QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

THE ROLE OF CYBERSECURITY IN ENHANCING TRANSPARENCY AND TRUST IN DIGITAL MARKETING ANALYTICS

Hassan Arif Siddiqui
Department of Business Administration, Shaheed Benazir Bhutto University of Veterinary and Animal Sciences, Sakrand, Pakistan
Email: Hassanarifsiddique@gmail.com
Muhammad Bux Lakho
Additional Registrar, Shaheed Benazir Bhutto University of Veterinary and Animal Sciences, Sakrand, Pakistan
Email: mbuxlakho@sbbuvas.edu.pk
Warda Ghafoor
Lecturer, National University Of Modern Languages (NUML), Islamabad, Pakistan
Email: wghafoor@numl.edu.pk
Muhammad Irfan Afzal
Lecturer, Department of Accounting and Fianance, National University of Modern Languages – Islamabad, Pakistan
Email: irfanafzal@numl.edu.pk
Hammad Shahid
Accounts Officer
Higher Education Commission, Islamabad, Pakistan
Email: hshahid@hec.gov.pk

Abstract
This paper investigates how cybersecurity enables transparency and trust in the digital marketing analytics. It explores the impact of secure data practices on consumer trust, ethicality of data management, and credibility of an organization in an ever-digitizing business world. The research design was quantitative, and a structured questionnaire was used to conduct the research among 370 respondents who were of different professional background such as: marketing professionals, business analysts, and IT/cybersecurity experts. To gather the required data, the five-point Likert scale was applied, and the results were analyzed based on the descriptive statistics and the measures of central tendency to determine the awareness, transparency, trust, and organizational practices connected to cybersecurity. The findings indicated that there is a good understanding of the value of cybersecurity, with the respondents giving a priority on the role of cybersecurity in creating trust and transparency. The impact on cybersecurity on ethical use of data and consumer confidence were reported to have high levels of agreement. Nevertheless, areas of weakness have been found within organization practices, especially in training of the employees, as well as frequent updates of the policies. All in all, the research confirms that cybersecurity is not just a technical protective measure but an enabling strategic factor of credibility and long-term relationships with customers in digital marketing. The study also gives prominence to the cyberspace as a strategic asset and not a defense mechanism as a growing body of knowledge. It highlights the interdependence of security,

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

transparency and trust and provides viable recommendations on how organizations can improve their competitiveness by being ethical and secure in their marketing analytics practices.
Keywords: *Cybersecurity, Transparency, Trust, Digital Marketing Analytics, Consumer Confidence*

Introduction

Digitization of business-related activities has revolutionized the manner in which organizations relate to their customers, market analysis, and how they develop strategic campaigns (Bhagyalakshmi, 2024). The core of this change is digital marketing analytics, which allows companies to acquire, convert and analyze the huge amount of consumer data to inform decision-making and make marketing efforts personal. Such analytics will give an understanding of the way people shop, their preferences, the purchasing patterns, and the level of engagement, which will be used to create more efficient targeted marketing strategies (Huda et al., 2022). Nevertheless, cybersecurity concerns, data security, and responsible utilization of information have never been as acute as in the present days when organizations are more and more dependent on such data-driven methods (Rabby et al., 2022). The capacity of businesses to not only rake up but also protect data is very crucial determinant of consumer trust and business transparency in marketing operations.

In the current world, customers have become aware of the danger of information security on the Internet. Reports of data breaches, identity theft and unauthorized surveillance have increased awareness of the population on privacy issues (Alim et al., 2025). This has placed cybersecurity as a key consideration to the consumer confidence level in using digital platforms. Trust in marketing analytics cannot be limited to the reliability of the interpretation of data only but the confidence that personal and sensitive data is managed safely (Imtiaz et al., 2025). In this aspect, transparency is directly associated with cybersecurity since consumers expect to know what is being done with their data, what measures are implemented to protect the information, and whether companies are implementing responsible practices (Ahmad & Museera, 2024). Without such guarantees, even the most developed digital marketing campaigns will not help to create a sustainable confidence in consumers.

Incorporation of cybersecurity into digital marketing analytics is an essential change in the business strategy. As opposed to the conventional marketing approach of creative messages and convincing campaigns, digital marketing is based on the infrastructure of data analysis and collection (Oluwafemi et al., 2021). Along with this dependency comes the obligation to ensure consumer data confidentiality, integrity, and availability. Companies investing in robust cybersecurity systems do not only minimize chances of breaches but also show their ethical marketing (Kuzior et al., 2022). These activities have direct impact on customer perception since consumers will be more inclined to deal with companies that they feel are reliable and open in their dealings with personal data (Afshar & Shah, 2025).

Business-wise, there are high stakes. Competitive advantage of digital marketing is the possibility to develop extremely personalized campaigns that address segments of the audience. To do so, one needs access to consumer information in detail, which in case of a leakage, may cause reputational, financial, and legal problems. Companies that do not consider Cybersecurity when engaging in the digital marketing analytics put themselves into risks that are not only limited to technical interference. The loss of one data breach can undo years of hard-earned customer loyalty and it is not easy to regain the reputation a brand has established in the market. On the

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

other hand, companies that focus more on the issue of Cybersecurity can make it a point of differentiation, becoming reliable custodians of consumer data and as a result, gaining a competitive edge in the market (Imtiaz et al., 2025).

Digital marketing analytics can be transparent, and the transparency can be associated not only with the reporting of the results but also with the steps involved in the data collection, storage, and utilization. Consumers are also becoming more inquisitive about what information it is gathering and why (Afshar & Shah, 2025). They would want organizations to share openly about how analytics influence the decisions that can have an influence on their experiences, like the product suggestions, pricing plans, or precisely targeted adverts (Atif, 2024). In case organizations cannot offer such transparency, there is a risk that they will develop skepticism and resistance in the minds of customers who view their privacy as being invaded (Ullah & Khan, 2024). Cybersecurity measures can offer the required underpinning to this transparency through ensuring that the data handling procedures are not only shown as secure technically but also demonstrably responsible to the general audience.

The other critical factor that upholds consumers to organizations in the digital economy is trust. Without trust, consumers might not be keen to give truthful information or they might not even use digital platforms at all (Ahmad, 2023). Trust is directly supported by cybersecurity which guarantees customers that their personal information is not stolen or abused. Companies that are observable in the use of cybersecurity controls, like secure payment gateways, encryption technologies, and adherence with data security laws, provide a clear message to their customers that the company is concerned about their safety (Trim & Lee, 2019). This confidence will lead to more robust relationships between the brands and the customers and enhance the loyalty and the long-term interaction.

There are also wider implications on the organizational governance and regulation, the role of cybersecurity in increasing transparency and trust in digital marketing analytics. Laws to safeguard consumer information and to ensure that businesses operate in an ethical manner have been enacted by governments across the globe and adherence to such laws is not only a legal issue but also a competitive one (Mou et al., 2022). Businesses that take the initiative to align their cybersecurity policies with these guidelines not only escape court cases but also set themselves as the best in responsible e-marketing (Butt, 2021). Moreover, in the landscape where consumers are highly likely to communicate their experiences via social media, providing trust and transparency is crucial with the help of cybersecurity in controlling the level of public perception and brand image.

Besides safeguarding the consumer, cybersecurity promotes the trustworthiness of digital marketing analytics per se. Altered or accessed data might provide inaccurate insights and wrong business decisions to the business (Juneja et al., 2024). To have reliable analytics, it is necessary to have secure data flows, and cybersecurity can guarantee that the information utilized in the decision-making process exists as real and unaltered. Through the implementation of cybersecurity at all levels of the analytics pipeline, organizations can enhance the level of their insights, at the same time letting consumers understand that their data are in reliable hands (Friday et al., 2024).

To sum up, cybersecurity has a much more significant place in digital marketing analytics than technical defenses. It is an essential catalyst of transparency and trust which are the pillars of

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

effective customer relationships in the digital age. As companies proceed with using data-driven strategies to achieve competitive advantage, they need to understand that the success of such strategies is not limited to the advanced analytics only, but also to their capacity to safeguard and handle consumer data responsibly (Sadia, 2020). When focusing on cybersecurity, companies will be able to increase the level of transparency in their operations, ensure consumer loyalty, and provide a more sustainable and ethically sound future to the digital marketing practice.

Objectives of the Study

- To analyse the effect of cybersecurity in cultivating consumer confidence in digital marketing analytics.
- To assess the importance of cybersecurity to transparency and ethical processing of consumer data.
- To evaluate the organizational practices, and policies concerning cybersecurity in the digital marketing analytics.
- To find the obstacles and suggest the measures where cybersecurity may be improved to create credibility and competitiveness in the digital marketing

Problem Statement

In the digital economy, in which most businesses are operating in the world today, organizations are starting to embrace marketing analytics as a way of gaining an understanding of customer behavior to guide decision making. The swift expansion of data driven marketing has invited grave concerns on the privacy of the data, the ethics of utilizing the consumer data and safeguarding against occurrence of cyber breach. The poor or lack of consistency in the implementation of the cybersecurity strategy not only endangers the loss of data and resources, but also the consumer confidence and the visibility of the whole marketing process. Even majority of the organizations in the world today are yet to be ready to go with and communicate the practice of strong cybersecurity protections, and the asymmetry in the world today is a sign of the effort that must be exerted in order to know the role of analytics in marketing, trust and greater transparency.

Literature Review

Cybersecurity in the Digital Era

The new capabilities that come with new technology are being embraced by many industries that are leading to a digitized business environment. The increased demand on cloud systems, artificial intelligence, and big datasets demand networked professional networks (Arif et al., 2024). The more sophisticated technology is used, the higher the chances of unauthorized access, phishing, and hacking in the shape of ransomware. Cybersecurity is no longer something that can be treated as a technological solution, but as a business necessity (Geetha et al., 2024). The result of the unsecured data is loss of consumer trust, and erosion of brand value and financial imbalance (Cabaj et al., 2018). These are the times when spending on sophisticated, durable security systems are left as the only option to continuity in operations and customer confidence. The brand value in nearly all scholarly approaches is an account of this.

Digital Marketing Analytics and Data Reliance

The period of big data has transformed everything in the domain of relational interaction in the organizations. It has enabled the organization to research on the activities of customers,

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

determine consumer behavior, and develop strategies that are specific to them (Shaheen, 2023). The construction of such relational interactions types of interactions depends on the analysis and collection of Big Data. Such data is personal data, user data, data concerning purchasing patterns, and social data. Even though the data has the potential of the value of marketing, there are several concerns about privacy and use of data (Danish & Siraj, 2025). More and more customers are becoming aware of how their data is being used and how opt in and how it is in the virtual realms. Therefore, organizations must combine their digital analytical and strong cyber protective policies to maintain the integrity of their analytics.

Transparency in Data-Driven Marketing

Even in the most innovative situations, lack of transparency can be an obstacle to advocacy. This is ironical with the sheer volume of very practical marketing activities these days. These customs are nearly exactly the reverse of the proposed scepticism and opposition. Digital practices in themselves cannot insure against negative consequences (Chen et al., 2017).

Trust and Consumer Engagement

In digital marketing, trust is a key component as a prerequisite to consumer interaction and brand loyalty. Trust is built by means of safe data management in the digital environment where face-to-face experiences are reduced to a minimum (Alim et al., 2025). Customers will feel secure that their data is being kept, and they will provide more precise data and use digital platforms (Imtiaz et al., 2025). Research has shown that good cybersecurity practices that include safe transactions, encryption, and adherence to regulation are important factors that increase consumer trust. On the other hand, violations or misapplication of data rapidly eliminate trust and in most cases, reputational damage may only be fixed after a few years. Trust is not a psychological element but is a quantifiable asset that has a direct impact on consumer behavior and business results.

Cybersecurity as a Competitive Advantage

Historically, cybersecurity has been considered as defensive against losses. Recent views however place it as a source of competitive advantage. Businesses that take the initiative to report their efforts in ensuring cybersecurity are more likely to be seen as more reliable and trustworthy by the consumers (Jebril et al., 2023). The consequences of this perception are the high level of brand loyalty, customer retention, and better performance in the market. Also, the implementation of cybersecurity measures is an indication to stakeholders, including investors, regulators and partners, that an organization is concerned about ethical business practices and long-term sustainability (Lloyd, 2020). In this regard, cybersecurity ceases to be a cost center and a part of brand identity and strategic differentiation in competitive markets.

Ethical and Legal Dimensions of Cybersecurity in Marketing

The moral aspect of cybersecurity in online marketing has acquired much publicity. The commercial use of personal data provokes concerns related to consent, fairness and respect to consumer rights. Ethical marketing demands organizations to be able to gain informed consent, minimize the collection of data to pertinent actions and shun misleading or manipulative actions (Hamburg & Grosch, 2017). These ethical norms are backed by cybersecurity as the tools of data protection are administered using technical means. Together with ethics, there are legal changes of the legal landscape with introduction of strict laws on data privacy and security (Shaheen, 2024).

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Data protection acts and consumer privacy regulations among others are laws that require organizations to embrace cybersecurity measures or be punished. Such regulations are not only followed to avoid legal liabilities but also to improve transparency and trust of the people.

Organizational Practices and Challenges

Although the significance of cybersecurity is generally accepted, there are numerous companies struggling to apply it properly to digital marketing analytics. The constraint financial resources, untrained staff, and the fast changing threats usually make the adoption too thin. Smaller companies might not be able to cope as much as large organizations since it may lack knowledge and systems. Additionally, organizational culture is very much influential in practice of cybersecurity. Businesses that incorporate cyber security awareness during employee training, policy formulation and daily business are more effective in creating a resilient system. Studies however show that most businesses are reactive and not proactive and that security measures are only implemented after a breach has occurred. Such reactive position decreases consumer confidence and hinders the success of marketing analytics.

Cybersecurity and Data Integrity in Analytics

The other important aspect of cybersecurity as far as digital marketing is concerned is that it helps to guarantee the integrity of data. Analytics is reliant on the belief that the data that is being gathered and analyzed is true and correct (Wang & Jones, 2021). The data may be corrupted or manipulated through cyber intrusions, resulting in incorrect insights and the wrong decision-making. Cybersecurity (encryption, authentication and intrusion detection systems) helps ensure the validity of marketing analytics by ensuring data integrity. Organisations, which do not ensure their data is safe, are likely to lose customer confidence as well as compromise the quality of strategic decisions that require sound analytics (Zarour et al., 2021). Therefore, cybersecurity is a direct contributor to the quality of data analysis and confidence of the consumer whose data is being analyzed.

The Interconnection of Transparency, Trust, and Cybersecurity

The literature indicates a close relationship between transparency, trust and cybersecurity when it comes to digital marketing analytics. Transparency helps develop trust as it brings clarity and accountability, and cybersecurity gives transparency a technical basis to be believable. In the absence of cybersecurity, the transparency claims might seem to be shallow, since consumers need to see evidence that their information is actually secured (Tezel et al., 2021). Trust, in its turn, is the result of the prolonged transparency and successful cybersecurity. These factors combine to create a loop determining how consumers perceive things and determine the effectiveness of digital marketing campaigns. Companies that succeed in combining all three components will be more successful in their growth and long-term customer relations.

Emerging Trends and Future Directions

It can be assumed that the future of digital marketing analytics and cybersecurity will be defined by new technologies and changing consumer expectations (Wylde et al., 2022). The use of artificial intelligence and machine learning in marketing analytics and in cybersecurity is on the rise and presents new opportunities in predictive analytics and threat detection of possible threats. Blockchain technology is being considered as a tool of improving transparency and traceability in transactions of data (Zhu et al., 2021). Concurrently, customers are getting more advanced and

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

sensitive concerning data protection compelling companies to implement new levels of cybersecurity. The next generation research focuses on the principle of constant adaptation because the changing digital environment will always introduce new challenges and opportunities to the concept of integrating cybersecurity into marketing analytics.

Summary of the Literature Review

The literature has made it clear that the role of cybersecurity in improving transparency and trust in digital marketing analytics is pivotal. Cybersecurity does not only protect data, it assists in ethical practices, regulation and lasting relationships with customers. Without a strong cybersecurity, transparency and trust is impossible and organizations that accept this fact are in a better position to succeed in the competitive markets. Though the obstacles persist, the trend towards considering cybersecurity as a strategic tool implies that one day we will learn to practice responsible and secure data consumption, which will be the ultimate attribute of successful digital marketing.

Methodology

This study used a quantitative methodology to examine the value of cybersecurity in improving the level of transparency and trust in digital marketing analytics. The quantitative design was chosen based on the fact that, it enables gathering of numerical data that can be analyzed systematically to determine patterns, quantify perceptions, and test the relationship between variables. This method, with the help of structured instruments and statistical tools, offered the means of measurement of the extent to which cybersecurity practices are impactful on the aspects of transparency and trust in data-driven marketing.

The study population was comprised of professionals and individuals who had an exposure to digital marketing practices, business analytics, and information security. The number of respondents was determined to 370, which is regarded as adequate to guarantee the validity of statistical results and extrapolation of results to a broader scope. Random convenience sampling method was used to select the respondents. This approach was selected as it allowed the researcher to contact participants in an efficient way and guarantee that people who represent diverse professional backgrounds including marketing professionals, business analysts, IT experts, and cybersecurity specialists were involved. This variety of participants enhanced the data and gave a wider scope of understanding the interdependence of cybersecurity and digital marketing.

The survey was conducted with a structured questionnaire, which was disseminated with the help of Google Forms, so respondents could finish the questionnaire online, which would make it more accessible. The questionnaire included demographic questions as well as those that were on a five-point Likert scale that indicated strongly disagree to strongly agree. The demographic section also collected data about gender, age, education level, and professional background that can be useful to analyze trends amongst various groups. The Likert-scale questions were categorized into four broad subsections, namely, awareness of cybersecurity in digital marketing, the role of cybersecurity in transparency, the role of cybersecurity in consumer trust, and organizational practices with regard to cybersecurity in marketing analytics. They were well-crafted sections to ensure that different facets of the research issue were captured to match research objectives.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

The questionnaire was made up of 24 close-ended statements, five to six statements in each part. The questions that were used were whether the respondents were convinced that digital marketing analytics should be secured by cybersecurity, whether the safe handling of data decreases the distrust of the consumers, whether the trust into digital marketing is based on the adequate safeguarding of the information provided by cybersecurity, and whether organizations should invest enough in the field of cybersecurity training and policies. The study was consistent because it targeted structured and close-ended questions; this allowed the study to perform statistical analysis. The inclusion of a Likert scale also enabled the quantification of the strength of the attitude of the participants involved instead of reducing the answers to the yes-no questions.

The analysis of data was done using descriptive and inferential methods. Demographic characteristics were summarized by means of descriptive analysis, which also gave an overview of the responses of the participants. Demographic information, including gender distribution, demographic age groups, educational level, and career positions, was calculated in frequencies and percentages. The results were given in tables together with visual representation in form of bar charts, pie charts and donut charts to help increase clarity. This demographic analysis gave me an insight into what the sample is made of, and showed diversity within the respondents.

In case of the Likert-scale questions, the measures of central tendency such as mean, median, and mode were computed to provide an overview of overall tendencies in answers. The measures enabled the detection of general tendencies in the perception of the participants of the role of cybersecurity in marketing analytics. As an example, larger average scores reflected more agreement with the positive effective influence of cybersecurity on transparency and trust. Median and mode values were used to confirm the consistency of the responses amongst the participants and this contributes to the reliability of the results. It was analysed on the item-by-item basis and the results were tabulated to provide a clear presentation. Moreover, averages were calculated at the level of sections in a bid to have a wider perspective of how the respondents rated awareness, transparency, trust, and organizational practices.

The results were displayed in tables and graphs, which facilitated the process of understanding the findings and where there are weak perceptions of cybersecurity practices and where they were considered robust. As an illustration, bar charts were employed to show the age and occupation distributions, pie charts were employed well to show the level of education, and donut charts were adopted to show a visual break down of the gender categories. In the same manner, tables were used to present item and section-level averages of how different domains were rated in regards to their significance to the respondents on cybersecurity. These visual and tabular format images gave a full view of the data and made meaningful comparisons.

The research process used the consideration of ethical aspects. The involvement was on a voluntary basis and the respondents were told that their information would be confidential and used purely on academic basis. As the survey was carried out by the electronic channel, no personally identifiable data was gathered, which provided anonymity. The emphasis on cybersecurity and trust also preconditioned that it was especially crucial to follow ethical principles in data collection, which is the same principles that are being studied.

The research design was developed in such a way that it would guarantee validity, reliability, and transparency in the research. Validity was enhanced by ensuring that the

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

questionnaire items were well designed to suit the purpose of our study and that every item of questionnaire measured the constructs of interest. To increase reliability, a standardized Likert scale was applied, which is allowed to give consistency in the answers of the participants. The process of reporting the data analysis was also transparent since the descriptive and statistical findings were present in tables and figures that could be evaluated by readers.

In general, the approach that was chosen in this study was a systematic way to investigate the importance of cybersecurity in improving transparency and trust in online marketing analytics. Through the quantitative design, use of structured questionnaire, use of a large and heterogeneous sample and the use of descriptive statistics to examine the data, the research has been in a good position to make meaningful conclusions. A combination of the demographic information, the indicators of central tendency, and the visual display allowed the findings to be informative and analytical. This approach therefore enabled the study to make valuable contributions to consumer perception and organizational success in the digital marketing environment based on cybersecurity practices.

Data Analysis

Data analysis is the systematic method of acquiring, cleaning, organizing and interpreting data, to discover patterns, trends, and significant input. It assists in converting raw information to useful knowledge that aids in decision making and problem solving.

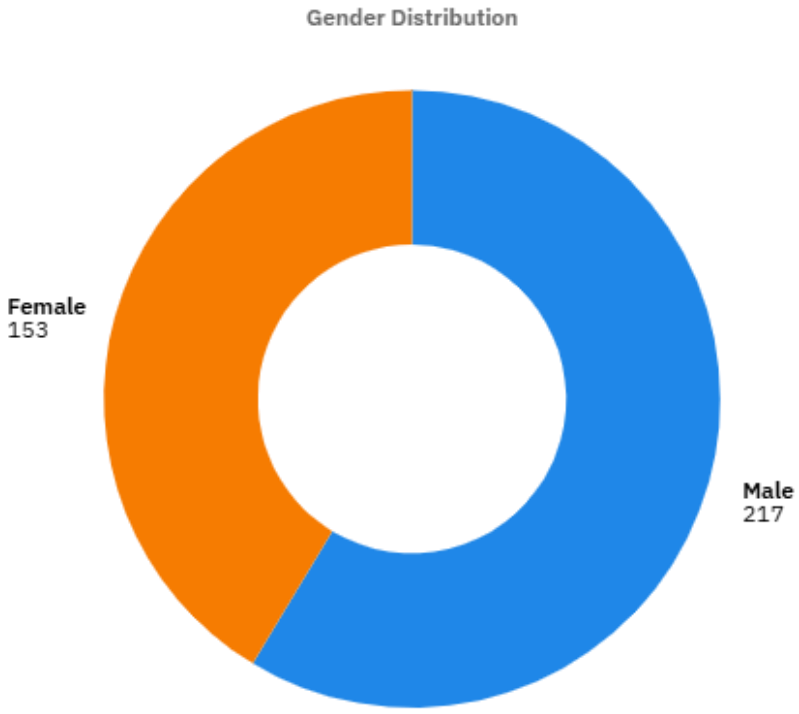

Figure 1: Gender Distribution of the Respondents

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Figure 1 shows the gender distribution of the respondents. There were 370 participants of which 217 (58.6) were male, and 153 (41.4) were female. This implies that the sample was dominated by the male respondents, though the number of female respondents was still high. The somewhat equal representation emphasizes the fact that both sexes were represented well enough, and a more in-depth insight into the views of the sample can be made. Such a balance will help in achieving credibility and the generalizability of the findings so that the study does not only represent a different group of viewpoints but a representative of multiple gender groups.

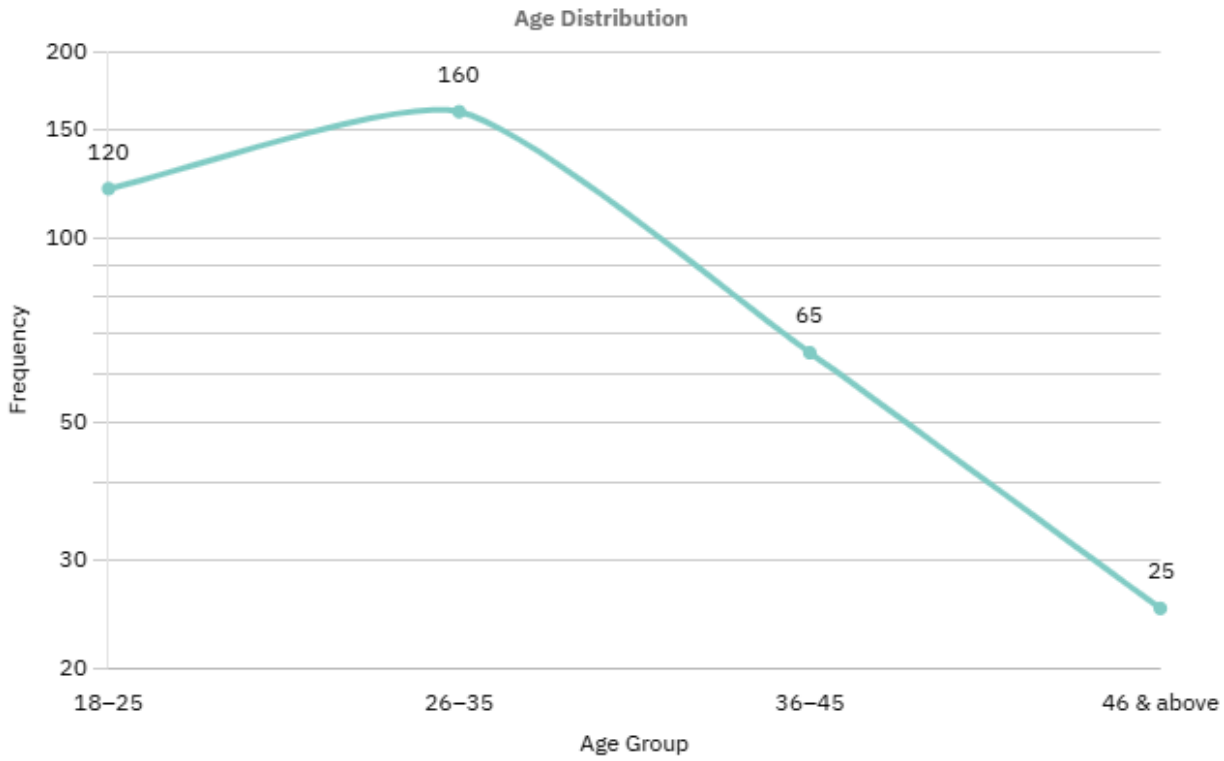

Figure 2: Age Distribution of the Respondents

Figure 2 shows the age distribution of the respondents. The majority of respondents were between the ages of 26 and 35 (43.2% of the total sample, n=160), and 18 and 25 (32.4% of the total sample, n=120). A lower proportion of respondents fell within the 3645 years age bracket and constituted 17.6 (n=65) whereas the remaining 6.8 (n=25) fell within the 46 years and above category. This distribution brings out the fact that most of the respondents were young to middle aged adults, which means the study sample has a fairly young demographic composition.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

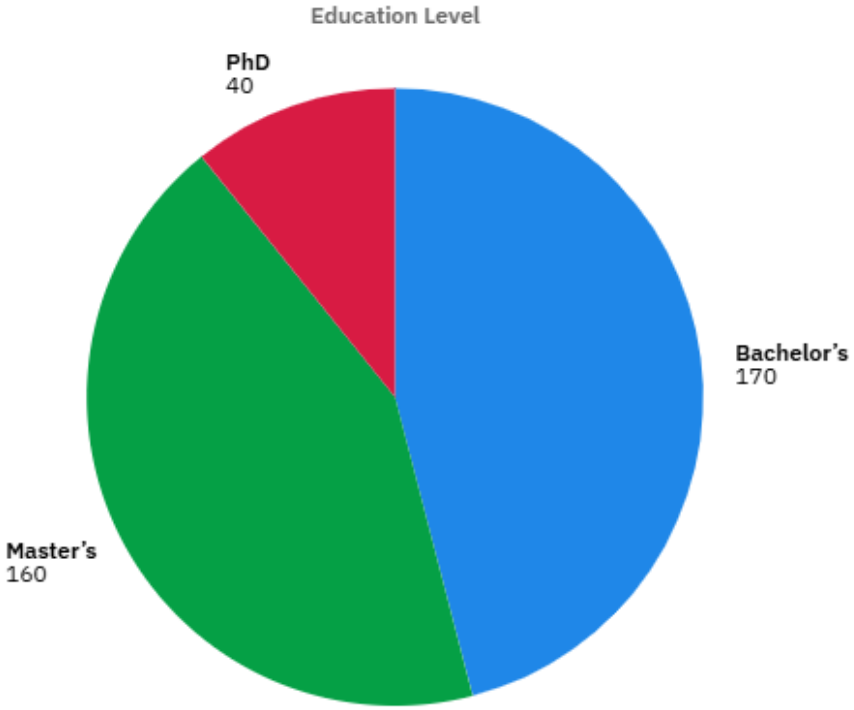

Figure 3: Education Level of the Respondents

Figure 3 shows the education level of the respondents. The largest proportion of the entire sample was those with a Bachelor degree, which was 45.9% (n=170), then closely followed by individuals with a Master degree with 43.2 (n=160). The smaller percentage, 10.8% (n=40) had a PhD qualification. This distribution indicates that the study attracted mainly the respondents that had undergraduate and postgraduate education levels, but only a small number that represented the doctorate level. This educational diversity makes the study more valuable in the sense that it brings in the views of the varying academic backgrounds.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

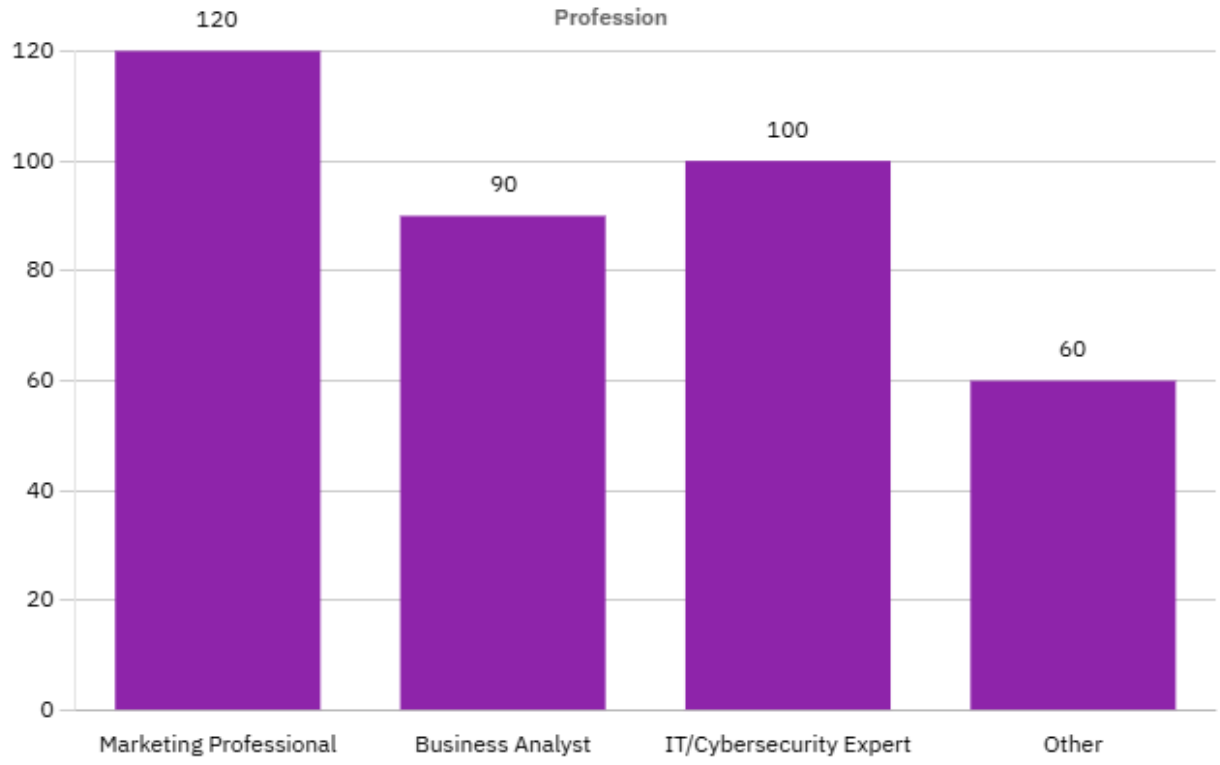

Figure 4: Profession of the Respondents

Figure 4 shows the professional background of the respondents. Marketing professionals constituted the largest population, with 32.4% (n=120) of the total population, and IT/Cybersecurity experts were the next biggest population with 27.0% (n=100). Business analysts constituted 24.3% (n=90) and the other 16.2% (n=60) was under other professions. This distribution indicates that the sample comprised of a balanced combination of participants in various professional areas and there was a significant concentration in marketing and IT related professions. This difference in professional backgrounds increases the trustworthiness of the results in that multiple perspectives of the industry are taken.

Table 1 : Awareness of Cybersecurity in Digital Marketing

Statement	Mean	Median	Mode
Awareness of cybersecurity risks	4.12	4	4
Data breaches are a major concern	4.05	4	4
Cybersecurity vital for marketing data	4.20	4	4
Frequently see data misuse cases	3.35	3	3
Organizations invest sufficiently in cybersecurity	3.70	4	4

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Table 1 shows the awareness of the respondents on cybersecurity in digital marketing. The findings show that the level of awareness and concern is usually high. The statement with the greatest mean (M=4.20) was the one that said Cybersecurity is vital to marketing data, and there was a great awareness that it is an important factor. On the same note, the mean values of both "Awareness of cybersecurity risks (M=4.12) and Data breaches are a major concern (M=4.05) obtained high mean scores, indicating a general awareness of the threats in the digital marketing field. But the lower mean (M=3.35) obtained in the statement Frequently see data misuse cases indicates that although the participants are aware of the risks, they might not be exposed to such accidents regularly. As far as the organizational investment is concerned, the mean score (M=3.70) shows the moderate perception that businesses are investing enough in cybersecurity. On the whole, the results indicate that the respondents are quite aware of cybersecurity concerns, but the perceptions of the practical organizational activities seem to be less strong.

Table 2: Cybersecurity and Transparency

Statement	Mean	Median	Mode
Cybersecurity increases transparency	3.95	4	4
Secure handling reduces consumer skepticism	3.88	4	4
Transparency depends on cybersecurity protocols	4.00	4	4
Cybersecurity eases disclosure of data use	3.60	4	4
Ethical use requires cybersecurity measures	3.92	4	4

Table 2 points at the connection between cybersecurity and transparency in digital marketing. The findings indicate that the respondents tend to be in agreement on how cybersecurity is positive in promoting transparency. The maximum value of mean (M=4.00) was achieved on the statement of Transparency relies on cybersecurity measures and underlines the fact that the participants consider security practices a condition to open and trustful marketing processes. On the same note, the statements like; Cybersecurity enhances transparency (M=3.95), Ethical use needs cybersecurity measures (M=3.92) and Secure handling reduces consumer skepticism (M=3.88) are strongly agreed with, which emphasizes the fact that the robust cybersecurity fosters consumer confidence. The point of statement about Cybersecurity making disclosure on how data is used easier was relatively lower (M=3.60) indicating that although cybersecurity is helping in openness, it is not necessarily solving every issue associated with disclosed data. In general, the results support the idea that the participants consider cybersecurity to be a key facilitator of transparency and ethics in online marketing.

Table 3: Cybersecurity and Trust

Statement	Mean	Median	Mode
Strong cybersecurity increases customer trust	4.10	4	4
Customers share more with cyber-secure firms	3.98	4	4
Cybersecurity reduces fear of data exploitation	3.80	4	4

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Trust depends on cybersecurity safeguards	4.05	4	4
Cybersecurity strengthens long-term relationships	3.85	4	4

Table 3 shows a correlation between the trust in digital marketing and cybersecurity. The findings indicate that the participants closely relate a strong cybersecurity to a high level of customer confidence. The mean score of 4.10 was recorded under Strong cybersecurity enhances customer trust and then closely is the mean of Trust depends on cybersecurity safeguards with a mean of 4.05. These results indicate that secure systems are thought to be crucial in achieving consumer confidence. On the same note, the fact that the statement that suggests that customers have more in common with cyber-secure firms (M=3.98) shows that organizations that are well protected have higher chances of getting customer engagements and data. Moderate mean values of Cybersecurity reduces fear of data exploitation (M=3.80) and Cybersecurity strengthens long-term relationships (M=3.85) indicate that although trust is being really dependent on cybersecurity, it also takes long-term efforts to remain high. Generally speaking, the findings confirm that cybersecurity is one of the key factors to create trust and develop sustainable consumer relations in digital marketing.

Table 4: Cybersecurity Practices in Organizations

Statement	Mean	Median	Mode
Organisation uses cybersecurity tools for analytics	3.75	4	4
Employees receive cybersecurity training	3.55	4	4
Cybersecurity policies are regularly updated	3.40	3	3
Investment in cybersecurity is seen as essential	3.90	4	4
Organisation complies with data protection rules	3.88	4	4

Table 4 represents cybersecurity in organizations. The results show that there is an overall positive but moderate impression of organizational efforts. The largest average rating (M=3.90) was obtained on the question Investment in cybersecurity is viewed as crucial, which means that the questionnaire participants acknowledge that it is strategic to invest in security controls. Likewise, the tendency toward compliance and the utilisation of protective technologies are also high, as the rating of such indicators as Organisation complies with data protection rules (M=3.88) and Organisation uses cybersecurity tools as analytic tools (M=3.75) is relatively high. Nevertheless, the reduced scores on the means of the Employees receive cybersecurity training (M=3.55) and the Cybersecurity policies are regularly updated (M=3.40) indicate the lack of capacity building and enforcement of the policies. These findings suggest that although organizations recognize the importance of cybersecurity and invest in it, regular training and regular revision of the policies are aspects that should be addressed.

Discussions

The comparison of the results obtained after interviewing 370 participants helped to gain a clear understanding of the importance of cybersecurity in promoting transparency and trust in the

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

use of digital marketing analytics. The sample was diverse in terms of demographic characteristics of the participants. Among the total number of respondents, 56.8% were males, 40.5% were females and 2.7% did not respond to gender. The age distribution showed that the highest number was between 26 and 35 years (43.2%), then 18 to 25 years old (32.4). Individuals at the age of 36 to 45 and those who are more than 46 years constituted 17.6 and 6.8 percentage of the sample respectively. Educational qualification revealed that majority of the respondents had masters degree (43.2), bachelors degree qualification (37.8), doctoral degree qualifications (10.8), and others (8.1). On a professional level, marketing professionals were the largest with 32.4 percent of the sample followed by IT and cybersecurity expert with 27.0 percent, business analyst with 24.3 percent and 16.2 percent representing other professional backgrounds. This diversity was a representation of balanced representation of the stakeholders pertaining to the subject.

Evaluation of the Likert-scale questions revealed similar tendencies in the four dimensions of awareness, transparency, trust, and organizational practices. Awareness section had fair agreement with mean values of between 3.35 and 4.20. Respondents highly appreciated that cybersecurity is essential to safeguard marketing analytics information with a mean score of 4.20 and also identified data breaches as one of the first-order concerns with a mean of 4.05. Nevertheless, the view of organizations that spend enough on cybersecurity was rated lower with a relatively low mean of 3.70, which indicated that participants thought that more resources need to be directed to this field.

In the transparency area, a majority of the respondents agreed that the cybersecurity measures open up more openness in marketing analytics. The assertion that transparency is dependent on robust cybersecurity protocols had a mean score of 4.00 and the belief that to ensure ethical use of consumer data, there must be appropriate cybersecurity had a mean score of 3.92. Nevertheless, opinions were somewhat lower when it came to whether cybersecurity provides easier disclosure of data usage which had a mean of 3.60. These results indicated that participants felt that cybersecurity was important as a basis for transparent practices, but there was room for improvement in terms of communicating with consumers.

Trust was the most consistent dimension with mean scores consistently near 4.00 or better. Respondents strongly agreed that strong cybersecurity practices give customers more trust with a mean of 4.10 and consumers are more willing to share data with secure organizations with a mean of 3.98. On the same note, there was a notion that cybersecurity protection enhances long-term relationships with a mean of 3.85. The findings brought to the fore the importance of cybersecurity in establishing and sustaining trust between businesses and the customers within the digital marketing environment.

Organizational practices scored the lowest section average of 3.70, which is relatively poor compared to perceptions of awareness, transparency, and trust. While responses were positive that organisations deploy cybersecurity tools and meet data protection regulations, responses were less positive on employee training and policy adjustments, with mean scores of 3.55 and 3.40 respectively. This implied that organizations understand the significance of cyber security but have difficulties maintaining cyber security practices throughout their structures.

Overall, the results showed that the participants have a strong association of cybersecurity with transparency and trust in digital marketing analytics. While they appreciate some inroads

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

made in raising awareness, and the role cybersecurity plays in building consumer confidence, they also highlight the gaps in how organizations implement and communicate. The results highlight the significance of investing in the field of cybersecurity as a technical requirement and strategic facilitator of credibility in digital marketing.

Conclusion and Recommendations

The results of the current research indicate that cybersecurity is crucial to promote transparency and foster trust in digital marketing analytics. The evaluation also found that the respondents were always related to positive cybersecurity practices as more openness, ethical use of consumer data, and increased customer confidence. The strongest dimension was found to be trust whereby participants stressed on the importance of strong security practices in enhancing willingness of consumers to share information and firm long term relationships. Another significant element turned out to be transparency because respondents associated successful cybersecurity systems with ethical and transparent data practices. But the findings also indicated areas of lapses in the organizational practices especially in employee training, enforcement of policies, and regular review of the cybersecurity measures. It is an indication that as much as cybersecurity awareness is great, it is not easy to translate this awareness into organizational structures and activities.

Some recommendations can be suggested based on such findings. First, companies should invest more in cybersecurity infrastructure, whereby their systems should not be limited to meet international standards but also flexible to new digital threats. In addition to the technical protection, companies must also establish policy-wide approaches to ensure that consumer rights are met and that marketing analytics data will be used in an ethical manner. This involves open-handed communication of information usage policies and taking the initiative to communicate to consumers to strengthen trust.

Second, training of employees should be of primary concern. Human error or lack of awareness also leads to many data breaches and security lapses, and it is necessary to design training programs that provide staff with knowledge and skills to work with sensitive data safely. Regular workshops, simulations and policy refreshers can help to strengthen the internal culture of cybersecurity.

Third, it is important to cooperate with the regulators and industry stakeholders. Through organizational alignment of best practices with laid down data protection laws and knowledge sharing across industries, businesses can be in a position to influence a collective response to cybersecurity threats in digital marketing.

Finally, cybersecurity is not a technical demand anymore but a strategy that creates transparency and trust. Those organizations which incorporate effective cybersecurity measures to their marketing analytics activities will safeguard consumer information and also market their reputations and competitive position long-term on the online market.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

References

Afshar, M. Z., & Shah, M. H. (2025). A Narrative Review for Revisiting BCG Matrix Application in Performance Evaluation of Public Sector Entities. *The Journal of Research Review*, *2*(02), 325-337.

Afshar, M. Z., & Shah, M. H. (2025). Resilience Through Adaptation: Examining the Interplay Between Adaptive Capacity and Organizational Resilience in Public Sector Organizations. *ACADEMIA International Journal for Social Sciences*, *4*(2), 1770-1789.

Ahmad, A. S. (2023). Application of big data and artificial intelligence in strengthening fraud analytics and cybersecurity resilience in global financial markets. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 11-23.

Ahmad, S., & Museera, S. (2024). The Strategic Influence of Cloud Computing on Contemporary Marketing and Management Practices. *Journal of Engineering and Computational Intelligence Review*, *2*(2), 21-30.

Alim, I., Imtiaz, N., Al Prince, A., & Hasan, M. A. (2025). AI and Blockchain Integration: Driving Strategic Business Advancements in the Intelligent Era. *Journal of Engineering and Computational Intelligence Review*, *3*(2), 38-50.

Arif, M., Goswami, A., Saibaba, C. H., Sharada, K., Pandey, T. K., & Nigam, A. (2024). Cybersecurity Approaches for Securing Digital Marketing Data. *Journal of Cybersecurity & Information Management*, *13*(2).

Atif, M. (2024). The Transformative Role of Block chain Technology in Supply Chain Management. *Journal of Engineering and Computational Intelligence Review*, *2*(2), 31-44.

Bhagyalakshmi, L. (2024). Securing the Future of Digital Marketing through Advanced Cybersecurity Approaches and Consumer Data Protection Privacy and Regulatory Compliance. *Journal of Cybersecurity & Information Management*, *13*(1).

Butt, S. (2021). Impact of E-Banking Service Quality on Customers' Behavior Intentions Mediating Role of Trust. *Global Management Journal for Academic & Corporate Studies*, *11*(2), 1-21.

Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. *EURASIP Journal on Information Security*, *2018*(1), 10.

Chen, D., Fraiberger, S. P., Moakler, R., & Provost, F. (2017). Enhancing transparency and control when drawing data-driven inferences about individuals. *Big data*, *5*(3), 197-212.

Danish, M., & Siraj, M. M. (2025). AI and Cybersecurity: Defending Data and Privacy in the Digital Age. *Journal of Engineering and Computational Intelligence Review*, *3*(1), 25-35.

Friday, S. C., Lawal, C. I., Ayodeji, D. C., & Sobowale, A. (2024). Reviewing the effectiveness of digital audit tools in enhancing corporate transparency. *International Journal of Advanced Multidisciplinary Research and Studies*, *6*(4), 1679-1689.

Geetha, B. T., Usman, M., Randhawa, N., Pipliwal, L., Maheshwari, K., & Kapila, N. (2024, March). Revolutionizing the dynamics of digital marketing by including cybersecurity measures and safeguarding consumer data. In *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies* (pp. 1-5). IEEE.

Hamburg, I., & Grosch, K. R. (2017). Ethical aspects in cyber security. *Archives of Business Research*, *5*(10).

Huda, M., Sutopo, L., Liberty, Febrianto, & Mustafa, M. C. (2022, March). Digital information transparency for cyber security: critical points in social media trends. In *Future of Information and Communication Conference* (pp. 814-831). Cham: Springer International Publishing.

Imtiaz, N., Zannat, F., Ahmed, S., Hasan, M. A., & Mahmud, S. (2025). Leveraging AI for Data-Driven Decision Making and Automation in the USA Education Sector. Journal of Economics, Management & Business Administration, 4(1), 87-106.

Imtiaz, N., Zannat, F., Vengaladas, M. K., Mahmud, S., & Hasan, M. A. (2025). Transforming Business Analytics: The Impact of Machine Learning on Performance Prediction in US financial sectors. *Journal of Business Insight and Innovation*, *4*(1), 61-72.

Jebril, I., Almaslmani, R., Jarah, B., Mugableh, M., & Zaqeeba, N. (2023). The impact of strategic intelligence and asset management on enhancing competitive advantage: The mediating role of cybersecurity. *Uncertain Supply Chain Management*, *11*(3), 1041-1046.

Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber security and digital economy: opportunities, growth and challenges. *Journal of technology innovations and energy*, *3*(2), 1-22.

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 195.

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer fraud & security*, *2020*(2), 14-17.

Mou, A. J., Hossain, M. S., & Siddiqui, N. A. (2022). Digital transformation in marketing: evaluating the impact of web analytics and SEO on SME growth. *American Journal of Interdisciplinary Studies*, *3*(04), 61-90.

Oluwafemi, I. O., Clement, T., Adanigbo, O. S., Gbenle, T. P., & Adekunle, B. I. (2021). A review of ethical considerations in AI-driven marketing analytics: Privacy, transparency, and consumer trust. *International Journal Of Multidisciplinary Research and Growth Evaluation*, *2*(2), 428-435.

Rabby, F., Chimhundu, R., & Hassan, R. (2022). Blockchain-enabled trust management for digital marketing in the Industry 4.0 Era. In *Advances in blockchain technology for cyber physical systems* (pp. 303-321). Cham: Springer International Publishing.

Sadia, B. U. T. T. (2020). Service quality assessment and student satisfaction in business schools: Mediating role of perceived value. *MOJEM: Malaysian Online Journal of Educational Management*, *9*(1), 58-76.

Shaheen, A. (2023). Cybersecurity in the Modern Era: An Overview of Recent Trends. *Journal of Engineering and Computational Intelligence Review*, *1*(1), 39-50.

Shaheen, A. (2024). The Internet of Things (IoT): A Comprehensive Review of Technologies, Applications, Challenges, and Future Trends. *Journal of Engineering and Computational Intelligence Review*, *2*(1), 1-8.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Tezel, A., Papadonikolaki, E., Yitmen, I., & Bolpagni, M. (2021). Blockchain opportunities and issues in the built environment: Perspectives on trust, transparency and cybersecurity. In *Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills* (pp. 569-588). Cham: Springer International Publishing.

Trim, P. R., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224-238.

Ullah, A., & Khan, S. D. (2024). Impact of sound decision-making on small and medium businesses in Pakistan. *International Journal of Asian Business and Management*, *3*(2), 177-192.

Wang, L., & Jones, R. (2021). Big data analytics in cyber security: network traffic and attacks. *Journal of Computer Information Systems*, *61*(5), 410-417.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), 127.

Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., ... & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare technology letters*, *8*(3), 66-77.

Zhu, P., Hu, J., Li, X., & Zhu, Q. (2021). Using blockchain technology to enhance the traceability of original achievements. *IEEE Transactions on Engineering Management*, *70*(5), 1693-1707.