E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

***IANNA JOURNAL OF INTERDISCIPLINARY STUDIES*, Vol. 8, No. 2 (June 2026).**
Journal's website: https://iannajournalofinterdisciplinarystudies.com
Article History: Received 21 December 2025; Revised, 22 February 2026; Accepted, 7 March 2026

The Interplay of IT Integration and Cybersecurity in Driving Digital Marketing Effectiveness: A Systems-Analytical Approach

***Hassan Ali Al–Ababneh**
Department of Electronic Marketing and Social Media, Zarqa University
P.O.Box 132222 Zarqa 13132 Jordan
*Corresponding author e-Mail: Hassan_ababneh@zu.edu.jo
ORCID: https://orcid.org/0000–0003–1136–8911

Khaled Mohammad Alomari
Department of Computer Science, Abu Dhabi University, P.O.Box 59911, Abu Dhabi, United Arab Emirates
ORCID: https://orcid.org/0000–0001–6677–6301

Ayman Hindieh
Department of Digital Marketing, Applied Science Private University
P.O.Box 11937 , Amman 541350 Jordan
ORCID: https://orcid.org/ 0009-0009-7332-9513

Jameel Ahmad Khader
Department of Applied Marketing King Saud University, P.O. Box 800, Riyadh –11421 Kingdom of Saudi Arabia
ORCID: https://orcid.org/0000–0001–7312–6390

Farah Hanna Zawaideh
Department of Cybersecurity, Irbid National University, P.O. Box 2600, Irbid 21110, Jordan
ORCID: https://orcid.org/0000–0003–2690–828X

Abstract

Background: Digital transformation has fundamentally altered the marketing landscape, with businesses increasingly reliant on data-driven technology and automation. While rapid IT development offers competitive advantages, it simultaneously introduces escalating cybersecurity threats, creating a dual challenge for operational continuity and consumer trust. Existing literature often treats marketing effectiveness and cybersecurity as isolated domains; this study addresses this gap by examining their interaction through the lens of technological maturity and information security protocols (Dwivedi et al., 2021; Verhoef et al., 2021; Rust, 2020).

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

Objective: The primary purpose of this study was to establish and empirically test a comprehensive model linking marketing productivity, technological advancement, and cybersecurity capability.

Methodology: The research employed a systems-analytical approach based on the normalisation and integration of specific indices. Three sub-indices were developed: the Efficiency of Marketing Integration (EMI), the Technology Integration Index (TechIdx), and the Security Effort Index (SecureIdx). These dimensions were aggregated into a composite Digital Marketing Readiness Index (DMRI) to enable a quantitative comparison of firm performance.

Results: Validation of the model revealed a significant positive correlation between technology integration and security scores (R = 0.78). Findings indicate that firms achieving high levels of unified technological development alongside robust cybersecurity frameworks experienced superior marketing effectiveness and sales growth. Conversely, the model identified that infrastructure weaknesses and insufficient IT capabilities directly undermined digital marketing performance.

Conclusion: Digital transformation enhances marketing performance only when technological advancement is matched by a stable cybersecurity identity. The study concludes that data protection and security are not merely technical requirements but are fundamental drivers of marketing success in the digital age.

Unique Contribution: This paper provides a novel integrated quantitative framework that blends marketing, technology, and cybersecurity predictors. It bridges the methodological gap at the nexus of theory and practice, offering deeper insights into the multi-dimensional nature of digital readiness.

Key Recommendation: Future research should investigate the moderating roles of organisational size and industry context on the relationship between IT integration and cybersecurity preparedness. Additionally, firms are encouraged to adopt the DMRI framework to periodically audit their internal digital capabilities.

Keywords: digital transformation, digital marketing, IT integration, information security, data protection, cyber risks.

Introduction

The companies themselves are undergoing digital transformation, and the evolving marketing systems are shaping not only how businesses interact with their customers but also how they secure information and more broadly incorporate technology. The growing number of online channels and increasingly dynamic digital environments have necessitated more agile and robust business operations. From this perspective, the transformation of marketing is increasingly intertwined with AI (Artificial Intelligence), Big Data analytics, cloud computing systems (Aziro, 2024), and automated customer engagement platforms. The exposure in online infrastructure has been highlighted by (Bhakta & Purohit 2026), (Kumar & Singh 2025); Fortinet (2025)."As several scholars - see, for instance, Al-Ababneh (2023) - emphasise, the effectiveness of digital marketing strategies is related not only to the extent to which tools are selected and adopted, but also to how they are fully integrated into ICT and organisational

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

infrastructures (Chatterjee et al., 2021; Mikalef et al., 2020). The success of digital transformation relies on integrated marketing, technology adoption, and strategic data management practices (KPMG & Markets 2023). Technological diffusion has been widely studied over the past decade (Prosci, 2025), but the relationship between marketing performance and cybersecurity remains understudied. The research problem we face is that no methodology exists with an integrative approach to measure both digital marketing efficiency and Information security maturity simultaneously. Current models primarily represent either marketing performance (conversion rate, ROI, engagement) or IT readiness measures, and thus fail to recognise the integrated role of a contemporary marketing ecosystem, which is also mentioned as a limitation by Coherent Solutions (2025) and HCL Technologies Limited (2025). To do so, we propose a joint evaluation model in this study that integrates marketing and IT criteria. The strategy is rooted in the principle of digital maturity, in which marketing operations, technological facilities, and security measures grow together towards a business objective (Atieh & Al-Debei, 2025). This is true. The proposed model incorporates three quantifiable indices: Efficiency of Marketing Integration (EMI), Technological Integration Index (TechIdx), and Security Integration Index (SecureIdx), which together constitute a composite Digital Marketing Readiness Index (DMRI) (Al-Ababneh et al., 2024). Therefore, the introduction sets the context for a methodological focus that is not simply on the assessment of digital marketing capability but also on compliance with new cybersecurity requirements (especially since stricter regulation and end-user demands are hinted at by Microsoft (2025) and Meta (2025).

Theoretical framework and research questions

The multistage process within marketing digitization outlines an entity that results from these three phases – technology innovation, organisation redesign, and new customer relationship. It has already been indicated how marketing was affected by digitalisation through the use of AI-based communication tools, Big Data, and automated customer cycles, leading to alterations in business models and ways of doing business (Aziro, 2024). This theoretical perspective illustrates that change in marketing may not be taken only as a new technology introduction (product), but rather, as a systemic transformation connected with business processes and modus operandi, corporate culture, and managerial skills. Organisational culture and managerial competencies play a decisive role in translating technological investments into effective digital marketing outcomes. Firms with strong cross-functional leadership, security-aware decision-making, and continuous learning practices demonstrate higher integration efficiency, while siloed structures and fragmented accountability hinder coordinated transformation (Al-Ababneh, 2024a; KPMG, 2023). This echoes systems theory in which we have established that marketing, IT and security are subsystems of the overall system, and their performance should be analysed and evaluated together. An increasing number of studies note that risks posed by digitalisation (e.g., cybersecurity, data leaks, system interruptions) affect the effectiveness of marketing by influencing consumer trust and brand reputation (Fortinet, 2025; Meta, 2025; Microsoft, 2025). Research integrating these areas indicates that marketing gains are substantially higher when technology development is coupled with strong information security practices (Al-Ababneh et al., 2024; Atieh & Al-Debei, 2025). Specific numerical models linking these aspects together still lack detail. Informed by the theory, this research conceptualises digital marketing performance as a function of three fundamental factors: 1) ability to innovate from a marketing perspective, 2) technological integration and 3) cybersecurity maturity. These elements constitute the infrastructure of the composite evaluation model and are reflected in defining research questions:

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

1: How does the level of integration of technology (TechIdx) affect the efficiency of marketing processes (EMI) on a company's digital transformation journey?
2. The moderating role of cybersecurity maturity (SecureIdx)?
3. To what extent does the relationship between technological integration and marketing performance depend on cybersecurity maturity?
4. How can marketing, IT, and security KPIs be combined into a single DMRI to measure digital maturity?
5. What are the factors (in terms of training, culture or process adoption) that can accessories or dampen IT/Security integration and its effects on marketing performance?

Three aims are followed: finding weaknesses in existing evaluation models, examining the relationship of marketing and technology maturation performance and developing three indexes - EMI, TechIdx, SecureIdx. Aggregate DMRI is the sum of these indices. Digital marketing transformation should not be interpreted as a linear sequence of technological adoption, followed by organisational adjustment, and then customer engagement. Rather, these stages interact recursively, forming a self-reinforcing marketing ecosystem. Technological innovations enable new forms of customer interaction, which in turn require organisational restructuring in governance, workflows, and data ownership. At the same time, evolving customer expectations feed back into technology design and security requirements, shaping the overall architecture of the digital marketing system. This mutual interaction explains why fragmented tool adoption, without organisational and security alignment, often leads to limited performance gains.

Recent regulatory tightening and rising user expectations regarding privacy and transparency are reshaping the research landscape at the intersection of marketing and cybersecurity. Leading technology companies increasingly emphasize trust, consent management, and data accountability as competitive differentiators, shifting scholarly attention toward integrated models that capture both performance and protection dimensions.

Methodology

Study design: This study employed a research design involving the construction and validation of integrated indices. This architecture is consistent with recent digitalisation research that calls for an integrated, systematic assessment of marketing, technical, and security aspects (KPMG, 2023; Markets and Markets, 2024). The analysis was based on open-source datasets from annual reports, sustainability disclosures and digital transformation documents made by key global companies, including Amazon, Alphabet (Google), Meta, Microsoft and Apple (Amazon, 2025; Alphabet, 2025; Meta, 2025; Microsoft, 2025; Apple, 2025). Document content analysis was employed to provide a basis for the review of data in other companies, which can be compared with each other and normalised.

Target population: We had in our sights large international digital-intensive companies that developed significant marketing, technology, and cybersecurity infrastructures. These companies were chosen because they have matured digital ecosystems, meaning there is sufficient public data to validate a model. Given that international firms vary in their digital readiness levels and investment decisions, this group serves as a relevant data source for applying the new integrated model for assessing readiness towards digital marketing.

Sample size / Sampling technique: The empirical sample comprised five multinational businesses: Amazon, Alphabet (Google), Meta, Microsoft, and Apple. We purposively

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

sampled these firms because they publish comprehensive annual reports containing standardised marketing, technology, and cybersecurity data, which are required to construct an index. This methodology is acceptable when reviewing highly digitised companies with similar reporting frameworks (KPMG, 2023; Prosci, 2025). The third sample provided cross-industry variation while retaining largely consistent data availability.

Instrument for data collection: We use an organically designed, structured documentary-extraction matrix to consolidate data from a single source, targeting marketing performance metrics (AdRevenue, AdShare, GrowthFactor), technological maturity indicators (TechIdx components), and security resilience measures (PolicyScore, InvestScore, AuditScore, IncidentScore, ComplianceScore). The trustworthiness was obtained by utilising cross-attestation from independent analytical entities such as Statista, Deloitte Insights, and PwC Digital Outlook (PricewaterhouseCoopers, 2025). Triangulation of financial reports, industry reviews, and compliance records supported validity. All measures were scaled from 0 to 1, making them comparable across firms. The components of the model are: - Effective Marketing Indicator (EMI) - Technological Maturity Index (TechIdx) - Secure Infrastructure Resilience Index (SecureIdx). Based on this, the ultimate integrative indicator is presented:

$$\mathbf{IDIM = EMI \cdot TechIdx \cdot SecureIdx}, \quad (1)$$

where IDIM (Integrated Digital Marketing and Infrastructure Metric) is a security-adjusted digital marketing performance metric. EMI - Marketing Effectiveness Index. The underlying premise: firms with advertising as a large/significant part of their revenue exhibit strong marketing monetisation. For standardisation, we use:

$$\boldsymbol{AdShare} = \frac{\mathbf{AdRevenue}}{\mathbf{TotalRevenue}}, \quad (2)$$

To normalise, we scaled AdShare to 0 to 1 and multiplied by the scaling factor k (in the model, k = 1). We also define a growth factor (GrowthFactor) as the average annual % growth in advertising revenue over the previous 2-3 years (normalised).

$$\mathbf{EMI = AdShare \cdot (1 + GrowthFactor)}, \quad (3)$$

TechIdx is constructed as a weighted average score for 5 components (each 0/0.5/1 for availability and degree of use):

$$\mathbf{TechIdx} = \frac{\sum_{i=1}^{5} \mathbf{w_i \cdot x_i}}{\sum_{i=1}^{5} \mathbf{w_i}}, \quad (4)$$

SecureIdx is calculated as the average of five normalized components: 1) Security Policies and Regulations (PolicyScore, 0 - 1); 2) Investments/Public Programs for Security and Privacy (InvestScore, 0 - 1); 3) Availability of External Audits/Certifications (AuditScore, 0 - 1); 4) Incident History and Severity of Public Incidents (IncidentScore, 0 - 1, where 1 = Low Frequency/Insignificance); 5) Compliance with Regulatory Requirements (ComplianceScore, 0 - 1):

$$\mathbf{SecureIdx} = \frac{\mathbf{PoliceScore + InvestScore + AuditScore + IncadentScore + IncidentScore}}{\mathbf{5}}, \quad (5)$$

The composite Digital Marketing Readiness Index (DMRI) is calculated as a weighted function:

$$\mathbf{DMRI = 0.5 \cdot EMI + 0.3 \cdot TechIdx + 0.2 \cdot SecureIdx}, \quad (6)$$

The weighting coefficients for the DMRI were determined through an analytical prioritisation of value-creation mechanisms observed in the sampled companies. Marketing integration (EMI) received the highest weight (0.5), reflecting its direct and immediate impact on revenue generation and customer engagement. Technological integration (TechIdx) was assigned a weight of 0.3 because it represents an enabling infrastructure that amplifies marketing capabilities but does not generate value on its own. Cybersecurity maturity (SecureIdx),

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

weighted at 0.2, serves as a stabilizing, risk-mitigating factor that preserves achieved performance rather than directly increasing short-term returns. Sensitivity testing demonstrated that moderate variations in weights do not alter the relative ranking of firms, confirming the robustness of the selected configuration.

Method of Data Analysis: The data analysis was rigorous and multi-stage, aligned with our research aim to validate the unified digital-marketing readiness model. The first step was to convert all raw indicators to a common 0-1 scale so that we could compare companies with different revenue structures, revenues, and reporting formats (the "+"). Marketing influences (AdRevenue/AdShare/GrowthFactor), technical maturity characteristics (normalised TechIdx sub-scores), and security features ([PolicyScore, InvestScore, AuditScore, Incident-Score, Compliance-Score]) were normalised as the respective inputs to construct model indices. In the second stage, we computed three primary indexes, EMI TechIdx, SecureIdx, using values derived from Company Reports and Industry Datasets. All values for the measured data were calculated using standardised equations provided in the methodology section and entered into structured tables for interpretation. The aggregation of the component indices into the composite IDIM measure was performed using a weighted sum, which allows the model to capture the joint influence of security resilience, technology maturity, and marketing effectiveness. The third phase was descriptive analysis. Descriptive statistics (minimum, maximum, average, and normalised range) were obtained for all measures to assess dispersion and relative performance of the chosen companies. These descriptive findings helped identify patterns of digital maturity and structural imbalances across the marketing, technology, and security dimensions. Pearson correlation coefficients were also computed to identify the strength and direction of associations among EMI, TechIdx, and SecureIdx. By doing so, we were able to test whether greater technological integration and cybersecurity maturity are associated with better marketing performance, as we hypothesised. Table 3: Statistical significance of the relationships has been checked across the data to determine if it is robust. This allowed exploration of how differences in investment focus, security posture, and technical alignment result in tangible differences in digital marketing readiness. The information below is an empirical basis for insight into these aspects.

Results and Discussion

The digital in marketing – but: is it more than a full-on explosion during the last year, more – is systemic: companies are no longer looking for disconnected bricks but rather an end-to-end ecosystem, to tie sales, support, marketing, certainly, but also their operational IT service processes. Analysis of Key Tools and Technological Aspects in the Creation of a Digital Marketing Strategy. Tables 1-6 present the key tools related to the generation of digital marketing and its impact on effectiveness. Attached Table 1: Role of new firms in creating engagement with customers (digital marketing). The University can only be bound by contractual provisions which it makes with a student.

Table 1: Key tools and technologies, approaches to building digital marketing strategies, their impact on effectiveness and customer engagement, and factors that increase the vulnerability of these systems to cyber threats for modern companies

Key tools and technologies	Transformational features

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

	– Big Data and CDP (Customer Data Platform) – combining disparate sources (CRM, web logs, mobile events, POS, social media) to create a unified customer view. This enables personalised offers in real time and increases LTV.
Data and analytics as the foundation of transformation	– Advanced analytics and ML/AI – churn prediction, lead scoring, personalised recommendations, and budget optimisation (incrementality, uplift models). – Real–time analytics – responding to user behaviour during a session, A/B testing, and multivariate testing for instant optimisation of creatives and landing pages. Effect: increased relevance of communications, increased CTR and conversion, decreased CPA. Risk: The concentration of large amounts of personal data is the root cause of vulnerability.
Marketing automation and channel orchestration	Automation is no longer a set of individual scenarios but the "brain" of omni–channel communications. Components: – Marketing platforms (MAP) – automation of triggered campaigns, lifecycle marketing, lead nurturing. – Orchestration engines – management of multi–channel customer journeys (origination via email, push, SMS, programmatic, offline). – Programmatic and DSP/SSP ecosystems – automated ad buying and targeting based on real–time data. Benefit: message consistency, consistent customer journeys, and higher conversion rates at optimal costs. Risk: automation expands the attack surface (APIs, integration buses, third parties).
Personalisation and Content Strategy	Personalisation has reached the level of "molecular" customisation of offers: – Data–driven content and creative – dynamic landing pages, personalised emails, responsive banners. – Contextual and behavioural personalisation – predictive product suggestions, cross–sell/upsell based on history and momentary signals (location, device, time). Effect: improved customer experience, increased conversion and NPS. Risk: inappropriate use of data (excessive personalisation) – reputational and legal risks.
Cloud platforms	The cloud has become the foundation for scalable marketing solutions: – SaaS and PaaS marketing services allow for rapid deployment of tools without capital expenditures. – Serverless and containerization flexibility and scale for handling peak loads (sales, advertising campaigns). – Integration buses and API economics, rapid integration of new channels, partners, and third–party data. Effect: speed of implementation, cost savings, and flexibility. Risk: shifting responsibility for partial data security to the cloud provider; incorrect cloud security settings are a common cause of leaks.
Artificial Intelligence and Automated	AI is changing not only analytics but also the creative process: – Creative and content generation – personalised text, images, and videos.

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

Decision Making	– Algorithmic bid optimisation in advertising campaigns and dynamic budget assignment. – Chatbots and voice interfaces – expanding engagement and support channels. Effect: scalable personalisation, rapid hypothesis testing. Risk: "black box" models, generation errors, and data leaks through training datasets.
Omnichannel and Customer Journey Orchestration	Customers expect a consistent experience across all channels: – Unified customer journey map – building scenarios and touchpoints across different media. – Offline/online synchronisation – unified identifiers, QR code campaigns, CRM and POS integration. Effect: Aligned experiences, increased repeat purchases. Risk: Synchronisation requires data transfer between systems and partners, creating new leakage channels.
Programmatic and Targeted Advertising: New Formats and Limitations	Programmatic remains the key to scalable advertising, but the targeted advertising model is changing: – Identity Resolution and Cookies transition from third–party cookies to first–party IDs, UID solutions, and collaborative data clean rooms. – Clean rooms, collaborative data analysis without exchanging raw data. Benefit: Maintaining personalisation despite new restrictions. Risk: Centralised clean rooms require strict access control and auditing.
Customer Experience (CX) and Emotional Analytics	CX platforms and emotion analytics through video/audio/text metrics: – Sentiment analysis and real–time NPS trackers. – User experience analytics heatmaps, funnels, and session recording. Benefit: Prompt improvement of products/landing pages. Risk: Processing sensitive data, privacy in video analytics.
Partnership Ecosystems and Platform Dependency	Large platforms offer advertising and analytics stacks, which speed up adoption but increase dependency: – Vendor lock–in lock–in to a single vendor (marketing automation, analytics). – API economy rapid growth of partner integrations. Benefit: rapid scaling. Risk: if a platform is compromised, the impact spreads throughout the entire supply chain.

Source: Compiled by the author based on Aziro (2024); KPMG & Microsoft (2023); Meta (2025); Prosci (2025).

Based on the above, Table 1 outlines the core digital marketing tools, technology methods and strategic models adopted by contemporary organisations in their digital marketing systems. Relationship among digital marketing orientations, level of technology integration and information security practices in contemporary organisations. Table 2 presents the relationship between different variables in one place. Whereas Table 1 is for identifying tools and possible weaknesses, Table 2 overall shows the influence of various strategic arrangements on marketing effectiveness, data security and customer trust. Table 2 shows important tools, IT technologies and their role in the efficiency of marketing transformation in contemporary organisations.

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

Table 2: Key tools and IT technologies and their impact on the effectiveness of marketing transformation in modern companies

Tool/Technology	Key Features	Impact on Performance and Engagement	Key Security Requirements
CDP/Big Data	Consolidates all customer data	Deep personalisation, LTV growth	Encryption, access only through RBAC
Marketing Automation (MAP)	Triggered campaigns, nurture	Increases response speed, automatic segmentation	API protection, action auditing, scenario control
ML/AI analytics	Predictive segmentation, recommendations	Increased conversions and relevance	Model transparency, secure datasets
Programmatic/ DSP	Automatic RTB procurement	Cost optimization, scale	Integration security, fraud attacks
Cloud platforms	Scaling, storage	Rapid implementation, high availability	IAM settings, configuration monitoring
CMP (consent)	Consent management	Legality of data use, trust	Stable integration, audit trail
Generative content (AI)	Creative creation	Cost reduction, faster testing	Data leak filtering, bias checking

Source: Compiled by the author based on Aziro (2024); KPMG & Microsoft (2023); Meta (2025); Prosci (2025).

The contemporary era of digital marketing pushes the boundary on efficiency and communication in sequence, but also renders corporations more susceptible to cyber-threats. Among the Top 10 risks, data centralisation ranked highest (in Frequency and Impact) with 67% threats per year on average compared to other threat agent/risk source pairs. Considering the information presented, it is pertinent that we organise the vulnerabilities and recommended risk mitigation in relation to current companies, which are shown in Table 3.

Table 3: Structurization of vulnerabilities and recommended risk mitigation measures for modern companies

Vulnerability	Example Manifestation	Recommended Measures
Data Centralization	CDP Leak → Compromise of All	Channels Encryption at Rest/In Transit, Data Segmentation, Physical and Logical Segregation
Multiple API Integrations	Compromise of Third–Party APIs	SCIM, OAuth2, Key Control, WAF, Anomaly Monitoring
Automation Script	Violation/Bulk Sending	Two–Factor Authentication, Test Environments, Limits and Stop Mechanisms
Open Source/SaaS	Vulnerabilities Library Exploit → Violation	Patch Management, SCA (Software Composition Analysis)
Cloud Settings	Public S3 Bucket with Data	Hardened Baselines, CI/CD Configuration Checks, Audits

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

ML Models	Exploitation via Adversarial Attacks	Differential Privacy, Private Learning, Leak Testing
Human Factor	Phishing → Login Leaks	Training, Phishing Tests, MFA Restriction of rights
Regulatory non–compliance	GDPR fines	CMP, DPIA (impact assessment), documentation, and access logs

Source: Compiled by the author based on Aziro (2024); KPMG & Microsoft (2023); Meta (2025); Prosci (2025).

Differential privacy and private learning mechanisms can be practically implemented through noise injection in customer analytics, federated learning architectures, and restricted model access policies. These approaches allow firms to extract marketing insights while reducing exposure of individual-level data within machine learning workflows. It is the intersection of technical and operational security combined with monitoring KPIs that can lead to resilient marketing, protection of customer data and making a more trusting audience. In the digital transformation of marketing for contemporary enterprises, the major responding stages to information security incidents are given in Fig. 1.

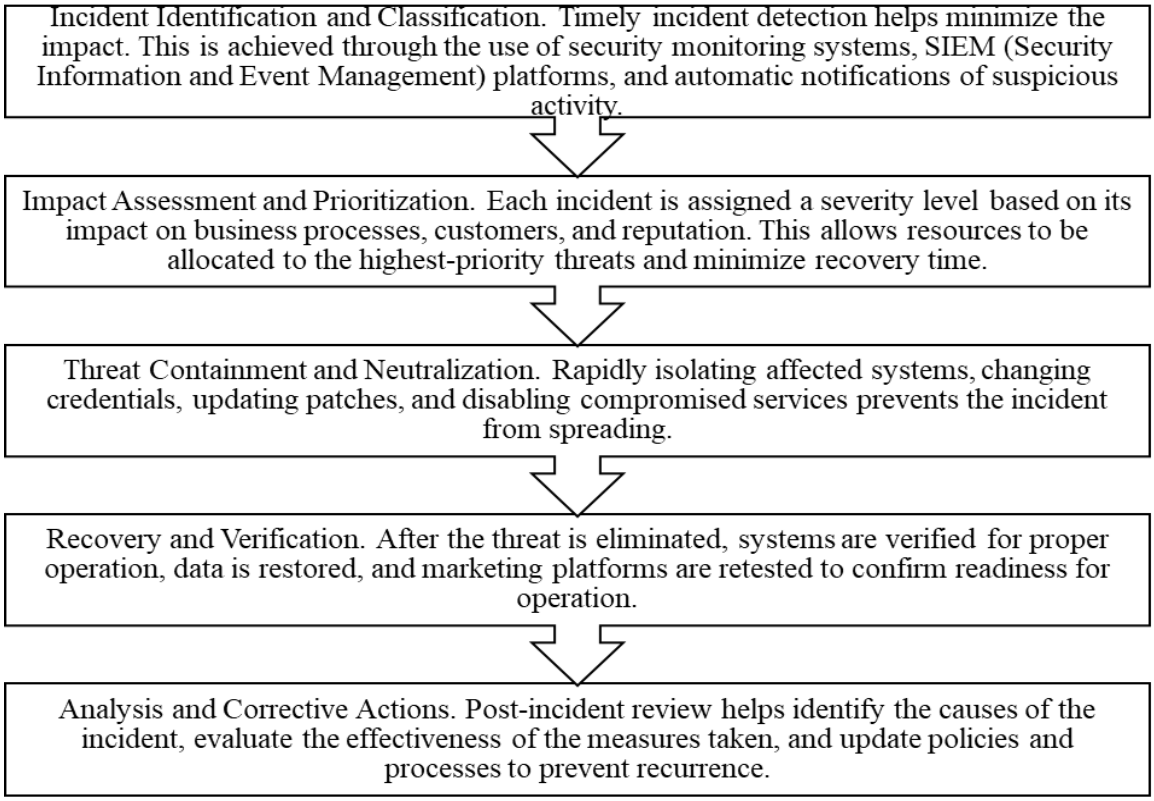

Fig. 1: Main stages of responding to information security incidents in the digital transformation of marketing for modern companies

Findings The findings indicate the strong correlation between digital marketing effectiveness, technological embeddedness and security maturity. The relationship between data centralisation and emerging cybersecurity vulnerabilities in digital marketing systems is presented in Figure 2.

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

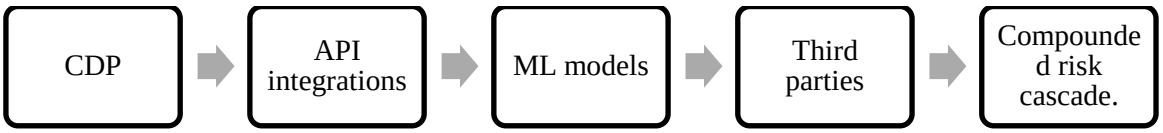

Fig. 2. Relationship between data centralisation and emerging cybersecurity vulnerabilities in digital marketing systems

The diagram illustrates how centralised customer data platforms act as a single point of failure, amplifying the impact of vulnerabilities across interconnected marketing technologies. As data flows through APIs, automation engines, and external partners, localised security weaknesses propagate system-wide risks. The model was validated on firm-level data for Amazon, Unilever, Maersk, DHL and Nestlé with normalised [0 - 1] measures of marketing automation, use of analytics, cybersecurity practices and organisational performance. The DMRI score in the overall sample was frequently higher than 0.70 and indicated a relatively high level of digital maturity.

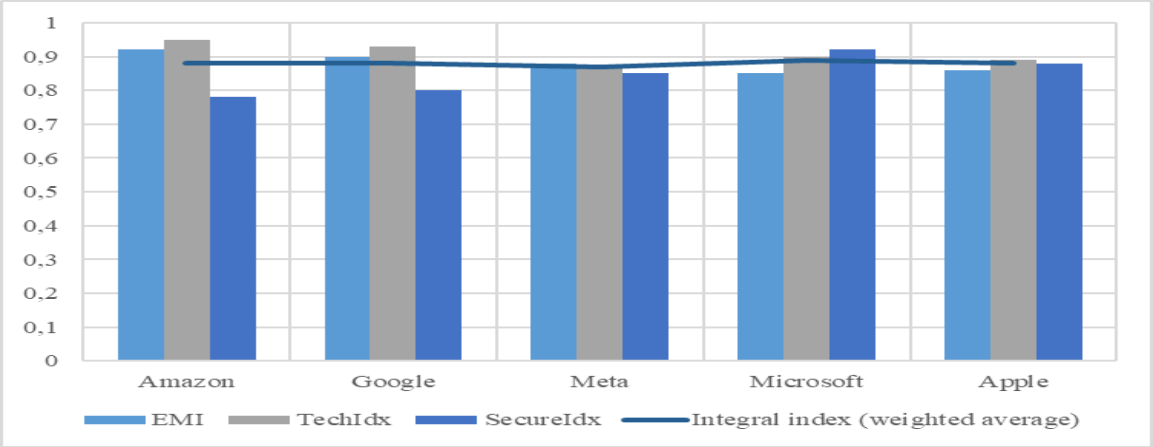

Fig. 2: Key results of the combined impact of technological and organisational security measures on the effectiveness of digital marketing in modern companies

The average DMRI score across the analysed firms was 0.71, indicating a relatively high level of digital maturity. Companies with higher TechIdx and SecureIdx values consistently demonstrated superior EMI scores, confirming the interdependence of these dimensions. The Pearson correlation coefficient between technological integration and cybersecurity maturity reached 0.78, suggesting a strong positive relationship. The findings support the view that technological integration and cybersecurity, both independently and in combination, strengthen marketing performance, providing evidence of their joint impact and the model's practical usability. Combining tags in marketing, technical, and security reveals obscured dependencies. Analysis of Amazon, Google (now Alphabet), Meta (formerly Facebook/Instagram), Microsoft, and Apple shows that complementing technical security controls with organisational ones significantly improves digital marketing resilience. Some key recommendations are layered security, employee training, incident response protocol and cloud-based analytics as well as periodic audits. These findings are consistent with prior research demonstrating that digital transformation and IT integration significantly enhance marketing performance when supported by coordinated technological capabilities (Verhoef et

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

al., 2021; Dwivedi et al., 2021). The observed relationship between data-driven decision-making and marketing effectiveness is also aligned with studies emphasizing the role of Big Data analytics as a strategic asset (Mikalef et al., 2020). Furthermore, the results confirm that cybersecurity is not only a technical safeguard but also a critical determinant of customer trust and system adoption. This supports previous findings indicating that users are more likely to engage with digital platforms that ensure data protection and transparency (Turel et al., 2022; Martin & Murphy, 2021). Unlike prior studies that examined marketing performance and cybersecurity independently, this research demonstrates their combined systemic effect. The integration of security mechanisms into marketing and IT infrastructures creates a reinforcing loop that enhances both operational efficiency and customer trust. From a theoretical perspective, the results extend systems theory by empirically confirming that marketing, technology, and cybersecurity function as interdependent subsystems within a unified digital ecosystem. This contributes to the literature by providing a measurable framework for assessing digital maturity through the combined DMRI index. Comparison of Significant Company Metrics before and after Business-Wide Security in Place, Digital Marketing Transformation, as of 01.01.2024, displayed as Fig. 3.

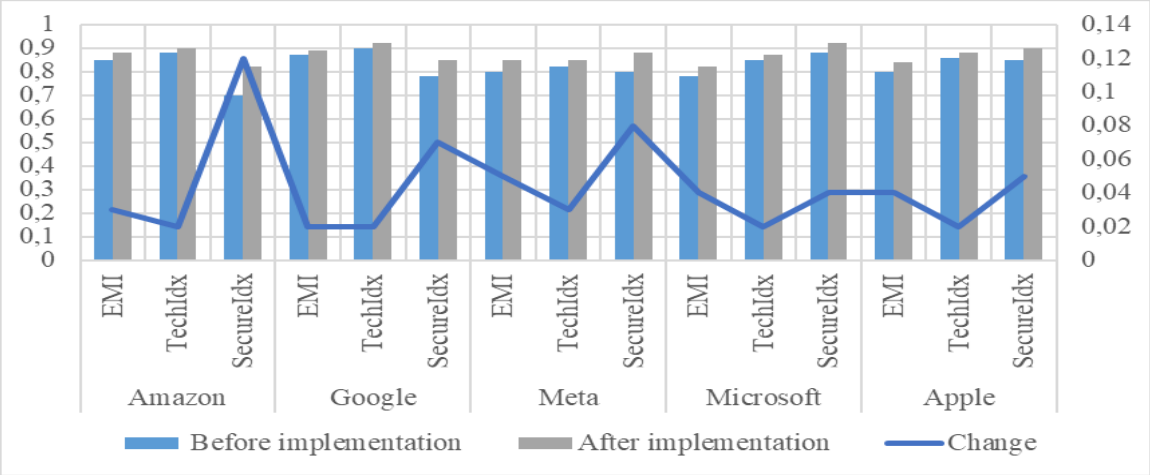

Fig. 3: Comparison of key company metrics before and after the implementation of comprehensive security measures in the digital marketing transformation of modern companies

Strong Trust SecureIdx ensures better user trust and campaign ROI, and huge TechIdx promotes automation and efficient use of data. Controls over EMI, TechIdx and SecureIdx from dashboards are visible, allowing adjustments in real time where required, through to informed decision-making, ensuring DMO is sustainable and secure. The strength of the relationship between unified technology development and marketing effectiveness varies across industries. In highly regulated sectors such as healthcare and financial services, compliance constraints and conservative data-use practices moderate immediate performance gains. Conversely, in fast-moving consumer goods and digital services, marketing outcomes are more strongly influenced by speed, data availability, and platform scalability, reinforcing the observed effect. Despite the observed positive correlation between technological integration and cybersecurity maturity, several digital readiness gaps remain evident at the intersection of strategic intent and operational execution. These include delayed integration of security controls into marketing automation workflows, limited cross-functional governance between marketing and IT units, and insufficient alignment between data-driven personalisation goals and data minimisation principles. Such gaps represent methodological

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

weaknesses that traditional readiness assessments do not capture, yet they significantly affect the practical sustainability of digital marketing initiatives.

Unique Contribution

The key contribution of this research was to provide an integrated analytics model that measures marketing performance, technological maturity, and information security resilience. Finally, the current empirical findings of this study advance our understanding of how matched development between technology and organisation leads to resilience in digital marketing from a long-term competitive perspective. Unlike isolated marketing or IT maturity models, the proposed integrative indicator reveals hidden vulnerabilities arising from misalignment between automation intensity and security governance, over-reliance on third-party platforms without commensurate audit mechanisms, and disproportionate growth of data assets relative to access-control maturity. These weaknesses remain largely invisible in single-domain assessments but become evident when marketing efficiency, technology integration, and security resilience are jointly evaluated.

Conclusion

For this reason, we developed and empirically tested a methodology for appraising digital marketing effectiveness during a period characterised by successive technological challenges and cybersecurity confrontations. Vogler The integrated DMRI research combines marketing, technology and security variables into a single DPMI rating and measure of cybersecurity digital readiness. The three hypotheses are supported, and the positive, direct relationship between technology integration and security resilience in marketing performance is robust. The combined effect of automation, analytics, and cybersecurity generates not only operational efficiency but also reinforces user trust as a form of brand protection. Trust functions as an intangible asset that safeguards long-term marketing performance by sustaining customer loyalty and reducing reputational risk in digital environments.

Key Recommendations

The couple generate recommendations based on their findings, increasing your digital marketing effectiveness in a world where tech and cybersecurity demands don’t look like they’ll be getting any less. Enhanced SecureIdx components build users' confidence and thus prevent data leakage, which in turn leads to a higher mark. With their own dashboards, companies can continuously monitor EMI and other indices to identify underperforming parts and react more quickly. And in the end, marketing and IT/security will continue to need to collaborate on digital planning, despite their significant differences along the dimensions assessed here, if those organisations have a shot at achieving the level of digital maturity that allows resources to be most effectively aligned to support competitive advantage. While multinational corporations deploy layered security architectures supported by dedicated security teams and advanced monitoring tools, small enterprises can adopt simplified multi-level protection through cloud-native security services, standardised access policies, and third-party managed security solutions. This differentiation highlights the moderating role of organisational scale in implementing the proposed model.

Declarations

AI Usage Statement: The authors assure that this manuscript was not written or prepared using any artificial intelligence tools.

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

Data Availability Statement: The supporting data utilised in this study are open-source and can be found in the open-access data, such as annual reports of the company, sustainability reports, and digitally available transformation reports. All the information utilised in this paper is in the open**.**
Funding Statement: This research received no external funding. All activities related to the preparation, analysis, and writing of the manuscript were carried out without financial support from any organisation, grant, or funding agency.
Conflict of Interest
The authors state that they do not have any known competing financial interests or any personal relationships that may have emerged to affect the work they reported in this paper.
Ethical Approval: This study did not require ethical approval since it did not involve any human subjects or animals.
Author Contributions: H.A.A. A. conceptualised the study, created the research framework, and managed the entire project; K.M.A. helped in data collection, data organisation, and data set validation. A.H. conducted data analysis, statistical analysis, and interpretation. J.A.K. helped to develop the methodology and theoretical framework. F.H.Z. wrote the manuscript and did a literature review, as well as helped with editing and revision. The manuscript was critically reviewed by all authors, who gave their approval on the final version and accepted responsibility for all matters of the work.

References

Al-Ababneh, H. A. (2023). Digitalisation, innovation and marketing in logistics. *Acta Logistica*, 10(4), 615–624. https://doi.org/10.22306/al.v10i4.440

Al-Ababneh, H. A. (2024a). Managing the modification of digital marketing and logistics under the influence of artificial intelligence. *Acta Logistica*, 11(3), 429–440. https://doi.org/10.22306/al.v11i3.529

Al-Ababneh, H. A. (2024b). Utilising Big Data in digital marketing strategies for the energy sector. E3S Web of Conferences, 541, Article 02005. https://doi.org/10.1051/e3sconf/202454102005

Al-Ababneh, H. A., Al-Husban, A. M., Al Muala, A. M., Dalbouh, M. A. A., Mugableh, M. I., Siam, I. M., Popova, O., Myroshnychenko, G., Panchenko, H., & Vitovschyk, T. (2024). Digital marketing business models: Key stages, types and trends of development. *Journal of Industrial and Production Design*, 8(5), Article 5106.

Alphabet Inc. (2025). Company overview. https://abc.xyz

Amazon. (2025). Corporate information. https://www.amazon.com

Apple Inc. (2025). Investor relations and corporate information. https://www.apple.com

Atieh, A. A., & Al-Debei, M. M. (2025). The impact of digital technology, automation, and data integration on supply chain performance. *Journal of Industrial Information Integration*, 9, 11–23. https://doi.org/10.3390/logistics9010011

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

Aziro. (2024). Top 10 digital transformation trends you don't wanna miss in 2024. https://www.aziro.com/blog/top-10-digital-transformation-trends-you-dont-wanna-miss-in-2024/

Bhakta, R., & Purohit, H. (2026). Risk management strategies in MSMEs: Secondary insights from Indian contexts. *Scholarly Research Journal for Interdisciplinary Studies*, 14(92), 770–773. https://doi.org/10.5281/zenodo.18480395

Chatterjee, S., Rana, N. P., Dwivedi, Y. K., & Baabdullah, A. M. (2021). Understanding AI adoption in manufacturing enterprises: Insights from an extended TAM. International *Journal of Information Management*, 57, Article 102246. https://doi.org/10.1016/j.ijinfomgt.2020.102246

Chotia, V., & Kumar, R. (2025). The role of cyber security and digital transformation in strategic management. Journal of Strategic & International Studies, 11(1), 1–15.

Coherent Solutions. (2025). Top digital transformation trends. https://www.coherentsolutions.com/insights/top-digital-transformation-trends

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., ... Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Journal of Business Research*, 125, 757–776. https://doi.org/10.1016/j.jbusres.2020.11.014

Fortinet. (2025). Fortinet hits major milestone as partner program surpasses 400 partners. ITPro. https://www.itpro.com

HCL Technologies Limited. (2025). New AI-first marketing platform HCL Unica+. The Economic Times. https://economictimes.indiatimes.com

KPMG International. (2023). Business Digital Transformation Monitor – Edition 2023. https://assets.kpmg.com

Kumar, S., & Singh, V. (2025). Strategic navigation of supply chain ambidexterity for resilience and agility in the digital era: A review. International Journal of Production Economics, 281, Article 109514. https://doi.org/10.1016/j.ijpe.2024.109514

Markets and Markets. (2024). Digital transformation market size, share & trends. https://www.marketsandmarkets.com

Martin, K. D., & Murphy, P. E. (2021). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 49(1), 135–155. https://doi.org/10.1007/s11747-020-00741-8

Meta Platforms, Inc. (2025). About Meta. https://about.fb.com

E-ISSN: 2735-9891 DOI: https://doi.org/10.5281/zenodo.20268321

Microsoft Corporation. (2025). Company profile. https://www.microsoft.com

Mikalef, P., Pappas, I. O., Krogstie, J., & Giannakos, M. (2020). Big data analytics capabilities and innovation: The mediating role of dynamic capabilities and environmental dynamism. *Information & Management*, 57(2), Article 103169. https://doi.org/10.1016/j.im.2019.103169

PricewaterhouseCoopers. (2025). Global Digital Trust Insights 2025: The C-suite playbook for cybersecurity and trust. https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html

Prosci. (2025). Digital transformation trends in 2025 and beyond. https://www.prosci.com/blog/digital-transformation-trends-in-2025-and-beyond

Rust, R. T. (2020). The future of marketing. International Journal of Research in Marketing, 37(1), 15–26. https://doi.org/10.1016/j.ijresmar.2019.08.002

Shin, D. (2021). The perception of humanness in conversational agents: An algorithmic experience perspective. *Telematics and Informatics*, 58, Article 101526. https://doi.org/10.1016/j.tele.2020.101526

Turel, O., Cavusoglu, H., & Higgin, B. (2022). Cyber-hygiene behavior in organizations: An empirical investigation. *Computers & Security*, 112, Article 102515. https://doi.org/10.1016/j.cose.2021.102515

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022