Migration Letters

Volume: 20, No: 7, pp. 1145-1156

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

Proposing a new CTPMC Model of Cyber Threat Protection for Marketing Communications during Digital Business Migration

Siti Nor Amalina Ahmad Tajuddin[1], Khairul Azam Bahari[2], Kamaruzzaman Abdul Manan[3], Nur Nadia Abd Mubin[4], Akmar Hayati Ahmad Ghazali[5], Nurul Fadly Habidin[6], Nur Raidah Radzi[7]

Abstract

The relentless march of digitization in today's world has heightened cybersecurity risks, especially within the framework of digital business migration. The sophistication of cyber-attacks further complicates this landscape. In response to these pressing concerns, this present study aims to achieve three main objectives: (1) To discover the knowledge and attitudes of small and medium-sized enterprise (SME) entrepreneurs towards cybersecurity and digital marketing communications; (2) To illuminate the firsthand experiences of SME entrepreneurs in grappling with cybersecurity threats within the realm of digital marketing communications; and (3) develop a new strategic cybersecurity threat protection model in digital marketing communications. A survey was conducted with 501 entrepreneurs, leading to the CTPMC model's development, tailored to defend against cyber threats during digital business migration. This model enriches the discourse on cybersecurity and digital marketing by integrating elements from the National Institute of Standards and Technology (NIST) framework.

Keywords: *Cybersecurity, CTPMC model, marketing communications, digital business migration, SME entrepreneurs.*

Introduction

The digitization of our world intensifies serious repercussions for public security as cybersecurity risks and cyber-attack casualties increase as a result of a growth in the number of wired and wireless connections and devices (Katsantonis et al., 2019). From the marketing communication perspective, it is much more complex in social media than traditional marketing such as print advertisements in newspapers or magazines, commercials on television or radio, billboard ads and brochures. Contemporary marketing efforts are now intricately interwoven with the digital sphere, utilizing websites, social media platforms, YouTube videos, pop-ups, and banner ads as primary conduits for brand promotion and engagement. This migration to digital business marketing channels is driven by the imperative to reach and engage a technologically savvy and digitally connected consumer base. These platforms help to increase sales and lower marketing

[1] Department of Communication and Media, Sultan Idris Education University, Tanjong Malim, Perak, Malaysia, sitinoramalina@fbk.upsi.edu.my
[2] Department of Communication and Media, Sultan Idris Education University, Tanjong Malim, Perak, Malaysia
[3] Department of Communication and Media, Sultan Idris Education University, Tanjong Malim, Perak, Malaysia
[4] Department of Communication and Media, Sultan Idris Education University, Tanjong Malim, Perak, Malaysia
[5] Department of Communication, Faculty of Modern Languages and Communication, Universiti Putra Malaysia, Selangor, Malaysia
[6] Faculty of Management and Economics, Sultan Idris Education University, Tanjong Malim, Perak, Malaysia
[7] INTI International College Penang, Bayan Lepas, Pulau Pinang, Malaysia

costs (Mazzucchelli et al., 2021) in addition to maintaining customer relationships and virally spreading the word about their goods and services (Filiz Bozkurt Bekoglu & Cemre Onaylı, 2016; García-Morales et al., 2022). Although digital marketing communications can be used efficiently to reach wider target audiences and trace return on investment, small and medium-sized enterprises (SMEs) always become primary targets for hackers and ransomware (Filiz Bozkurt Bekoglu & Cemre Onaylı, 2016; García-Morales et al., 2022; Wallang et al., 2022) because they lack cybersecurity-related practices to withstand serious security incidents. Thus, in the context of digital business migration, SMEs are particularly exposed to these cybersecurity challenges, necessitating the development of comprehensive protective measures.

According to a recent study, certain SME characteristics, such as agility, huge cohort sizes, and fragmented IT architecture, may enable a greater cyber-security (Tam et al., 2021). In Malaysia, a recent survey showed that 84 percent of small and medium-sized enterprise companies have been the victim of cyber incidents in the year 2022 due to their size and resources to invest in cyber risk management tools (Malaysia Digital Economy Corporation (MDEC), 2022). They also discovered that 76 percent of SMEs are subject to more than one threat. The main problem with these incidents is that many people believe that they do not know how to protect their online systems or are unaware of the consequences without Internet security protection (Bada & Nurse, 2019). Previous studies on the cybersecurity model are too technical and too difficult for non-techies to understand and apply to the practice. Moreover, cyber-attacks are becoming more sophisticated as cybercriminals continually display deep technical knowledge and new special skills in exploiting technological and social resources (Katsantonis et al., 2019). Without a proper investigation of digital marketing communications and a strategic cybersecurity model, the problem is expected to worsen for small and medium-sized enterprises. As such, we believe that in the year 2024, with many companies and entrepreneurs going for digital marketing communications, there are new cybersecurity issues and challenges yet to be discovered in this current study. To address this gap, this current study aims to:

1) discover the level of SME entrepreneurs' knowledge and attitudes toward cybersecurity and digital marketing communications

2) disclose SME entrepreneurs' experiences with cybersecurity threats in handling digital marketing communications

3) develop a new strategic cybersecurity threat protection model in digital marketing communications

Digital Business Migration

Businesses of all sizes run the very real risk of losing relevance in a society that is obsessed with all things smart, mobile, and ubiquitous if they lack the commitment to invest and the agility to quickly adopt new technologies (Dillon, 2022). With the growth of the Internet and the World Wide Web, technology's function was elevated to that of a facilitator of new modes of operation. This evolution underscores the critical importance of digital business migration as companies navigate this transformative landscape, integrating advanced technologies into their operations to remain pertinent and competitive. As a result, organizations started to build business and technology strategies concurrently, changing the structure of a firm and how it functions, thus inadvertently driving them to adopt a technology-led strategy (Dillon, 2022). The phrase 'digital business' describes companies that run their daily operations using electronic technologies (Vaz, 2021). This can involve carrying out transactions, managing their finances online, and using social media to advertise their goods and services (Vaz, 2021). As more individuals turn to the Internet for product and service purchases, there has been a recent shift towards digital marketing communications, a trend closely associated with the concept of digital business migration.

Thus, the rise of immersive digital marketing communications has profound effects on targeted markets and has the potential to influence mass audiences through increased exposure and repeated consumption of digital messages (Ahmad Tajuddin & Zulkepli, 2019). As such, social media marketing has emerged as one of the most preferred and successful types of digital marketing over the last several years (Dencheva, 2023). Advertising companies have instant access to billions of prospective clients due to the sizable user bases of social media platforms. For example, popular social media platforms such as Facebook, Instagram, WhatsApp, Twitter, and YouTube have initiated a process of transformation of business activities including marketing, promotion, and advertising which affects Internet users greatly and thus forms a fundamental part of consumer behavior and lifestyle (García-Morales et al., 2022). As a result, digital marketing communication led to greater exposure for goods and services, and boosted the brand, among the many benefits of using social media platforms for business purposes, as well as the increased traffic on commercial websites (Dencheva, 2023). This transformation is a key aspect of the ongoing process of digital business migration, where companies leverage digital tools and strategies to optimize their presence and operations.

Nonetheless, it is evident that as businesses expand their consumer base and aim for increased profits, they simultaneously face heightened risks. Consequently, prioritizing cybersecurity emerges as a paramount concern in tackling digital threats, both on an international and regional scale, especially within the context of digital business migration.

Cybersecurity Incidents and Threats

Nowadays, a number of marketers and entrepreneurs around the World are making extensive use of digital marketing communications as explained in the previous section, thus, their security is of paramount importance. Moreover, vital information stored in several databases is in demand by hackers irrespective of the geographic location of a target (Maalem Lahcen et al., 2020; Muango & Shaojian, 2019). As a result, there is an increasing demand for cybersecurity training for people to help protect against this growing threat. New threats arise with the advance of technology, defenses strengthen and attackers adopt new strategies, exploiting previously unknown weaknesses. Thus, the traditional lone hacker is no longer the primary threat to society. Although technical security measures are deployed and security policies are developed for the purpose of digital data protection, in many cases, people fail to follow those specific policies for several reasons either people do not know (or do not perceive) the threats or do not know (or fully understand) the right conduct (Bada & Nurse, 2019). This challenge underscores the need for comprehensive education and training in digital business migration to ensure that individuals are well-informed and aligned with the established security measures. This is especially relevant in the context of digital business migration, where interconnected processes in the manufacturing and distribution of goods depend on robust cybersecurity practices to prevent disruptions. The next section further discusses SMEs and how they are connected to cybersecurity threats.

Small and medium-sized enterprises (SMEs)

Entrepreneurship is a very significant phenomenon in the business world since it is considered the primary engine of the economies in many countries. The term entrepreneur refers to a person who perceives an opportunity and starts a business (venture) to pursue this opportunity (Agusdin, 2018). In a broad definition, an entrepreneur is usually interpreted as an individual capacity to transform concepts into workable new businesses. An entrepreneur from the Malaysian context can be referred to as an independent individual who operates a so-called small business, functions as an employee, and assumes all the risks and rewards offered for sale by a given business enterprise, concept, product, or service (Hashim et al., 2016). Despite the fact that SME entrepreneurs run small businesses, they also reap the opportunities to reach wider potential customers

through digital marketing on the Internet and social media. To be specific, SMEs grow their companies online, which boosts their competitiveness and provides a high level of flexibility in adjusting to the client, multitasking personnel, and a focus on the innovative development of products or services (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023). This dynamic digital expansion aligns with the principles of digital business migration, empowering SMEs to flourish in the ever-evolving digital landscape.

Thus, the current model offers a more vibrant digital marketing communications discourse that disseminates information, perspectives from business or entrepreneurs' insights, and ways to respond to cybersecurity threats that will empower especially small and medium-sized enterprises. The necessity to protect private and confidential data has become ever more critical as small and medium-sized businesses increasingly embrace work-from-home policies, reflecting the ongoing shift in the landscape of digital business migration.

Methodology

The methodology for carrying out this study has been divided into two phases: 1) the investigation of SMEs' knowledge and attitudes of cybersecurity in their digital marketing communications as well as their experience with cyber threats and 2) the development of a new strategic cybersecurity model in digital marketing communications. The first phase of constructing the questionnaire as the research instrument was used to form items relevant to the sample of the study, gather data, and explore SMEs' perceived usefulness and perceived ease of use of digital business and cyber security. This questionnaire has been adopted from several past studies (Filiz Bozkurt Bekoglu & Cemre Onaylı, 2016; Pham et al., 2021; Zwilling et al., 2020) and revised according to the Malaysian context.

Part A of the questionnaire items are questions related to the demographic characteristics of the SMEs consisting of gender, age, residence, level of education, income, business size, types of business, and years of business operation. Section B related to items asking about SME entrepreneurs' knowledge of digital marketing communications and cyber security. In this section, the 5-Likert scale that was adopted was: Not know at all (1), Know little (2), Probably Know (3), Know (4), and Absolutely Know (5). Furthermore, in section C, the items that have been constructed are related to SME entrepreneurs' attitudes toward digital marketing communications and cyber security. These items used the 5-Likert scale of: Not very useful (1), Not useful (2), Slightly useful (3), Useful (4), and Very useful (5). The last section (Section D) asks questions on SMEs' experience with cyber threats using the 5-Likert scale, including Never (1), Seldom (2), Sometimes (3), Often (4), and Always (5).

Out of the numerous questionnaires distributed to SME entrepreneurs using several approaches with the help of research enumerators via an online platform, only 501 SME entrepreneurs responded to the questionnaires. As mentioned earlier, our samples were among entrepreneurs of small and medium enterprises. We distributed the questionnaire randomly to SME entrepreneurs from the four states namely Kedah, Perak, Selangor and Melaka. We used systematic random sampling through a database of business operations obtained from the Companies Commission of Malaysia (SSM) to distribute to respondents. The questionnaire was distributed between May and August 2022 where the profile of the respondents included age, gender, academic level, marital status, monthly income, SME ownership status, type of business, business category, and years of operation. This study utilized quantitative data analysis, and a large part of the study's findings are based on quantitative data. The statistical package for social sciences (SPSS) version 29.0 for macOS was used to conduct the analysis. Using SPSS, the data were unpacked and then summarized.

In the second phase, a new strategic cybersecurity model in digital marketing communications has been developed by incorporating several aspects from the previous National Institute of Standards and Technology (NIST) cybersecurity framework. The core structure of the framework serves five functions: Identify, Protect, Detect, Respond, and Recover (National Institute of Standards And Technology, 2018) as demonstrated in Figure 1. By establishing best practices, standards, and recommendations, the NIST cybersecurity framework (CSF) assists organizations in enhancing their cyber-security measures and offers an integrated organizing structure for various approaches to cybersecurity. In other words, this framework offers a way to define cybersecurity requirements which might be useful in identifying gaps in an organization's cybersecurity practices (Taherdoost, 2022).

Figure 1. NIST Cybersecurity Framework (Source: NIST, 2018)

The model was developed by six experts and each of them has contributed to the clarity of the model. While developing the model, the findings received from SME entrepreneurs concerning their experiences with cybersecurity threats for handling digital marketing in their businesses were taken into consideration. A three-day workshop was conducted lasting approximately twenty hours to analyze pertinent data and further develop the new model. The model was later refined by the designer, and the two model designs were prepared for the final selection. The final model was selected based on the usability and applicability of the model. The development and design of the model were carried out by six members of the research project who are experts in this area of study. Once the model has been developed, it has been submitted to the Intellectual Property Corporation of Malaysia (MyIPO) for getting copyright of this model. This model has been granted with the copyright under the registration number LY2022C04270.

Human Research Ethics

The research was carried out in compliance with the principles of human research ethics as well as the best scientific practices following universal research ethics (Msoroka & Amundsen, 2018). Prior to participating in the study, our research associates received written informed consent from all individuals. The meaning, purpose, and method of the study and the handling of the obtained data were all explained to all student participants. The surveys were fully voluntary, and participants could drop out at any time. Pseudonyms were used for all personal identification. Researchers are responsible for ensuring that participants are protected from any physical, mental, or social harm that may arise as a result of the research, as well as predicting any potential negative outcomes. Adhering to the ethical principle of conducting research, we also acknowledge our main reference to the National Institute of Standards and Technology (NIST) cybersecurity framework for developing a new strategic cybersecurity model in digital marketing communications. The new model also incorporated SME entrepreneurs'

responses toward the aforementioned knowledge of marketing communications and cybersecurity as well as their experiences with cyber threats.

Results and Discussions

The main purpose of this study was to develop a new strategic cybersecurity threat protection model in digital marketing communications. In order to measure SME entrepreneurs' level of knowledge and attitudes towards cyber security in their digital marketing communications, as well as their experience with cyber threats, the analyzed data are presented in the form of descriptive and percentage statistics.

Table 1. Participant's gender

Gender	Frequency	Percent	Valid percent
Male	192	38.3	38.3
Female	309	61.7	61.7
Total	501	100.0	100.0

A total of 501 entrepreneurs took part in this study involving 61.7% of females and 38.3% of males from the four states (Kedah, Perak, Selangor and Melaka) as shown in Table 1.

Table 2. Level of entrepreneurs' knowledge and attitude

Variables	N	Mean	St. Deviation
Knowledge of digital marketing	501	43.9	7.87
Knowledge of cyber security	501	44.7	7.20
Attitudes towards digital marketing	501	41.5	4.92
Attitudes towards cyber security	501	49.0	10.52
Total	501		

Table 2 presents the findings related to the first research question, which aimed to assess the level of SME entrepreneurs' knowledge and attitudes toward cybersecurity and digital marketing communications.

For entrepreneurs' knowledge, the mean knowledge score in digital marketing was 44.7 (SD = 7.87), while in cybersecurity, it was slightly lower at 43.9 (SD = 7.20). This suggests that, on average, participants in the study demonstrated a slightly higher level of knowledge in digital marketing compared to cybersecurity. The standard deviation values indicate the variability in knowledge scores within each domain, with digital marketing showing slightly greater variability compared to cybersecurity.

In terms of entrepreneurs' attitudes, participants had a mean attitude score of 41.5 (SD = 4.9) toward digital marketing, whereas their attitude score toward cybersecurity was notably higher at 49.0 (SD = 10.5). This indicates that, on average, participants held a more positive attitude toward cybersecurity than toward digital marketing. The standard deviation values reflect the spread or variability of attitudes within each domain, with cybersecurity exhibiting higher variability compared to digital marketing.

These findings provide insights into the knowledge and attitudes of SME entrepreneurs regarding cybersecurity and digital marketing communications, addressing the first study objective.

Table 3. Entrepreneurs' experience with cyber threats

Activities	Never (%)	Seldom (%)	Sometimes (%)	Often (%)	Always (%)
Experiencing difficulties in handling social media due to hacking.	32.5	4.6	14.6	13.4	34.9
Dealing with customers who are frauds or known as scammers.	24.4	3.0	14.0	16.8	41.9
Suffered considerable losses due to being hacked by cyber hackers.	36.3	3.6	12.0	11.4	36.7
Spending money to recover inaccessible data.	38.5	2.4	12.2	9.6	37.3
Getting threatened by hackers to comply with their demands so that the system can be used.	36.1	5.4	9.4	12.2	36.9
Get a virus that cripples a computer system.	30.1	8.4	11.4	10.4	39.7
Receive emails to enter personal details to websites created by hackers.	25.0	5.2	11.8	15.8	42.3
Experience online bank account hacking attempts.	32.3	10.2	10.4	12.6	34.5

The findings in Table 3 shed light on entrepreneurs' experiences with cyber threats, revealing a diverse landscape of major challenges:

1. Dealing with Fraudulent Customers: Dealing with customers who are fraudulent or scammers is a common occurrence, with almost half of entrepreneurs (41.9%) reporting that they always encounter such individuals. Conversely, 24.4% of them have never had to deal with scammers. This underscores the need for vigilance in customer interactions to mitigate potential risks.

2. Computer System Viruses: Experiencing a virus that cripples a computer system is common among entrepreneurs, with more than one-third (39.7%) always facing this issue. Nevertheless, 30.1% have never encountered such incidents.

3. Emails for Personal Details: Almost half of entrepreneurs (42.3%) have received emails requesting personal details for websites created by hackers. However, one-fourth (25.0%) have never experienced this situation.

These findings underscore the multifaceted nature of cyber threats faced by entrepreneurs, with varying degrees of occurrence and severity, thus answering the second study objective. To address these challenges and protect business interests in the digital age, it is imperative to prioritize cybersecurity measures and enhance knowledge among entrepreneurs.

Model Development – Cyber Threat Protection for Marketing Communications (CTPMC) Model

Developing a new model for combating cyber threats is a complex and multifaceted process that involves various academic disciplines and methodologies. The process begins with a thorough review of existing literature to understand the current state of cyber threats and cybersecurity measures. This step helps researchers identify gaps and

areas where a new model could be beneficial for businesses. Next, collaboration with subject matter experts (digital marketing, lean technology, business and cyber security) in the field is crucial. Surveys and workshops help gather domain-specific knowledge about the challenges and evolving cyber threats prior to developing this model. As the new cyber threat protection model relies on data, researchers need access to large datasets of cyber incidents, attacks, and vulnerabilities. The model development aims to achieve the last study objective of developing a new strategic cybersecurity threat protection model in digital marketing communications, emphasizing the pivotal role of data and reflecting the broader context of digital business migration.

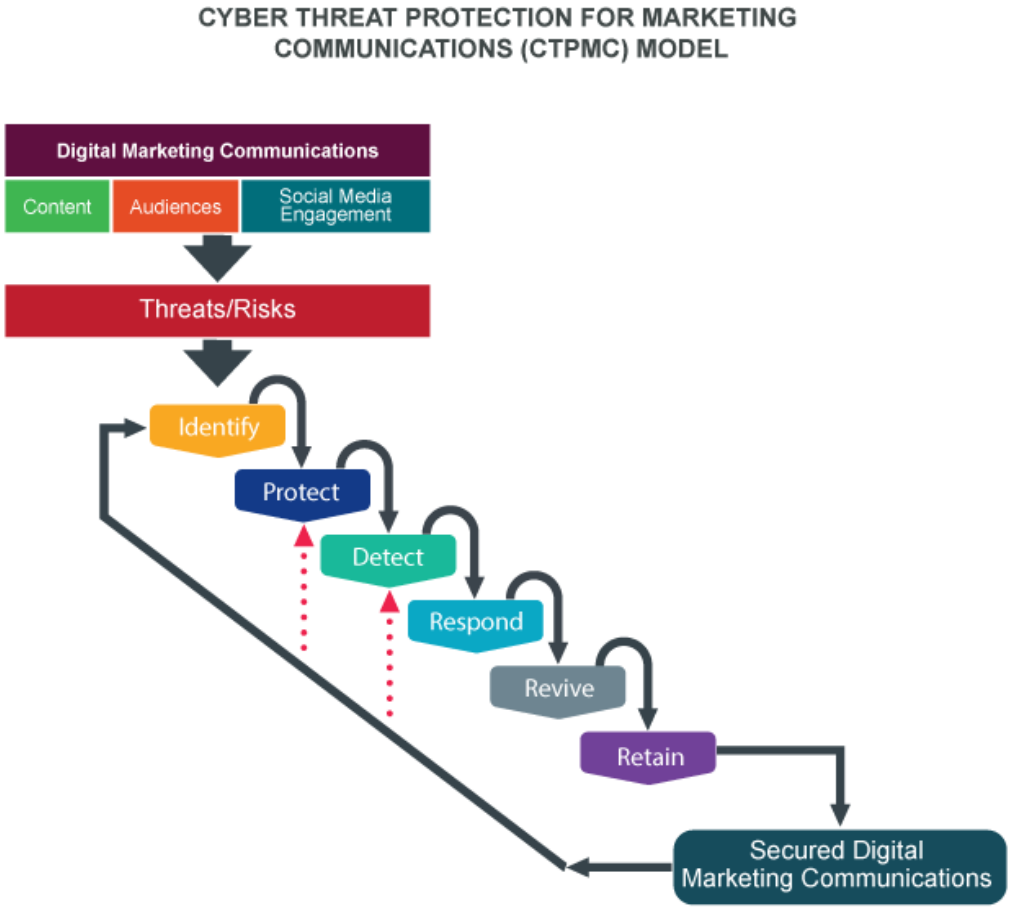

Figure 2. A research-based model of the Cyber Threat Protection for Marketing Communications (CTPMC) model

The new Cyber Threat Protection for Marketing Communications (CTPMC) model is a framework designed to enhance cybersecurity measures and safeguard digital enterprises. This model addresses the evolving landscape of cyber threats in the context of marketing communications, offering a strategic approach to mitigate risks and protect digital business interests which is further explained in Table 4.

Table 4. Elements of the Cyber Threat Protection for Marketing Communications (CTPMC) model

No.	Elements of CTPMC Model	Descriptions
1	Content	Content marketing is strategically designed for users, not just for consumption, but also for social media sharing across various digital platforms (du Plessis, 2022) to stimulate profitable customer engagement in delivering pertinent and beneficial content to potential customers and existing clients (Content Marketing Institute, 2018).
2	Audiences	In the context of social media marketing, the term 'audience' refers to the group of individuals or users who follow, engage with, and consume the content created and shared by a brand or organization on social media platforms (Santos et al., 2023).
3	Social Media Engagement	Social media platforms have transformed the bilateral communication that empowers users to engage in actions such as commenting, reviewing, creating and sharing content, thereby fostering direct interactions with brands and facilitating collaborative content creation (Trunfio & Rossi, 2021).
4	Threat/ Risks	Cyber threats refer to any intentional and unauthorized actions or activities, often originating from malicious actors or entities, with the intent to exploit vulnerabilities or weaknesses in digital systems, networks, or data, thereby posing risks to the security and functionality of these assets (NIST, 2018).
5	Identify	In order to manage cyber security threats, it is necessary to first identifying the critical assets of a business, their interdependencies, and risks (potential threats or vulnerabilities that can harm or compromise the critical assets and system) (Blum, 2020).
6	Protect	Security measures, including but not limited to firewalls, antivirus software, robust password policies, encryption, and similar safeguards, constitute essential elements for achieving success in protecting digital assets (Wallang et al., 2022).
7	Detect	The necessary actions to notice the occurrence of an information security problem are known as detection.

		The ‘detect’ function serves the essential purpose of promptly identifying cybersecurity incidents through the execution of suitable procedures designed to recognize their unfolding (Kaur et al., 2023).
8	Respond	This function is important for developing and implementing the appropriate activities to act regarding a detected cybersecurity event (National Institute of Standards And Technology, 2018).
9	Revive	The implementation of lessons learned is required when recovery strategies are put into practice during incidents. To quickly restore any capacity or services that have been compromised as a result of a cybersecurity event, revive includes all essential efforts and recovery techniques. (National Institute of Standards And Technology, 2018).
10	Retain	Keeping context information accurate, up to date, and accessible is pivotal for the efficacy of security surveillance (Blum, 2020). What kind of information is stored, how long it is stored, whether it is stored online or offline, and whether the data is confidential are some important factors to look into.
11	Secured Digital Marketing Communications	How should people secure their businesses? The best call to action is end-to-end encryption and this model provides guarantees to address security concerns for businesses venturing digital marketing.

Conclusion

The pressing need to safeguard businesses from cyber threats arises from the growing demands placed on them to embrace technology. This pressure emanates from various sources, including the rising attractiveness of businesses as targets for hackers, evolving customer expectations, and global events. Our developed model, based on a combination of research and insights from entrepreneurs, contributes significantly to the pursuit of cybersecurity, particularly for small and medium-sized enterprises (SMEs). This contribution becomes especially pronounced in the context of digital business migration, where businesses are navigating the transition to technology-driven operations. By conducting this study of digital marketing communication and cybersecurity, we could enhance our comprehension of the cybersecurity requirements and vulnerabilities specific to SME businesses. This improved understanding can contribute to the development of more resilient small enterprises. This improved understanding can pave the way for the creation of cybersecurity solutions that are customized to the unique needs of small businesses, rather than expecting them to adapt to existing cybersecurity frameworks that are more technical in nature. Notably, such an approach benefits not only small businesses but also the wider industry, government, and society as a whole (Tam et al., 2021). More importantly, it helps mitigate the yearly increasing number of cyber

incidents and thus protect people's businesses. This aligns with the ongoing process of digital business migration as businesses integrate technology and digital strategies into their operations.

Acknowledgments: This is a study that has been carried out as part of the Fundamental Research Grants Scheme with the grant code (FRGS/1/2020/SS0/UPSI/02/5) funded by the Ministry of Education, Malaysia. The authors would like to express their appreciation to Universiti Pendidikan Sultan Idris for their help in managing the grant. Moreover, the authors sincerely acknowledge the Intellectual Property Corporation of Malaysia (MyIPO) for granting them the copyright of this model under the registration number (LY2022C04270).

References

Agusdin, A. (2018). Contribution of Creative Tourism to Entrepreneurship. In M. Sotiriadis (Ed.), The Emerald Handbook of Entrepreneurship in Tourism, Travel and Hospitality Skills for Successful Ventures (pp. 387–401). Emerald Group Publishing Ltd.

Ahmad Tajuddin, S. N. A. S. N. A., & Zulkepli, N. (2019). An investigation of the use of language, social identity and multicultural values for nation-building in Malaysian outdoor advertising. Social Sciences, 8(1), 18. https://doi.org/10.3390/socsci8010018

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Blum, D. (2020). Rational Cybersecurity for Business. In Rational Cybersecurity for Business. https://doi.org/10.1007/978-1-4842-5952-8

Content Marketing Institute. (2018). What Is Content Marketing? Content Marketing Institute. https://contentmarketinginstitute.com/what-is-content-marketing/

Dencheva, V. (2023). Social media platforms used by marketers worldwide 2022. Statistica.

Dillon, S. (2022). The future of digital business. Why all businesses need a digital technology strategy. https://www.management.ac.nz/about/subject-areas/digital-business/the-future-of-digital-business

du Plessis, C. (2022). A Scoping Review of the Effect of Content Marketing on Online Consumer Behavior. SAGE Open, 12(2). https://doi.org/10.1177/21582440221093042

Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2023). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. Enterprise Information Systems, 17(3), 1–27. https://doi.org/10.1080/17517575.2021.1942997

Filiz Bozkurt Bekoglu, & Cemre Onaylı. (2016). Strategic Approach in Social Media Marketing and a Study on Successful Facebook Cases. European Scientific Journal, ESJ, 12(7), 261–274. https://doi.org/https://doi.org/10.19044/esj.2016.v12n7p261

García-Morales, V., Garrido-Moreno, A., Martín-Rojas, R., & Lockett, N. (2022). Entrepreneurship and Digital Transformation: Managing Disruptive Innovation in a Changing Environment. In V. J. G. Morales, A. Garrido-Moreno, N. Lockett, & R. Martín-Rojas (Eds.), Frontiers in Psychology. Frontiers Media SA. https://doi.org/10.3389/978-2-88971-439-1

Hashim, N. A., Nor, S. M., & Janor, H. (2016). Riding the waves of social commerce: An empirical study of Malaysian entrepreneurs. Geografia: Malaysian Journal of Society & Space, 12(2), 83–94.

Katsantonis, N. M., Kotini, I., Fouliras, P., & Mavridis, I. (2019). Conceptual framework for developing cyber security serious games. IEEE Global Engineering Education Conference, EDUCON, April-2019(June), 872–881. https://doi.org/10.1109/EDUCON.2019.8725061

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97(April). https://doi.org/10.1016/j.inffus.2023.101804

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(10), 1–18. https://doi.org/10.1186/s42400-020-00050-w

Malaysia Digital Economy Corporation (MDEC). (2022). Simple & smarter with matrix cybersecurity for SMEs.

Mazzucchelli, A., Chierici, R., Di Gregorio, A., & Chiacchierini, C. (2021). Is Facebook an effective tool to access foreign markets? Evidence from international export performance of fashion firms. Journal of Management and Governance, 25(4), 1107–1144. https://doi.org/10.1007/s10997-021-09572-y

Msoroka, M. S., & Amundsen, D. (2018). One size fits not quite all: Universal research ethics with diversity. Research Ethics, 14(3), 1–17. https://doi.org/10.1177/1747016117739939

Muango, C. O., & Shaojian, Q. (2019). Tackling cyber threats: cybersecurity model for developing countries. International Journal of Computer Science and Information Security, 17(4), 177–194.

National Institute of Standards And Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2018). NIST Releases Version 1.1 of its Popular Cybersecurity Framework. National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Pham, H. C., Ulhaq, I., Nguyen, M. N., & Nkhoma, M. (2021). An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice. Australasian Journal of Information Systems, 25(2017), 1–23. https://doi.org/10.3127/ajis.v25i0.2177

Santos, S., Gonçalves, H. M., & Teles, M. (2023). Social media engagement and real-time marketing: Using net-effects and set-theoretic approaches to understand audience and content-related effects. Psychology and Marketing, 40(3), 497–515. https://doi.org/10.1002/mar.21756

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics (Switzerland), 11(14). https://doi.org/10.3390/electronics11142181

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. In Computers and Security (Vol. 109, p. 102385). Elsevier Advanced Technology. https://doi.org/10.1016/j.cose.2021.102385

Trunfio, M., & Rossi, S. (2021). Conceptualising and measuring social media engagement: A systematic literature review. Italian Journal of Marketing, 2021(3), 267–292. https://doi.org/10.1007/s43039-021-00035-8

Vaz, N. (2021). Digital Business Transformation How Established Companies Sustain Competitive Advantage From Now to Next. Wiley.

Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022). Cyber security in Small and Medium Enterprises (SMEs): What's good or bad? Journal of Governance and Development (JGD), 18(1), 75–87. https://doi.org/10.32890/jgd2022.18.1.5

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 1–17. https://doi.org/10.1080/08874417.2020.1712269