Int. j. adv. multidisc. res. stud. 2023; 3(1):1782-1785

Received: 03-01-2023
Accepted: 13-02-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Digital Vigilance in the Modern Era: The Role of Cyber Oversight in Digital Marketing Effectiveness and Business Continuity Management

Dr. Emad Ali Kasasbeh
National University College of Technology, Amman, Jordan

DOI: https://doi.org/10.62225/2583049X.2023.3.1.5749
Corresponding Author: **Dr. Emad Ali Kasasbeh**

Abstract
His study aimed to examine the role of digital vigilance in the modern era and its impact on both digital marketing effectiveness and business continuity management, within the context of cyber oversight. The research was conducted on a population of 32 Jordanian pharmaceutical companies, from which a sample of 11 companies was selected, comprising a total of 400 employees. A structured questionnaire was developed as the primary data collection instrument, yielding 388 valid responses for analysis. The collected data were analyzed using SPSS Version 16.
The findings indicated that respondents perceived a high level of digital vigilance in relation to cyber oversight practices. Moreover, the results demonstrated a statistically significant impact of digital vigilance on digital marketing effectiveness, particularly in enhancing customer engagement, data security, and marketing decision-making. In addition, digital vigilance was found to have a significant positive effect on business continuity management, with its dimensions explaining 51% of the variance in business continuity management. The study highlights the critical role of cyber oversight as a strategic enabler that strengthens digital marketing performance while ensuring organizational resilience and continuity in an increasingly digital business environment.

Keywords: Digital Vigilance, Cyber Oversight, Digital Marketing Effectiveness and Business Continuity Management

Introduction

Administrative control represents one of the fundamental and indispensable functions of modern management, serving as a systematic process through which organizations ensure the efficient and effective implementation of their plans in pursuit of predefined objectives. Over time, this function has evolved significantly in response to continuous environmental changes, particularly those driven by rapid technological advancement. Control is no longer limited to traditional supervisory mechanisms; rather, it has become a dynamic and integrated process that safeguards organizational resources, monitors performance, and ensures alignment between strategic intentions and actual outcomes (Coiciu & Militaru, 2024) [3].

In the contemporary digital environment, organizations operate within highly complex and technology-driven ecosystems characterized by accelerated innovation, extensive data exchange, and increasing reliance on digital platforms. These conditions have intensified exposure to cyber risks, operational disruptions, and reputational threats, making digital vigilance and cyber oversight critical components of modern administrative control. Cyber oversight functions as an advanced form of control that enables real-time monitoring, early detection of deviations, and rapid corrective action, thereby transforming control from a reactive practice into a proactive and continuous managerial process. This shift is particularly vital in maintaining operational stability and ensuring business continuity in the face of cyber threats and technological uncertainties. (Makka & Kampova, 2024) [14].

Moreover, as organizations increasingly depend on digital marketing to reach customers, enhance engagement, and sustain competitive advantage, the effectiveness of these digital activities has become closely linked to the robustness of cyber oversight mechanisms. Secure digital infrastructures, accurate data governance, and continuous monitoring contribute not only to protecting organizational assets but also to enhancing trust, service quality, and marketing performance. Consequently, digital vigilance emerges as a strategic necessity that bridges cyber oversight, digital marketing effectiveness, and business continuity management. (Shaffi, 2025) [15].

Based on the above, this study seeks to examine Digital Vigilance in the Modern Era, highlighting the role of cyber oversight as a contemporary control mechanism that supports digital marketing effectiveness while ensuring organizational resilience and continuity in an increasingly complex digital landscape.

Literature Review

Adapting to shifts in the external business environment prompts businesses to proactively address potential threats through strategic planning and effective implementation. Recognizing the importance of this proactive approach, successful management authorities underscore the significance of Business Continuity Management (BCM). Supriadi & Pheng's (2018) research defines BCM as the proactive act and process of mitigating critical incidents through responsive functions and processes to enhance overall business performance through careful planning. The primary objective of BCM is to develop contingency strategies for future emergencies, allowing businesses to respond constructively to changing dynamics without disrupting core activitie Kato & Charoenrat, (2018). Consequently, BCM becomes a collective effort across diverse organizational functions to eliminate uncertainties in operational management. Supriadi & Pheng (2018) note that BCM actively enhances business adaptability to both macro and micro challenges. Initially focused on a structured crisis mitigation plan, the BCM process has evolved from a technological necessity to a strategic requirement, enabling firms to competitively navigate crises or disasters Alharthi & Khalifa, (2019) [1].

Alharthi & Khalifa (2019) [1] emphasize the strategic importance of BCM in ensuring employee safety, maintaining work effectiveness, and safeguarding the business reputation against adverse impacts on outputs. The BCM strategy further guarantees the quality of operations, governance, business strategies, decisions, tools, insurance, legal compliance, and other regulatory considerations, thereby preserving the brand image during vulnerable situations. To achieve these goals, BCM managers emphasize three versatile mindsets: technology, value-based, and auditing Supriadi & Pheng, (2018).

The evolving practices of BCM, as illustrated by Supriadi & Pheng (2018), expand the scope of the approach to minimize the impact of a hostile environment on business performance. The transformation is evident in the shift from a focus on technology to a comprehensive strategy that incorporates value-chain analysis, multi-disciplinary teams, protection measures, flexible structures, prevention tactics, and sustainable advantages, as depicted in the accompanying figure.

In the modern digital era, forward-thinking organizations increasingly recognize the importance of digital vigilance and cyber oversight as essential drivers of effective Business Continuity Management (BCM) and digital marketing performance. (Day and Schoemaker, 2019) [4] highlight that embedding vigilance within organizational operations strengthens continuity planning and enhances risk mitigation capabilities. By leveraging advanced digital tools and technologies, firms are able to sustain growth, reduce operational inefficiencies, and safeguard financial performance. Key digital solutions including e-procurement systems, electronic payment platforms, and corporatewebsites have become central to maintaining operational resilience and ensuring uninterrupted market engagement.

In response to unprecedented challenges, particularly during the pandemic, organizations significantly restructured their business models by adopting digitally innovative frameworks. Technologies such as e-payment and e-procurement enabled contactless transactions, ensuring continuity in consumer product sales and preserving revenue streams. Furthermore, the strategic deployment of digital platforms and websites minimized physical interaction, facilitated direct communication with target audiences, and supported efficient delivery services, thereby enhancing digital marketing effectiveness (Gabriel & Loredana, 2020) [5]. This heightened level of digital vigilance proved instrumental in strengthening BCM during periods of disruption.

Empirical research further emphasizes the relationship between strategic vigilance and BCM effectiveness. (Niemimaa, Järveläinen, Heikkilä and Heikkilä, 2019) demonstrated that BCM serves as a proactive and responsive mechanism for addressing sudden crises, including supply chain disruptions and demand volatility. Effective continuity management relies on clearly defined responsibilities, robust digital communication channels, employee training, and heightened awareness of external cyber and operational risks. Organizations that prioritized Business Continuity Planning (BCP) alongside strategic digital vigilance were better equipped to navigate complex and hazardous environments.

Supporting this view, (Suresh, Sanders, and Braunscheidel, 2020) argued that firms exhibiting strong cyber awareness, contingency planning, and vigilance achieved superior outcomes in BCP implementation. Such organizations demonstrated greater adaptability to environmental disruptions and enhanced their capacity to manage digital and operational risks in real time.

Within supply chain contexts, the integration of digital vigilance and BCM has delivered substantial performance improvements. (Blos, Hoeflich, and Miyagi, 2015) emphasized that aligning BCP with vigilant, technology-driven oversight strengthens supply chain resilience. Organizations adopting this approach followed six critical steps: risk identification, impact analysis, vigilance-based continuity strategy development, plan formulation, testing, and continuous maintenance. These measures resulted in enhanced customer experience, operational flexibility, innovation, efficiency, inventory control, financial stability, revenue growth, service quality, market competitiveness, order cycle efficiency, and delivery performance. Overall, digital vigilance has played a transformative role in reinforcing business continuity and digital marketing effectiveness, enabling organizations to respond swiftly and strategically to evolving external challenges.

Research Methodology

For an effective research, it is imperative to select an appropriate research methodology. An appropriate research design is important to determine the type of data needed, method of collecting the data, and type of sampling technique to apply. Therefore, research design is very crucial to actualize the research objectives. This study applied a quantitative research design. Quantitative research design will enable the researcher to test the relationship between the research variables. It will also enable the

researcher to unvaryingly determine if one concept or idea is better than the others. It can also respond to questions on the relationships that exist among measured variables with the aim of elucidating, envisaging, as well as controlling phenomena (22).

Thus, quantitative research design is an appropriate method for this study since it permits testing the relationship between variables with the use of statistical approaches (22). This is in line with the main objective of this study that focus Thus, quantitative research design is an appropriate method for this study since it permits testing the relationship between variables with the use of statistical approaches.

Population and Sampling

Sekaran (23) defines a research population as the entire group of people, events, or things of interest that the researcher wishes to investigate. The population size of this study consists of (900) mangers, assistant manager, and heads of sections working at departments of Jordanian pharmaceutical companies. The most basic element of a research study is unit of analysis (24). (24) a unit of analysis can be referred as "the level of aggregation of the data collected during the subsequent data analysis stage" while.Therefore, the unit of analysis is individual based, means that data was collected from (mangers, assistant manager, and heads of sections) in Jordanian pharmaceutical companies is the unit of analysis of the study.

This study used probability simple random sampling method. Sampling methods can be divided into probability and non-probability sampling. This study adopts the simple random sampling technique, which is a probability sampling method, in order for each aspect of the population to be represented in the sample (24). Hence, (400) questionnaires were distributed to the sample, ten of them were excluded because they were not filled completely or correctly so (388) questionnaires were valid.

Testing Hypotheses

H0: There is no statistically significant effect of digital vigilance, represented by cyber oversight, on digital marketing effectiveness and business continuity management. at level ($\alpha \leq 0.05$).

To test this hypothesis the researcher uses the multiple regression analysis to ensure the impact of Digital Vigilance: Navigating the Intersection of Cyber Oversight according to (Digital Security, Digital Balance, Privacy Rights) on digital marketing effectiveness and business continuity management shown in Table (1).

Table 1: Stepwise Multiple Regression effect of Digital Vigilance: Navigating the Intersection of Cyber in digital marketing effectiveness and business continuity management.

Order of entry of independent elements in the equation to predict	R^2	(F) Value	T Calculated	Sig
Digital Security	0.533	308.140	7.473	0.000
Digital Balance	0.577	271.822	8.862	0.000
Privacy Rights	0.576	244.824	6.861	0.000

Table 1 shows that the order of entry independent variables in the regression equation, Digital Security has occupied the first place with amount (0.533), while the Effect of Digital Balance was (0.577), while the Effect of Privacy Rights was (0.576), This Explains Reject the Null Hypothesis and accept Alternative Hypothesis. There is significant effect of Digital Vigilance: Navigating the Intersection of Cyber according to (Digital Security, Digital Balance, Privacy Rights on digital marketing effectiveness and business continuity management at level ($\alpha \leq 0.05$).

Conclusions

In today's digital era, the effectiveness of digital marketing is closely tied to the robustness of cyber oversight and business continuity management. The increasing reliance on digital platforms for marketing campaigns makes organizations more vulnerable to cyber threats, which can disrupt not only IT systems but also customer engagement, brand reputation, and overall business performance.

Interconnectedness of Cyber Oversight and Business Continuity in Digital Marketing:

Cybersecurity and business continuity are fundamental to sustaining digital marketing effectiveness. Cyber incidents ranging from data breaches to system outages can directly affect marketing operations, customer trust, and campaign delivery. Organizations must adopt holistic strategies that integrate cyber vigilance with operational resilience, ensuring that marketing processes remain uninterrupted despite evolving threats.

The modern marketing landscape characterized by cloud-based tools, social media platforms, Internet of Things (IoT) integrations, and remote collaboration expands the digital attack surface. Organizations must implement agile cyber oversight and adaptive continuity plans to maintain both operational stability and marketing impact. Compliance with regulatory standards is essential, as it strengthens organizational resilience, protects consumer data, and ensures ethical digital marketing practices.

Human Element and Organizational Awareness:

Employees play a critical role in maintaining cyber vigilance, as insider threats and social engineering remain significant risks. Training programs and awareness initiatives are vital to safeguard both operational continuity and the integrity of marketing campaigns.

Collaboration, Innovation, and Technology:

Sharing cyber threat intelligence within industries enhances collective defense capabilities. Additionally, leveraging advanced technologies such as artificial intelligence and machine learning enables real-time threat detection, faster response, and more secure digital marketing ecosystems.

In conclusion, sustaining digital marketing effectiveness in the modern era requires proactive cyber oversight embedded within comprehensive business continuity management. By integrating security measures, regulatory compliance, employee awareness, and technological innovation, organizations can build resilient digital operations that protect brand reputation, customer trust, and marketing performance against the dynamic landscape of cyber threats.

Recommendations

Enhance Cyber Oversight in Digital Operations: Pharmaceutical companies and organizations should integrate continuous cybersecurity monitoring across all digital platforms, including marketing channels, to protect sensitive data, ensure the continuity of campaigns, and minimize risks associated with evolving cyber threats.

Develop Business Continuity Plans for Digital Marketing: Organizations should establish and regularly update comprehensive business continuity strategies that specifically cover digital marketing operations. This includes rapid recovery protocols to maintain campaign

effectiveness and ensure uninterrupted customer engagement during cyber incidents.

Strengthen Employee Awareness and Training: Regular training programs should be conducted to educate employees about cybersecurity risks, social engineering, and best practices for secure digital marketing. Empowering staff reduces human error, which remains a critical vulnerability in both operational continuity and marketing effectiveness.

Invest in Advanced Technology and Industry Collaboration: Companies should leverage cutting-edge technologies, such as artificial intelligence and machine learning, for early threat detection and rapid response. Additionally, fostering collaboration and sharing cybersecurity intelligence within the industry enhances collective defense and strengthens organizational resilience.

References

1. Alharthi MNAN, Khalifa GS. Business continuity management and crisis leadership: An approach to re-engineer crisis performance within Abu Dhabi Governmental entities. International Journal on Emerging Technologies. 2019; 10:32-40.
2. Blos MF, Hoeflich SL, Miyagi PE. A general supply chain continuity management framework. Procedia Computer Science. 2015; 55:1160-1164.
3. Coiciu I, Militaru G. Improvement of cyber resilience by implementation of a digital Business Continuity Management system: Evidence from Romania. Proceedings of the International Conference on Business Excellence. 2024; 18(1):2492-2505.
4. Day GS, Schoemaker PJ. See sooner, act faster: How vigilant leaders thrive in an era of digital turbulence. MIT Press, 2019.
5. Gabriel D, Loredana D. Using internet as a solution for sales in Covid-19 pandemic: E-Commerce. Annals of DAAAM & Proceedings. 2020; 7(1).
6. Kato M, Charoenrat T. Business continuity management of small and medium sized enterprises: Evidence from Thailand. International Journal of Disaster Risk Reduction. 2018; 27:577-587.
7. Kasasbeh EA. The impact of e-marketing on competitive advantage of Jordanian commercial banks. Journal of Human and Social Sciences. 2020; 9(2):169-191.
8. Kasasbeh EA. The relationship between knowledge-based systems (E-Systems) and competitive advantage. Scientific International (Lahore). 2023; 35(6):791-794.
9. Kasasbeh EA. Analysis of factors influencing consumers' use behavior with mobile banking services in Jordanian commercial banks. Scientific International (Lahore). 2024a; 36(3):355-359.
10. Kasasbeh EA. Analysis effects of e-services quality on customer trust and online shopping: An empirical study on Amazon customers in Jordan. Journal of Al-Hussein Bin Talal University for Research. 2024b; 10(3).
11. Kasasbeh EA, Al-Bloush TB, Alshauaura A. The mediating effect of business intelligence systems on the relationship between supply chain management and customer relationship management. Journal of Intelligence Studies in Business. 2024; 14(1):31-41.
12. Kasasbeh EA, Al-Bloush TB, Alnaser ASM, Shwawreh AM, Alkasassbeh WAK. The impact of marketing innovation on creating value for the brand in Jordanian food industry companies. Pakistan Journal of Life and Social Sciences. 2024; 22(2):20942-20951.
13. Kasasbeh EA, Al-Bloush TB, Abdelaziz GAM. Big data-enabled analysis and its impact on enhancing marketing capabilities: A field study of Islamic banks in Jordan. Scientific International (Lahore). 2024; 36(3):271-276.
14. Makka K, Kampova K. Cyber security and Business Continuity Management: Ensuring resilience in a digital world. Challenges to National Defence in Contemporary Geopolitical Situation. 2024; 1(1).
15. Shaffi SM. Comprehensive digital forensics and risk mitigation strategy for modern enterprises. arXiv, 2025.
16. Supriadi LSR, Pheng LS. Business Continuity Management (BCM). In Business Continuity Management in Construction. Springer, Singapore, 2018a, 41-73.
17. Supriadi LSR, Pheng LS. Business continuity management in construction. Springer, Singapore, 2018b.