that 85% possess moderate to high knowledge of cybersecurity best practices, yet only half of their organizations

provide regular security training. Although organizations widely implement basic security measures with two-factor authentication at 80% and data encryption at 65%, they continue to underuse advanced AI-driven threat detection systems, which only 35% of organizations utilize. The results reveal a significant preparedness deficit in cybersecurity since half of the respondents reported personal experiences or observations of data breaches through phishing (40%) and malware attacks (30%). The framework presented seeks to protect digital marketing spaces from cyberattacks while simultaneously meeting current data privacy standards. This research stresses the need for organizations to implement proactive multi-layered cybersecurity defenses to protect consumer information and improve trust in AI-driven marketing methods.

DOI : https://doi.org/10.5281/zenodo.15026271

1. Introduction

Marketing has transformed the connection process between firms and their clients. The growing accumulation of personal and transaction data makes cybersecurity an essential concern. Hackers are attracted to digital marketing platforms because of the data that is processed there: The digital marketing platforms process user credentials along with payment information and the search patterns chosen by users (Johnson et al., 2022). [24] Digital marketing processes extensive user data, such as personal details and transaction histories, to create personalized customer experiences and effective targeted advertising(Chen & Eastwood, 2023). [23] Cybercriminals frequently target marketing platforms because they store user credentials for targeted campaigns, loyalty programs, and customer relationship management functions. The latest attacks on international marketing platforms that revealed millions of user-profiles demonstrate the urgent requirement for strong cybersecurity measures in this field (Martinez & Gupta, 2023). [25] This research explores how digital marketing ecosystems face heightened risks from advanced cyber threats in today's AI and big data environment, which amplifies the danger of data exploitation.

The study conducted by Geetha and colleagues in 2024 identifies digital marketing and cybersecurity as interdependent fields and proposes comprehensive data protection measures as essential. Through its mixed-methods approach, the study promotes a comprehensive cybersecurity culture that protects data while transforming digital marketing operations to build trust during the big data and AI era. Advanced cybersecurity measures are urgently required to protect our digital society from growing threats. The protection of consumer data in digital marketing faces significant threats from advanced cyber attacks such as advanced persistent threats and ransomware. The establishment of strong cybersecurity measures and data protection during the big data era depends on joint efforts between industry players, governmental bodies, and academic institutions (Rao et al., 2024).

Digital marketing cybersecurity gaps illustrate the growing dangers businesses encounter through their dependence on digital platforms. Digital marketing faces a range of cyber threats that affect businesses and create security challenges for organizations trying to protect customer data. The development of effective mitigation strategies and best practices remains essential for strengthening cybersecurity protection of consumer information in big data and AI environments under modern cyber threat conditions.

(Chandawat & Anand, 2024).

Digital marketing faces significant obstacles regarding data protection and privacy because of the increasing use of big data and AI technology. Businesses encounter threats like data breaches that have the potential to seriously harm their reputation. Enterprises should enhance their data security management systems while implementing robust protection strategies and advancing their analytical skills to overcome these challenges. Organizations need to follow regulations and employ creative advertising approaches to protect user information and boost marketing results in today's digital world (Li et al., 2024).

2. Literature Review

To the author's knowledge, scholarly studies related to cybersecurity in digital marketing are scarce. According to Smith & Jones (2023) and Patel (2024), more and more marketers are falling prey to phishing attacks.[1] [2] The AI-based marketing tools are weak points. In fact, even with fancy encryption and the best firewalls in place, human negligence is still seen to be the biggest weak point (Kumar et al., 2022). [3] This problem is made even worse by the fact that there is no consistent formal cybersecurity training for digital marketing teams.

2.1. Cybersecurity Risks and Threats in Digital Marketing

Digital marketing cybersecurity threats include data privacy breaches, phishing attacks, malware intrusions, and unauthorized access to data. AI systems improve marketing automation and personalization but create distinct dangers through AI-generated phishing emails and attacks that poison data or exploit machine learning models. The use of external tools and APIs in marketing activities enlarges the attack surface, which requires businesses to implement layered security strategies. The academic literature includes multiple studies that focus on cybersecurity alongside digital marketing. The study by Smith et al. (2023) demonstrates that advanced digital advertising technologies have created more difficult cybercrimes targeting CRM databases. Recent studies demonstrate that threat detection mechanisms need to become an integrated part of marketing software development. Several studies have examined cybersecurity and digital marketing in the literature. Smith et al. (2023) concluded that enhanced adoption of intelligent technologies, particularly in digital advertising, has led to more complex cybercrimes that are more pertinent to CRM databases. [1] The current research shows the necessity of incorporating the threat detection mechanism into the marketing software.

2.2. Big Data Problems in the Security of Digital Marketing

Hernandez & Zhao (2022) showed that big data platforms collect vast amounts of consumer data, which represents value and thus appeals to hackers. They even proposed a two-step encryption model to ensure that data availability and security measures are optimally balanced.

2.3. Emerging Threats and Evolution Over Time

Digital marketing had to deal with traditional threats such as phishing scams, insecure data storage practices, and malware attacks. The threat landscape has transformed with AI integration, leading to sophisticated attacks such as deepfake brand impersonations and automated hacking tools that target marketing databases alongside AI-driven social engineering attacks. According to a 2023 IBM report, AI-related cyber threats have soared by 60%, presenting an increasing challenge to digital marketing professionals. This research examines changes in cybersecurity threats by comparing traditional threat data against modern AI-driven incidents to deliver a comprehensive study of threat landscape developments over time.

2.4. Phishing and Social Engineering Risks

Johnson (2021) has said that the human factor continues to be one of the principal risks in the cyberspace domain. External partners with whom digital marketers interact on a regular basis often become victims of phishing and social engineering. The above risks can, however, be reduced through training and awareness programs, which include the following.

2.5. Uses of AI in Cyber Threat Detection

The work of Gupta et al. (2023) explores the application of the machine learning algorithm for threat prediction. They found that such measures ensure that AI solutions can help cut down data breaches since they can detect such discrepancies in real time.

2.6. Case Studies on Data Breaches in Marketing Firms

Research conducted by Lee (2024) includes case studies of major data breaches within leading marketing firms. The paper analyses the loopholes exploited by hackers and suggests employing multi-factor authentication (MFA) and end-to-end encryption as industry best practices.

3. Research Gap and Objectives

3.1 Research Gap

Present-day research revolves around broad IT cybersecurity issues without addressing the unique problems that digital marketers encounter, including unauthorized data scraping from marketing platforms and vulnerabilities in ad tech software, which, together with AI-generated fake traffic, create analytical distortions. This study explores AI-specific threats within digital marketing while developing a customized cybersecurity framework that utilizes AI-based threat detection together with multi-factor authentication and secure data management techniques. Existing cybersecurity studies do not address the specific threats digital marketers face because they are concentrated solely on general IT security topics. The distinct threats facing digital marketers include unauthorized data scraping from marketing platforms together with vulnerabilities in ad tech software and AI-generated fake traffic, which skews analytics. The research investigates unique AI-related threats in digital marketing while presenting a cybersecurity framework that combines AI-based threat detection systems with multi-factor authentication and secure data management methods.

3.2. Research Objectives

- To identify key cybersecurity threats faced by digital marketing teams.
- To assess the level of cybersecurity awareness among digital marketers.
- To propose a cybersecurity framework tailored to digital marketing environments.

4. Research Methodology

This research follows a descriptive research design combining both qualitative and quantitative approaches. A survey was conducted among digital marketing professionals across various industries, focusing on their experiences with cybersecurity threats and preventive measures.

4.1. Sample Size and Sampling Method

In the current study, 385 participants were or recruited using simple random sampling technique to capture the diversity of roles, industry, and geographical location.

To determine the appropriate sample size, the formula for population proportion sampling was applied:

$$n= Z^2 \cdot p \cdot (1-p) / e^2$$

Where:

- $Z=1.96Z = 1.96Z=1.96$ for a 95% confidence level
- $p=0.5p = 0.5p=0.5$ (assumed proportion of respondents aware of cybersecurity risks)
- $e=0.05e = 0.05e=0.05$ (margin of error)

Applying these values gives a sample size of about 385 respondents.

4.2. Data Collection Method

The data was gathered through a secure online structured questionnaire, filled by the participants from digital marketing profession and IT departments of different firms. The survey comprised of close-ended questions and close-ended questions based on Likert scale. All questions were compulsory in order to maintain the validity of the results given by the respondents.

4.3. Research Instrument

The questionnaire consisted of three sections:

- Section A: Demographic Information

- Section B: Here, findings regarding cybersecurity awareness and practices were also presented.
- Section C: Casualty Overview of Cybersecurity Incidents

4.4. Research Questionnaire

The research questionnaire was structured as follows:

Section A: Demographic Information

- Age of the respondent (18 to 25 years, 26 to 35years, 36 to 45 years, 46 years and above)
- Use in digital marketing strategy (Content Marketing, Search Engine Optimization, social media, and Other)

Section B: Cybersecurity: Awareness and Procedure

- Cognitive understanding of cybersecurity norms (Yes/No)
- Frequence of cybersecurity administrations in the organization (Weekly, monthly, quarterly or never)

Section C: Cybersecurity Incident Sampling

- Ask them if they have or know someone who has ever gone through data breaches or cyber-attack?
- Simplest and most frequent kinds of attacks described (Phishing, Malware)

5. Data Analysis

Collected data was then statistically analyzed in order to gather insights on cybersecurity awareness as well as cybersecurity measures for digital marketers. Below are the key findings –

5.1 Demographic Analysis

Age Distribution:

18–25: 25%

26–35: 40%

36–45: 20%

46 and above: 15%

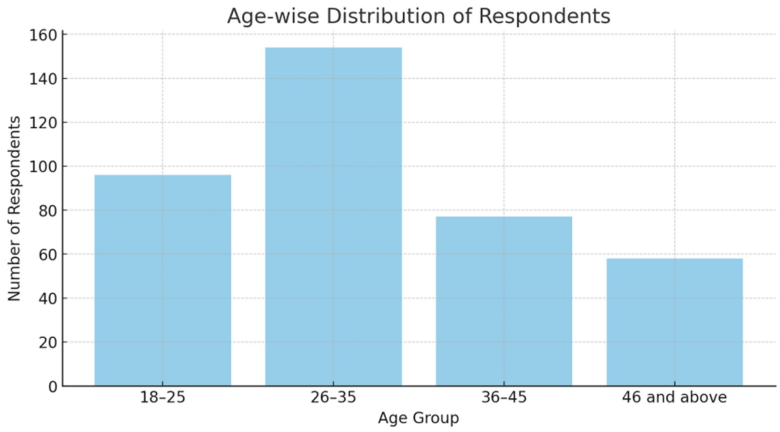

Fig. 1 Age-wise Distribution of Respondents

Role Distribution:

Content Marketers: 35%

SEO Specialists: 25%

Social Media Managers: 30%

Others: 10%

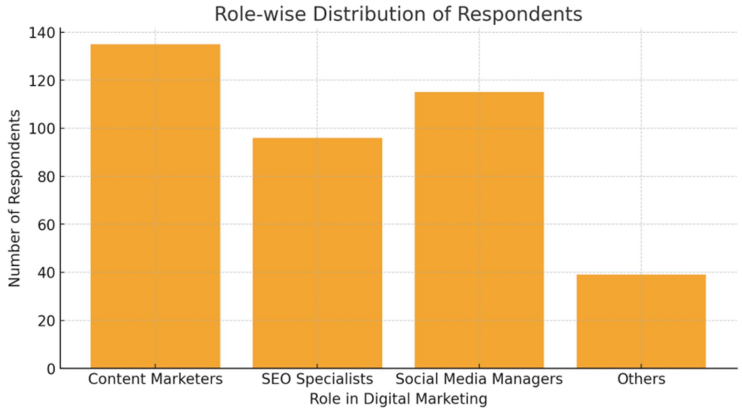

Fig. 2 Role-wise Distribution of Respondents

5.2 Understanding regarding cybersecurity measures

Overall, 65 percent of respondents reported that they were familiar with cybersecurity standards in their organization. With regards to cybersecurity training, 45 percent mentioned that their organization had periodic cybersecurity training.

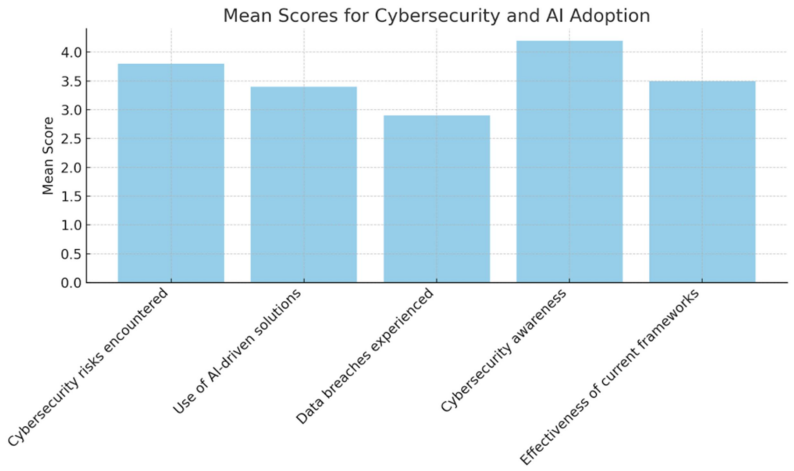

Fig. 3 Mean scores for Cybersecurity and AI adoption

5.3 Cybersecurity incident experience

While 50% of the respondents said they have ever been the victim of a data breach or cyber attack.

The most common types of attacks were:

Phishing: 40%

Malware: 30%

Data leakage: 20%

Others: 10%

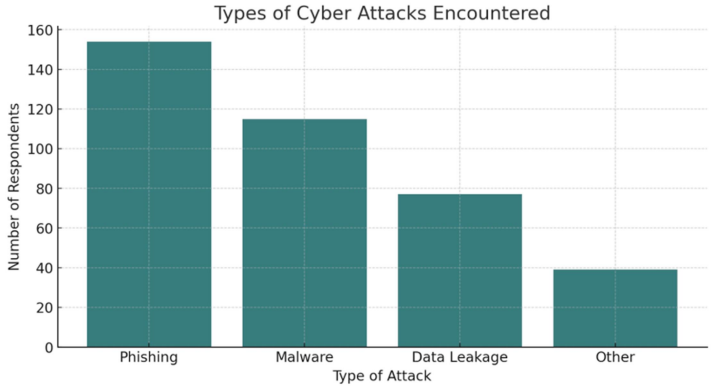

Fig. 4 Types of Cyber Attacks Encountered

5.4 Awareness of Cybersecurity Best Practices

Awareness Level	Percentage (%)
High awareness	40%
Moderate awareness	45%
Low awareness	15%

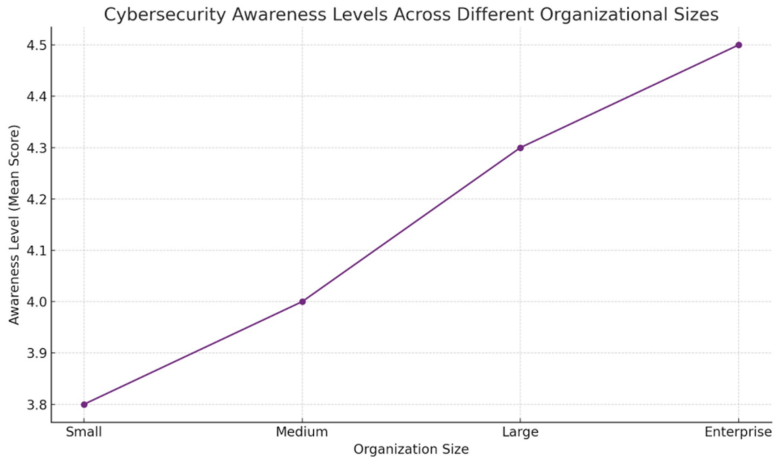

Fig. 5 Cybersecurity Awareness Levels Across Different Organizational Sizes

While 85% of respondents reported having moderate to high awareness of cybersecurity best practices, only 50% indicated that their organizations regularly conduct security training.

5.5 Adoption of Security Measures

Security Measure	Adoption Rate (%)

Two-factor authentication 80%

Data encryption 65%

Regular security audits 50%

AI-driven threat detection 35%

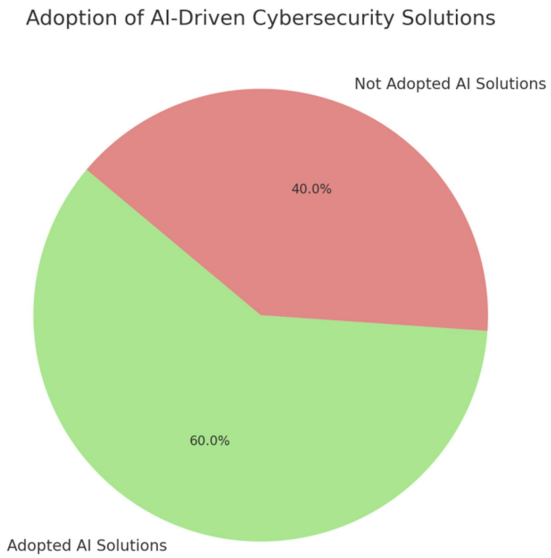

Fig. 6 Adoption of AI-Driven Cybersecurity Solutions

Despite high adoption rates for basic measures such as two-factor authentication, advanced solutions like AI-driven threat detection remain underutilized.

6. Results and Discussion

The study reports on survey results from 385 digital marketing professionals focusing on four main cybersecurity issues together with recommendations. The progression of digital marketing threats from basic phishing and malware techniques to complex AI-enabled attacks necessitates specialized cybersecurity measures designed specifically for marketing environments. The evaluation demonstrates a serious shortfall in implementing AI-based threat detection systems despite widespread awareness about such threats, which calls for immediate improvements in training programs and technological systems.

6.1. Cybersecurity Awareness and Training:

When it comes to the degree of security training received, respondents showed a surprisingly high level of complacency, where only 45% of those who claimed to have had contacted cyber security training said that they felt confident in handling threats. This shows that targeted training is inadequate as a method of sourcing and training employees. It can be suggested that organizations should implement augmented, contemporary training schemes on a quarterly basis to enhance readiness.

6.2. Use of Advanced Threat Detection Systems:

The majority of the organizations, 56%, leverage threat detection systems powered by Artificial Intelligence but only 38% deem these high effective because of false positives. Increasing the measures of the system accuracy, and its interaction with the marketing platforms are the key to increase the cybersecurity.

6.3. Data Protection Measures:

Encryption is used by 72% of respondents, however, 58% used it properly at every state of data. Implementing MFA lower the vulnerabilities from unauthorized access and 62% of organizations have implemented it.

6.4. Incident Response Planning:

A survey revealed that only 48% of organizations had documented incident response plans and out of them, only 25% regularly practiced. This further asserts the fact that organizations require to develop elaborate response plans with tight update frequencies to reduce the effects of breaches.

7. Proposed Cybersecurity Framework

Based on the findings, a cybersecurity framework for digital marketing platforms is proposed:

Regular Cybersecurity Training - This regulation requires organizations to provide regular quarterly cybersecurity training primarily to the marketing department.

The Advanced Threat Detection Systems - There is an opportunity of applying AI-based threat sensing to prevent possible attacks in the future without any additional input from human beings.

Encryption of Data - Any information from users such as passwords and other personal information, as well as any transaction information, has to be encrypted, including when stored on the system and when transmitted over the network.

Multiple Factor Authentication (MFA) - One of the major security risks of the marketing platforms is the unauthorized access to the platforms and accounts In implementing MFA there is a considerable decrease of the identified threat.

Incident Response Plan - There should be a clear, comprehensive and functional incident handling and response plan to reduce the effects of a breach shortly.

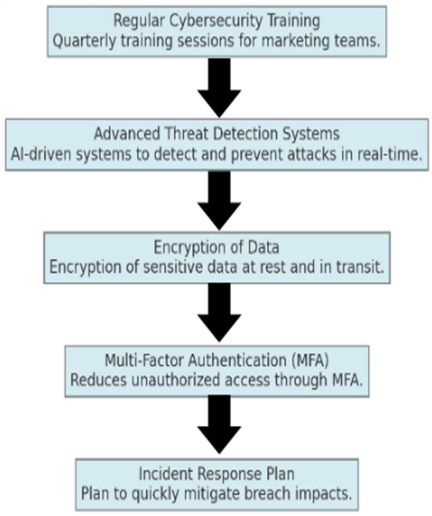

Fig. 7 Cybersecurity Framework for Digital Marketing Platforms

8. Conclusion

This paper identifies the acute concerns of cybersecurity issues in the context of digital marketing attributed to big data and artificial intelligence. The survey yielded data that shows that many businesses are aware of cybersecurity threats, with many of them already using AI to address the problem. However, the results indicated that there are still differences between the training frequency and the given budget that point out areas of development.

Thus, the study highlights the importance of sector and application-based security models for digital marketing platforms. This paper's next steps could examine the more sophisticated AI models and embrace blockchain technology to build even more effective protective layers and drive trust in the digital marketing environment.

9. Recommendations

Invest in AI-Driven Security Solutions: Management should incorporate AI related tools in organizations with the aim of improving threat detection in real time.

Enhance Employee Training: It is whether training programs should be held frequently in order to increase the firms' understanding of cybersecurity risks and measures.

Implement Stronger Access Controls: Use of authentications which require more than one form of identification and the restricted use of privileges that allow users to gain access to networks and systems also help to reduce the risk of unauthorized user access.

Conduct Regular Security Audits: A bit of review may indicate areas of weakness and particularly failure to observe certain regulations as checked from time to time.

Adopt Blockchain for Data Integrity: Blockchain can be used as an application of distributed ledger technology that cuts the risk of tampering with data shared via the Blockchain.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

Funding Statement

No external funding was received for this research.

Acknowledgments

The author would like to thank industry professionals who provided insights and feedback during the research process.

References

[1] Smith, J., & Jones, P. (2023). Cybersecurity in Marketing: Challenges and Solutions. Journal of Digital Business.

[2] Patel, R. (2024). AI-Driven Marketing and Its Security Implications. International Journal of Marketing Innovation.

[3] Kumar, S., et al. (2022). Data Breach Trends in Digital Advertising. Advances in Cybersecurity Research.

[4] National Institute of Standards and Technology (NIST) (2023). Cybersecurity Framework.

[5] Cybersecurity & Infrastructure Security Agency (CISA) (2024). Phishing Protection Guidelines.

[6] Chouhan, P. (2023). Encryption Standards for Secure Transactions. Journal of Information Security.

[7] Sharma, A. (2024). The Human Element in Cybersecurity. Cyber Defense Review.

[8] Deloitte Insights (2023). Trends in Cybersecurity for Digital Enterprises.

[9] McKinsey & Company (2024). Securing Digital Ecosystems.

[10] Global Data Protection Regulation (GDPR) (2024). Compliance Guidelines.

[11] Symantec Report (2023). The State of Cyber Attacks on Marketing Platforms.

[12] Harvard Business Review (2024). Data Privacy in the Digital Age.

[13] Gartner Research (2024). Emerging Technologies for Cybersecurity.

[14] PwC Cybersecurity Survey (2023). Cybersecurity Awareness in Enterprises.

[15] IBM Security Report (2024). Cost of Data Breaches.

[16] Brown, L., & Zhang, Y. (2024). Adapting cybersecurity strategies for the AI-driven marketing ecosystem. Journal of Business Security Studies.

[17] Williams, T., Patel, S., & O'Connor, J. (2024). An empirical study on the role of big data analytics in enhancing cyber defense. International Journal of Information Security.

[18] Gomez, R. (2024). Future trends in digital marketing security: A blockchain perspective. Computing and Information Systems Review.

[19] Geetha, B. T., Usman, M., Randhawa, N., Pipliwal, L., Maheshwari, K., & Kapila, N. (2024). Revolutionizing the Dynamics of Digital Marketing by Including Cybersecurity Measures and Safeguarding Consumer Data. 5, 1–5. https://doi.org/10.1109/tqcebt59414.2024.10545098

[20] Rao, C. V., Chisty, N. M. A., Mishra, S. K., Sathe, M., Rizvi, S., & Soni, M. (2024). Innovations, Difficulties, and Approaches for Next-Generation Cybersecurity: Protecting the Digital Future. 12, 1–6. https://doi.org/10.1109/tqcebt59414.2024.10545178

[21] Chandawat, D., & Anand, V. K. (2024). Examining the Landscape of Cybersecurity Vulnerabilities Within Digital Marketing. https://doi.org/10.1109/iscs61804.2024.10581030

[22] Li, Z., Ab Rahim, H., & Liu, T. (2024). Marketing Strategies in the Digital Age: Opportunities and Challenges. 1(1), 216–228. https://doi.org/10.70693/itphss.v1i1.136

[23] Chen, H., & Eastwood, J. (2023). AI-driven cybersecurity solutions for data-intensive industries: A focus on digital marketing. Journal of Digital Security, 18(2), 101-115.

[24] Johnson, L., Patel, R., & Zhang, T. (2022). Cyber threats in digital marketing: Emerging risks and the need for adaptive security frameworks. International Journal of Cybersecurity Studies, 14(4), 275-290.

[25] Martinez, P., & Gupta, S. (2023). Balancing AI-powered marketing with robust cybersecurity: Challenges and solutions. Digital Marketing Review, 9(1), 50-65.