Integrating Cybersecurity and Digital Marketing Effectiveness: Exploring Resilience in Small to Medium-Sized Enterprises in Scotland

Kathy-Ann Fletcher
Faculty of Design, Informatics and Business
Abertay University
Scotland, United Kingdom
e-mail: k.fletcher@abertay.ac.uk

Nicole Carle
Faculty of Design, Informatics and Business
Abertay University
Scotland, United Kingdom
e-mail: n.carle@abertay.ac.uk

***Abstract*— As Small to Medium-sized Enterprises (SMEs) adopt digital marketing strategies to drive market growth, they face heightened exposure to cybersecurity threats. Through a qualitative methodology involving semi-structured interviews with SMEs in Scotland, the study identifies key themes including digital maturity, cybersecurity awareness, user trust, industry-specific challenges, and implementation barriers. Findings reveal a significant gap between cybersecurity awareness and practical implementation. The study proposes a model to guide SMEs in embedding cybersecurity into their marketing, thereby enhancing their resilience.**

Keywords- SMEs; cybersecurity; digital marketing; data protection; readiness.

I. INTRODUCTION

This paper presents an exploration of the relationship between cybersecurity readiness and digital marketing effectiveness among Small and Medium-sized Enterprises (SMEs). These two variables are increasingly essential to the resilience of SMEs with [1] defining organisational resilience as "an organisation's capability for turning adverse conditions into an organisational opportunity, positive attitude of 'bouncing back' and a relatively agile deportment". This investigation covers challenges, identifies common vulnerabilities, and evaluates cybersecurity adoption from the perspective of the Technology Acceptance Model (TAM) illustrating the factors that build perceptions of ease of use and usefulness of cybersecurity protocols for SME digital marketing objectives. Studies have demonstrated the power of digital marketing tools (e.g., social media) by SMEs to improve brand visibility, customer acquisition, and operational efficiencies [2]. However, this increasing reliance on digital platforms exposes SMEs to a more sophisticated range of cybersecurity threats. There is the need for SMEs to have readiness strategies that align marketing innovation with cybersecurity resilience, which is the focus of this study. These strategies are important to build resilience into the SMEs themselves and the wider society as it protects against financial, reputational, social, and broader harms as identified by [3] and [4]. This paper will explore the literature review in Section II, the methodology in Section III, findings and analysis in Sections IV and V, discussion in Section VI, and conclusion and future work in Section VII.

II. LITERATURE REVIEW

A. The Adoption of Digital Marketing by SMEs

Extant research acknowledges the power of digital marketing as an enabler of customer acquisition but also of long-term relationship management [5] by fostering innovation and agility in business models, particularly in resource-constrained environments [6]. Fear of the security of digital marketing tools can limit the adoption of e-commerce and digital marketing [7]. According to the research, the fear of data breaches, phishing attacks and the intimidation posed by data protection regulations like General Data Protection Regulation - GDPR (2018) and Data Protection Act (2018) [8]. Loo et al. [7] note that some SMEs will perceive digital platforms as a risk due to their limited capacity to mitigate against cybersecurity threats. This limits their ability to benefit from the full range of digital marketing tools such as marketing automation, customer relationship management systems, and online advertising platforms. This aligns with Technology Acceptance Model (TAM) [9] by showing their attitude towards adopting cybersecurity protocols. The Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) reflect a user's attitude towards using a system which then influences their behavioural intention to use and then their ultimate use of technology [10].

B. Cybersecurity Challenges for SMEs

Larger enterprises often have dedicated Information Technology (IT) security teams or the ability to outsource expertise, formal risk management protocols, and the resources to invest in advanced cybersecurity infrastructure, which may not be available to SMEs [11]. This leaves SMEs targets for bad actors who commit phishing, malware, data breaches, account takeovers, and other cyber-attacks [12], [13]. While SMEs face a heightened risk due to their limited cybersecurity adoption and over-reliance on third-party digital platforms [12], Jahankhani et al. [15] emphasise the role that digital tools have in wider market reach which complicates the security risks for SMEs. These challenges are amplified by SME underestimation of cyber

risk [14] and a lack of compliance with industry and regulatory standards such as GDPR or ISO/IEC 27001 [12], [15]. Research needs to consider the systemic harm caused by the human factor, which represents a critical weakness [16], [17], [18] to organisational resilience. This danger exists at various levels from management lack of cybersecurity readiness and strategy to employee lack of literacy [14] and buy-in, posing a risk to the resilience of organisations by exploiting the trust and routine business process to cause harms to the SMEs and their stakeholders [17], [19].

SMEs frequently lack formal cybersecurity policies or governance structures [20]. The absence of internal frameworks and policies as well as industry-wide or governmental policies and infrastructure is critical to the level of unpreparedness identified in SMES [21], [22]. The challenges include insider threat being one of the more dangerous [23], [24]. This threat comes from employees, contractors or partners who have access to internal systems and data [25]. These threats can be malicious or unintentional [26], highlighting the crucial need for training, awareness, and monitoring of threats from the SME [25]. SMEs are particularly vulnerable to insider threat [27], [28], due to their high trust and low oversight operations which gives employees broad access to sensitive systems and little role-based access controls [29].

C. Integrated Cybersecurity Readiness and Digital Marketing Effectiveness Model for SME resilience

SMEs, which are adopting digital tools for their operational success [30], now need to embed cybersecurity into their marketing strategies. Cybersecurity strategies that work to secure customer data, ensure platform integrity and train marketing teams on cyber hygiene practices [12], hold immense potential to build trust between the company and its stakeholders. Consumer trust is a strategic asset [31], [32] where data privacy and integrity are paramount [33]. Research identifies several instruments by which cybersecurity builds trust. Firstly, [29] posits that trust is nurtured by transparency and systematic communication of security policies and data handling practices and breach response protocols. Secondly, authentication and access control protocols are signals to customers that their data is safeguarded [34], as they are strong identity and access management systems. Consequently, privacy protection and encryption are important for consumer trust especially in industries that manage sensitive data [35], [36]. Further, [37] notes the importance of detecting and mitigating threats early, which demonstrates a proactive approach to cybersecurity and reassures customers in the ability of the organisation in protecting their interests. Research like that discussed in [38]'s systematic review showed that compliance with international standards and participation in cybersecurity information sharing networks build trust by demonstrating accountability and collaboration. Considering all these identified links between cybersecurity, trust, and digital marketing [39], [40], it is imperative that cybersecurity is treated as a strategic business tool.

D. Research Gaps

There are robust cybersecurity frameworks such as ISO/IEC 27001, GDPR and advice provided by the National Institute of Standards and Technology (NIST), however, SMEs face significant barriers to implementation [19]. For instance, SMEs are prioritising business growth and customer acquisition over investing in cybersecurity, which is seen as a cost [41], [42], [43]. In so doing, they miss the relationship between cybersecurity and their business goals of growth, profitability, and customer acquisition. The research in [44] argues that SMEs are failing to match their digital marketing ambitions to the technical and regulatory demands of the noted cybersecurity frameworks. Frameworks might mandate responsible practices like ethical data handling [45] and small firms either may be unaware of their responsibilities or lack the cybersecurity tools to operationalise them effectively [15]. This, therefore, creates a gap between intent and actual practice of cybersecure digital marketing, which undermines consumer trust, exposes businesses to reputational and legal risks, threatening their resilience and long-term viability. To address this gap, there are calls for simplified, SME-specific adaptations of frameworks based on usability, affordability, and ethical alignment. This study explores the relationship between cybersecurity and effective digital marketing practices in the context of SME resilience in Scotland.

E. Technology Acceptance Model (TAM)

TAM has been widely applied across diverse disciplinary domains, [46], [47], [48], [49]. TAM was originated by [9], building on the Theory of Reasoned Action [50] and was designed to explain user acceptance of email technologies. Within TAM, the perceptions of users: Perceived Usefulness (PU) - the belief that a technology enhances performance [9], [51] - and Perceived Ease of Use (PEOU) - the belief that the technology requires minimal effort, shape their attitudes, which in turn influence behavioural intention and actual system use [52]. Although TAM is often praised for its simplicity [53], it has evolved to address its limitations. TAM2 [54] introduced social influence and cognitive instrumental processes, while the Unified Theory of Acceptance and Use of Technology [55] integrated multiple models to include performance expectancy, effort expectancy, social influence, and facilitating conditions. TAM3 [56] further incorporated perceived enjoyment and self-efficacy. Despite its widespread use, TAM has faced criticism. Scholars such as [57] and [58] argue that it overlooks contextual, cultural, and longitudinal factors. Others highlight its overreliance on self-reported data [59] and its individualistic orientation [60]. Additionally, [61] notes the model's neglect of variables like trust, perceived risk, and social norms. Nonetheless, TAM remains a foundational framework in

technology adoption research. This study builds on TAM by adapting it to explore the relationship between cybersecurity readiness and digital marketing effectiveness - addressing a key gap by incorporating contextual variables.

III. METHODOLOGY

To address the research gaps, identified in the literature review, this paper discusses the qualitative research undertaken for the project. We completed ten semi-structured interviews with key decision-makers from SMEs in various industries, including marketing executives, IT representatives, and owners. The sample was recruited through chambers of commerce members, SME organisations, and social media. The interviews were analysed using thematic analysis, developed by [62].

IV. FINDINGS AND ANALYSIS

The qualitative research interviews identified themes around digital marketing practices, cybersecurity awareness and industry-specific challenges faced by SMEs.

A. Theme 1: Digital Marketing Practices

The organisations vary in their adoption of digital marketing, from basic social media use to advanced search engine optmisation and analytics. This displays varying levels of digital maturity around SMEs, with some further progressing in digital adoption than others. However, their success is measured based on the purpose of SMEs in using digital marketing. These measures include engagement, awareness, increased sales, and subscription in addition to financial return on investment. The respondents identify a shared growing intent to align public relations, communications, and digital strategies. With this shared intention, the need for rigorous industry-specific cybersecurity protocols for SMEs is growing.

B. Theme 2: Cybersecurity Awareness and Practices

The participants demonstrate awareness of cybersecurity protocols that range from basic understanding to more structured practices. They more consistently use external IT support with some internal training. However, formal cybersecurity policies at an institutional level were lacking amongst the respondents. Many are only now beginning to take cybersecurity seriously as they perceived themselves as low-risk targets. They also mostly did not consider themselves targets, even in the face of digital marketing use, not previously making the link between the two variables.

C. Theme 3: User Trust and perception

The respondents display a strong link between trust in digital platforms and customer engagement. Trust is a signal to the audience that websites are secure, and the branding is consistent, which is crucial for user engagement. The SMEs owners are aware of this link as their users are increasingly cautious about data sharing and cookies, especially on unfamiliar platforms. Trust is important beyond engagement but also allows users to share financial details and donate money to causes supported by the SME. This trust can be essential even in the aftermath of an attack to allow users to perceive that the company took all the precautionary steps to prevent the attack and will take accountability in the case of a successful threat.

D. Theme 4: Industry-Specific Challenges

The respondents demonstrate several industry-specific challenges to adopting both digital marketing and cybersecurity protocols. Firstly, most of the organisations interviewed operate with limited financial and human resources that can be dedicated to improving either their digital outreach or cybersecurity. Participant B agreed that their SME is a soft target, but they do not have a large budget for cybersecurity. This implies that relying on external IT support creates gaps in responsibility, accountability, and awareness, creating the industry-specific gap in awareness and implementation. Despite these limited resources, some of the SMEs are handling extremely sensitive data, such as personal information of vulnerable individuals.

E. Theme 5: Barriers and Gaps

The responses show a lack of formal training and industry-wide communication regarding formal cyber security protocols. Even with external IT support, this does not extend to internal training, capacity-building, or awareness. The human factor creates a weak link in the SMEs cybersecurity. This is related to a lack of clear roles about who is responsible for what within the cybersecurity, meaning SMEs are under the impression that it is being handled at some point, resulting in gaps in implementation. Even with awareness of resources, such as National Cyber Security Centre (NCSC) guidance or Charity Excellence Framework, these often go underutilised by the respondents, reflecting a gap between available support and the practical application of recommendations within these resources. Another barrier is that some SMEs did not see cybersecurity as a pressing concern, especially if they do not see themselves as targets or if they have not had any cybersecurity incidents. The lack of industry-wide dialogue or collaboration on cybersecurity is also a barrier. Without shared standards or peer learning threatening SMEs on an individual and industry-wide basis do not have the ability to plan and recover from cyberattacks, therefore, posing a real risk to their organisational resilience.

V. SUMMARY OF KEY FINDINGS

SMEs measure digital marketing success through purpose-built metrics such as engagement and sales. There is a growing intention to integrate PR, communications, and digital strategies with robust cybersecurity protocols. SMEs show increasing awareness of cybersecurity but often lack formal policies and underestimate their vulnerability, which contributes to complacency and inconsistency in

implementation of cybersecurity protocols. SMEs recognise that secure, consistent branding and transparency are vital to managing user confidence and loyalty. Unique challenges such as limited financial and human resources restrict SMEs' adoption of cybersecurity measures as they make use of the digital platforms to manage their customer relationships. The lack of formal training, internal capacity and industry-wide collaboration are further unique barriers to effective cybersecurity in SMEs.

VI. DISCUSSION

Theme 1 revealed varying levels of digital maturity among SMEs. This aligns with TAM's construct of Perceived Usefulness (PU), where technology is adopted based on its potential to enhance performance [9], [51]. Theme 2 highlighted a gap between cybersecurity awareness and implementation. This implementation gap is critical, as cybersecurity readiness influences digital marketing effectiveness and overall resilience. This readiness and implementation gap is linked to the resource challenges identified by authors like [12] and [15]. The assumption that external IT support covers all cybersecurity needs reflects a lack of internal ownership, which undermines the organisation's ability to respond to disruptions. Venkatesh and Davis [54] expanded TAM to include social influence and job relevance, suggesting that organisational context shapes technology adoption—a factor often ignored in relation to SMEs. Theme 3 underscored the importance of user trust in digital platforms, linking it to engagement and other positive outcomes including resilience, diverging from arguments made by [61] that TAM neglects variables such as trust and perceived risk. Regarding resilience, trust is a strategic asset that empowers SMEs to recover from cyber-attacks while maintaining stakeholder confidence.

Theme 4 revealed that SMEs are faced with unique challenges due to their limited resources and the high data sensitivity of the services they provide. Despite handling vulnerable user data, many organisations lacked industry-specific cybersecurity frameworks. Authors of works like [57] and [58] critique TAM for failing to address contextual and cultural factors, a gap that this study addresses by adapting TAM to the specific case of resource-constrained industries. This study suggests that organisational resilience in these contexts would be improved with tailored guidance and shared standards. Theme 5's findings revealed barriers such as informal training, accountability gaps, and poor utilisation of available resources for improving cybersecurity implementation. This finding supports arguments that there are gaps in TAM's model, where it fails to predict sustained use and organisational integration [59] [60]. The lack of industry wide dialogue further isolates SMEs, affecting their resilience. This places the insight from industry wide dialogue as a crucial resource for SMEs that is useful for building capacity and safeguarding digital marketing operations.

VII. CONCLUSION AND FUTURE WORK

This study has explored the critical intersection between cybersecurity readiness and digital marketing effectiveness within SMEs, highlighting the importance of integrating these domains to enhance organisational resilience. Through qualitative interviews and thematic analysis, the research identified key challenges including limited resources, low internal cybersecurity capacity, and a disconnect between awareness and implementation. The findings underscore the strategic value of cybersecurity not only as a protective measure but also as a trust-building tool that supports digital engagement and long-term viability.

By adapting the Technology Acceptance Model (TAM), the study offers an evaluation of the context of SME adoption of cybersecurity protocols within their digital marketing strategies. This adaptation addresses gaps in traditional TAM applications by incorporating variables such as trust, perceived risk, and organisational context—factors that are particularly relevant to SMEs operating in resource-constrained environments.

Future research should focus on developing simplified cybersecurity frameworks tailored to SMEs, aligning security practices with marketing goals and ethical data handling. Quantitative validation of the adapted TAM model across sectors would enhance its applicability, while longitudinal studies could assess the long-term impact of integrated cybersecurity-marketing strategies on resilience. Additionally, exploring industry-wide collaboration and policy support could foster a culture of cybersecurity, and targeted training initiatives may help address internal capacity gaps and reduce human-factor vulnerabilities. By bridging the gap between cybersecurity and digital marketing, this research contributes to a more holistic understanding of SME resilience and offers a foundation for future innovation, policy development, and academic inquiry.

ACKNOWLEDGMENT

This work was supported by funding from the Carnegie Trust for the Universities of Scotland.

REFERENCES

[1] D. Kantur and A. İşeri-Say, "Organizational Resilience: A Conceptual Integrative Framework," Journal of Management & Organization, 18(6), pp. 762–773, 2012, Available at: 10.1017/S1833367200000420.

[2] J. R. Saura, D. Palacios-Marqués and D. Ribeiro-Soriano, "Digital Marketing in SMEs Via Data-Driven Strategies: Reviewing the Current State of Research," Journal of Small Business Management, 61(3), pp. 1278–1313, 2023, Available at: 10.1080/00472778.2021.1955127.

[3] I. Agrafiotis, J. R. C Nurse, M. Goldsmith, S. Creese and D. Upton, "A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How they Propagate," Journal of Cybersecurity, 4(1), pp. 1, 2018, Available at: 10.1093/cybsec/tyy006.

[4] E. Islam, C. Rudolph and G. Oliver, "Managing Cyber Harm: A Survey of Challenges, Practices, and Opportunities,"

Information Security Journal, pp. 1–31, 2025, Available at: 10.1080/19393555.2025.2484348.

[5] S. Habib, N. N. Hamadneh and A. Hassan, "The Relationship between Digital Marketing, Customer Engagement, and Purchase Intention via OTT Platforms," Journal of Mathematics (Hidawi), 2022 (1) Available at: 10.1155/2022/5327626.

[6] N. Laila, P. Sucia Sukmaningrum, W. A. Saini Wan Ngah, L. Nur Rosyidi and I. Rahmawati, "An In-Depth Analysis of Digital Marketing Trends and Prospects in Small and Medium-sized Enterprises: Utilizing Bibliometric Mapping," Cogent Business & Management, 11(1), p. 2336565, 2024.

[7] M. K. Loo, S. Ramachandran and R. N. Raja Yusof, "Systematic Review of Factors and Barriers Influencing E-Commerce Adoption among SMEs over the Last Decade: A TOE Framework Perspective," Journal of the Knowledge Economy, 2024, Available at: 10.1007/s13132-024-02257-5.

[8] K. K. Kapoor, K. Tamilmani, N. P Rana, P. Patil, Y. K. Dwivedi and S. Nerur, "Advances in Social Media Research: Past, Present and Future," Information Systems Frontiers, 20, pp. 531-558, 2018.

[9] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly, pp. 319-340, 2018.

[10] F. Abdullah, R. Ward and E. Ahmed, "Investigating the Influence of the Most Commonly Used External Variables of TAM on Students' Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) of e-portfolios," Computers in Human Behaviour, 63, pp. 75–90, 2016, Available at: 10.1016/j.chb.2016.05.014.

[11] U. Awan, A. Keprate and P. Braathen, "A Conceptual Framework of An Integrative Leadership for Cybersecurity Management and Designing Digital Road Map for Organizations," Digital Transformation, Routledge India, pp. 47-59, 2025.

[12] A. Papathanasiou, G. Liontos, A. Katsouras, V. and E. Glavas, "Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era" Journal of Information Security, 16(1), pp. 1–43, 2025, Available at: 10.4236/jis.2025.161001.

[13] F. D. De Arroyabe, J. C. Arroyabe, M. Fernandez and C. F. A. Arranz, "Cybersecurity Resilience in SMEs. A Machine Learning Approach," The Journal of Computer Information Systems, 64(6), pp. 711–727, 2024, Available at: 10.1080/08874417.2023.2248925.

[14] C. R. Junior, I. Becker, and S. Johnson, "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity," arXiv preprint, 2023, Available at: arXiv:2309.17186.

[15] H. Jahankhani, L. N. K. Meda and M. Samadi, "Cybersecurity Challenges in Small and Medium Enterprise (SMEs) 'Blockchain and Other Emerging Technologies for Digital Business Strategies," Switzerland: Springer International Publishing AG, pp. 1–19, 2022.

[16] U. D Ani, H. He and A. Tiwari, "Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce," Journal of Systems and Information Technology, 21(1), pp. 2–35, 2019 Available at: 10.1108/JSIT-02-2018-0028.

[17] N. C. Edeh, "Cybersecurity and Human Factors," Cybersecurity for Decision Makers. 1st edn. United Kingdom: CRC Press, pp. 45–56, 2023.

[18] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," The Oxford Handbook of Cyberpsychology, Ithaca: Oxford University Press, 2018.

[19] M. Wilson, S. McDonald, D. Button and K. McGarry, "It Won't Happen to Me: Surveying SME Attitudes to Cyber-security," The Journal of Computer Information Systems, 63(2), pp. 397–409, 2023, Available at: 10.1080/08874417.2022.2067791.

[20] B. Saha and Z. Anwar, "A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework," Journal of Information Security, 15(1), pp. 24–39, 2024, Available at: 10.4236/jis.2024.151003.

[21] A. Chidukwani, S. and P. Koutsakis, "Cybersecurity Preparedness of Small-to-Medium Businesses: A Western Australia Study with Broader Implications," Computers & Security, 145, pp. 104026, 2024, Available at: 10.1016/j.cose.2024.104026.

[22] M. Neri, F. Niccolini and L. Martino, "Organizational Cybersecurity Readiness in the ICT Industry: a Quanti-Qqualitative Assessment," Information and Computer Security, 32(1), pp. 38–52, 2024, Available at: 10.1108/ICS-05-2023-0084.

[23] A. S. Abdullah, S. Dhiman and A. Ansari, "A Robust Model for Enabling Insider Threat Detection and Prevention: Techniques, Tools and Applications," Securing the Digital Frontier, Hoboken, NJ, USA: John Wiley & Sons, Inc, pp. 133–168, 2025.

[24] N. Ayanbode, O. A. Abieba, N. Chukwurah, O. O. Ajayi and A. I. Daraojimba, "Human Factors in Fintech Cybersecurity: Addressing Insider Threats and Behavioural Risks," International Journal of Multidisciplinary Research and Growth Evaluation, 5(1), pp. 1350–1356, 2024, Available at: 10.54660/.IJMRGE.2024.5.1.1350-1356.

[25] U. Inayat, M. Farzan, S. Mahmood. M. F. Zia, S. Hussain and F. Pallonetto, "Insider threat mitigation: Systematic Literature Review," Ain Shams Engineering Journal, 15(12), pp. 103068, 2024.

[26] A. Jaiswal, P. Dwivedi and R. K. Dewang, "Machine Learning Approaches to Detect, Prevent and Mitigate Malicious Insider Threats: State-Of-The-Art Review," Multimedia Tools and Applications, 2024, Available at: 10.1007/s11042-024-20273-0.

[27] A. Moneva and R. Leukfeldt, "Insider Threats among Dutch SMEs: Nature and Extent of Incidents, and Cyber Security Measures," Journal of Criminology, 56(4), pp. 416–440, 2023, Available at: 10.1177/26338076231161842.

[28] S. Pawar and H. Palivela, "LCCI: A Framework for Least Cybersecurity Controls to be Implemented for Small and Medium Enterprises (SMEs)," International Journal of Information Management Data Insights, 2(1), pp. 100080, 2022.

[29] A. Pigola, and F. de Souza Meirelles, "Unraveling Trust Management in Cybersecurity: Insights from a Systematic Literature Review," Information Technology and Management, 2024, Available at: 10.1007/s10799-024-00438-x.

[30] M. R. I. Bhuiyan, M. R. Faraji, M. Rashid, M. K. Bhuyan, R. Hossain and P. Ghose, "Digital Transformation in SMEs Emerging Technological Tools and Technologies for Enhancing the SME's Strategies and Outcomes," Journal of Ecohumanism, 3(4), pp. 211-224, 2024.

[31] L. Oliveira and M. Johanson, "Trust and Firm Internationalization: Dark-side Effects on Internationalization speed and How to Alleviate them," Journal of Business Research, 133, pp. 1–12, 2021, Available at: 10.1016/j.jbusres.2021.04.042.

[32] D. Koehn, "Integrity as a Business Asset", Journal of Business Ethics, 58(1/3), pp. 125–136, 2005, Available at: 10.1007/s10551-005-1391-x.

[33] A. Das, "Developing Dynamic Digital Capabilities in Micro-Multinationals Through Platform Ecosystems: Assessing the Role of Trust in Algorithmic Smart Contracts," Journal of International Entrepreneurship, 21(2), pp. 157–179, 2023, Available at: 10.1007/s10843-023-00332-7.

[34] W. Said, E. Mostafa, M. Hassan, and A. Mohamed Mostafa, "Multi-Factor Authentication-Based Framework for Identity Management in Cloud Applications," Computers, Materials & Continua, 71(2), pp. 3193–3209, 2022, Available at: 10.32604/cmc.2022.023554.

[35] N. J. King and V.T. Raja, "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud," Computer Law & Security Review, 28(3), pp. 308–319, 2012, Available at: 10.1016/j.clsr.2012.03.003.

[36] Z. Morić, V. Dakic, D. Djekic and D. Regvart, "Protection of Personal Data in the Context of E-Commerce," Journal of Cybersecurity and Privacy, 4(3), pp. 731–761, 2024, Available at: 10.3390/jcp4030034.

[37] M. Tahmasebi, "Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises," Journal of Information Security, 15(2), pp. 106–133, 2024, Available at: 10.4236/jis.2024.152008.

[38] R. Posso and J. Altmann, "Trust and Trust-Building Policies to Support Cybersecurity Information Sharing: A Systematic Literature Review," International Conference on the Economics of Grids, Clouds, Systems, and Services, Cham: Springer Nature Switzerland, pp. 212-228, 2024.

[39] H.N. Şenyapar, "Digital Marketing in the Age of Cyber Threats: A Comprehensive Guide to Cybersecurity Practices," Journal of Social Science, 8(15), pp. 1–10, 2024, Available at: 10.30520/tjsosci.1412062.

[40] L. Bhagyalakshmi, "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), 2024.

[41] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, "Cyber Risk Assessment and Optimisation: A Small Business Case Study," IEEE Access, 11, pp. 1, 2023, Available at: 10.1109/ACCESS.2023.3272670.

[42] A. Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," IEEe Access, 10, pp. 85701-85719, 2022.

[43] M. Dinkova, R. El-Dardiry and B. Overvest, "Should Firms Invest More in Cybersecurity?," Small Business Economics, 63(1), pp. 21–50, 2024, Available at: 10.1007/s11187-023-00803-0.

[44] M. F. Arroyabe, C. F. A. Arranz, I. F. De Arroyabe, and J. C. F. de Arroyabe, "Revealing the Realities of Cybercrime in Small and Medium Enterprises: Understanding Fear and Taxonomic Perspectives," Computers & Security, 141, pp. 103826, 2024, Available at: 10.1016/j.cose.2024.103826.

[45] K. Macnish and J. van der Ham, "Ethical Approaches to Cybersecurity," Oxford Handbook of Digital Ethics, Oxford University Press, 2023.

[46] D. A. Adams, R. R. Nelson and P. A. Todd, "Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication", MIS Quarterly, pp. 227-247, 1992.

[47] A. L. Lederer, D. J. Maupin, M. P. Sena and Y. Zhuang, "TAM and the World Wide Web," AMCIS Proceedings, pp. 258, 1997.

[48] M. H. Alhumsi and R. A. Alshaye, "Applying Technology Acceptance Model to Gauge University Students' Perceptions of Using Blackboard in Learning Academic Writing," Knowledge Management & E-Learning, 13(3), pp. 316-333, 2021.

[49] Y. C. Huang, L.L. Chang, C.P. Yu and J. Chen, "Examining an Extended Technology Acceptance Model with Experience Construct on Hotel Consumers' Adoption of Mobile Applications," Journal of Hospitality Marketing & Management, 28(8), pp. 957-980, 2019.

[50] M. Fishbein and I. Ajzen, "The Theory of Reasoned Action as Applied to Moral Behaviour: A Confirmatory Analysis," Addison-Wesley Publishing Company, Reading. MA, 1975.

[51] S. Jeong, S. Kim and S. Lee, "Effects of Perceived Ease of Use and Perceived Usefulness of Technology Acceptance Model on Intention to Continue Using Generative AI: Focusing on the Mediating Effect of Satisfaction and Moderating Effect of Innovation Resistance," International Conference on Conceptual Modeling, Cham: Springer Nature Switzerland, pp. 99-106, 2024.

[52] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology," Journal of Management Science. 35 (8), pp. 982-1003, 1989.

[53] F. D. Davis and A. Granić, "Evolution of TAM," The Technology Acceptance Model. Human–Computer Interaction Series," Cham: Springer, 2024, Available at: https://doi.org/10.1007/978-3-030-45274-2_2.

[54] V. Venkatesh and F. D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," Management Science, 46(2), pp. 186-204, 2000.

[55] V. Venkatesh, M. G. Morris, G. B. Davis and F. D Davis, "User Acceptance of Information Technology: Toward a unified view," MIS Quarterly, pp. 425-478, 2003.

[56] V. Venkatesh, and H. Bala, "Technology acceptance model 3 and a research agenda on interventions," Decision sciences, 39(2), pp. 273-315, 2008.

[57] R. P. Bagozzi, "The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift," Journal of the Association for Information Systems, 8(4), p. 3, 2007.

[58] I. Benbasat, and H. Barki, "Quo vadis TAM?', Journal of the Association for Information Systems," 8(4), p.7, 2007.

[59] P. Legris, J. Ingham, and P. Collerette, "Why do People Use Information Technology? A Critical Review of The Technology Acceptance Model," Information & Management, 40(3), pp. 191-204, 2003.

[60] N. Marangunić and A. Granić, "Technology Acceptance Model: A Literature Review from 1986 to 2013," Universal Access in the Information Society, 14, pp. 81-95, 2015.

[61] A. Y. L. Chong, "Predicting M-Commerce Adoption Determinants: A Neural Network Approach," Expert Systems with Applications, 40(2), pp. 523-530, 2013.

[62] V. Braun and V. Clarke, "Using Thematic Analysis in Psychology", Qualitative Research in Psychology, 3(2), pp. 77–101, 2006.