Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://akademiabaru.com/submit/index.php/arca/index
ISSN: 2462-1927

The Preliminary Result of Technology Digital Branding Practices in Malaysian Cyberspace

Rohana Mijan[1,*], Noor Aziah Abdullah[1], Norsiah Abdul Hamid[1]

[1] Department of Media Technology, Universiti Utara Malaysia, Kedah, Malaysia

ARTICLE INFO

Article history:
Received 6 October 2022
Received in revised form 12 December 2022
Accepted 19 February 2023
Available online 20 March 2023

Keywords:
Digital branding; cybersecurity; technology; Grand Strategy Model

ABSTRACT

The transition from analogue to technology digital greatly influences advertisers to transform branding strategy to digital applications and styles. The digital revolution had promised great opportunities for industries and businesses, yet great challenges too. The advertiser's enthusiastic has triggered many decks of consequences, intruding individual privacy as worst could extend beyond the country's privileges and sovereignty. This enthusiasm has risen the curve to more than 5000 cases during Movement Control Order of pandemic Covid-19 in Malaysia. Without proper guidance, these invisible threats could contagious seriously. Therefore, the objective of the study is to identify the secure strategy adopted by the company and policymakers in refrain from the risks. The preliminary data has shown two themes were presented, which is humanity and technical. These themes become a secure strategy for both parties. The parallel alignment of the secure strategy will be a marching trajectory underlying the privileged of humankind to pace the continuity of pragmatic practice toward the digital age. This study contributes to creating awareness and provide a comprehensive understanding of secure digital branding practices. It is among the first to respond to the calls for empirical research on digital branding with and cybersecurity policy.

1. Introduction

Digitisation and globalisation have increased competition, which in turn, businesses to find new ways to distinguish themselves in the market [3,12]. Digital branding now becomes in the track of the brand development strategy that emphasises on digital media such as Facebook, Twitter, YouTube, Pinterest and relevance. So, the transformation of marketing is underway as the sales number rely upon the fingertips.

For the company, the old way of doing business is unsustainable. Thus, this transition has inspired them to utilise the opportunity, leverage the brand cross boundaries to build consumers engagements in meaningfully. As they were also updating skills to make the most of these fast-moving and highly relevant campaign through digital to ensure it worked across social media, display advertising and e-commerce.

* *Corresponding author.*
E-mail address: rohana.mijan@uum.edu.my (Rohana Mijan)

Despite the beauty of digital branding, the advertisers' compelling narratives and creativity have invited the invisible threats unnoticedly due to the lack of knowledge and awareness on cybersecurity surveillances which is the precaution steps of cyberspace's protection and its engagement. Advertisers often forget crucial steps in developing a brand in the digital environment. The digital environment has its characteristics and dynamics that have to be understood to be able to select effective branding tactics and strategies [3]. This is because, without a thorough knowledge of secure digital branding practices and cybersecurity strategies, the company keep exploring the possibilities to achieve their marketing targets, includes Malaysia.

In Malaysia, the cybersecurity cases curve has increased in 2020 especially during Movement Control Order (MCO) that is triggered the company to utilise digital media maximumly in their daily transaction to maintain the sales, unaware of the adverse effects on the contrary [15]. Even though the National Cyber Security Strategy recently launched in 2019 was to curb international threats [13], yet this strategy is still in pre-test stages as many elements need to improvise parallel with the changing of cybersecurity landscapes.

Precisely, the exploring of the research on digital branding still in its infancy [3,5]. A majority of the available studies are on digital marketing where branding act as a small part in the research. In Malaysia, researchers are more focused on the fundamental of digital issues such the importance and role to economic development; and surveillances. Despite the understanding on the importance of digital practices in business increased, a recent literature review on digital branding reveals the topic is still nascent and fragmented. Therefore, it is imperative to explore the possibility of opportunity in living with emerging technology in the digital era without overshadowed by pessimistic action by revealing sufficient knowledge for the company. The exposure of digital in business practices are significant as it is capable of interacting with the audience countlessly, results are to a great extent easy to measure, reasonably cheap and rapid way to, the broader consumer reaches and ability to go viral.

Studies regarding the main strategy of the company and country commonly employ the Grand Strategy Model (GSM) as it has been extended to describe a multi-tiered strategy in general, including strategic thinking at the level of corporations and political parties [10]. In business, a grand strategy referred to a comprehensive general plan of major actions through which a firm intends to achieve its long-term objectives.

It can be customised for a specific company aim includes concentration, market development, product development and innovation. Grand strategy is suitable for the study of cyber policy because it can provide a framework on how prevailing policy strategy fits into related issues [10] such as digital branding strategy with a cybersecurity strategy.

Against this background, research has been silent in revealing the secured digital branding strategies and cybersecurity strategy to defence threats in encouraging the conducive business environment to drive secured digital branding practices. These findings elucidate a pragmatic approach for the company and policymaker in enduring the safe digital environment for economic development.

To this end, we review the relevant literature concerning digital branding and cybersecurity, as well as contemporary theories surrounding digital issues. A discussion of the methodology, following methods of analysis and presentation of the preliminary result. The sequel, we discuss the meaning of these results and conclude it.

2. The Scenario of Digital Branding in Malaysian Cyberspace

The revolution of Internet use has brought a massive impact in everyday life, especially to businesses. In Malaysia, a total of 28.7 million Internet users, equivalent to 87.4 per cent in 2018 compared to 76.9 per cent in 2016. Duration daily use of the Internet is a maximum of 1-4 hours a day, and the majority of users are youths between the ages of 20-30. A smartphone is a top medium of surfing Internet, especially Facebook, with 97.3 per cent and WhatsApp with 98.1 per cent [15]. The data reflected the engagement of Malaysian on digital media is high as well as the focus to enhance business performance through digital media is increasing curving. it revealed more than 42 per cent of businesses were conducted online globally in 2017. In Malaysia, even though only 16.9 per cent users fully utilised Internet for selling goods or service yet the activities from the consumer are merrier as the other online activities involved communication via text, visit social networking platform, to get information and work related to interest.

The underpinning result was reflected from the initiative of digital economy fostering by the government. The digital economy has been proposed to boost and improve the economy to the advance level. Malaysia's digital economy is set to contribute 20 per cent of the Nation's GDP in the year 2020, more than 18.2 per cent in 2016. To support it, Malaysia has set up a digital free trade zone (DFTZ) located near the Kuala Lumpur International Airport (KLIA). This free trade zone will serve as a regional e-fulfilment centre as well as a one-stop local centre for small medium enterprises (SMEs), marketplaces and mono brands [9].

The adoption of digital technology becomes critical to boosting the competitiveness and growth; and development of companies. Equally, the shifting from traditional marketing to digital is essential as it is offered less resource-consuming such as time, financial, human resources and so on. The passion of the entrepreneur to be a keyboard warrior to position brand with the lack of awareness among Malaysians on the impact of the Internet is used without precaution would invite invisible threats.

The company face an unauthorised use and attacks which are malicious such as theft, destruction of intellectual property, abuse by insiders and illegal use of information which tantamount to a loss of data reliability and confidentiality [6]. Internet scams are becoming more common, especially during pandemic Covid-19. Employment without knowledge has elevated the cybercrime cases. The risk is very high if the focus is only on the development of digital technology without increasing the protection of the technology itself as digital branding is pervasive, boundless and engaging in nature.

Urge of the technological advancement of technology and the capabilities of its protection system has pointed out by the ministry in tandem to counteract the attacks and threats to the technology. The National Cyber Security Agency (NACSA) subordinate under the National Security Council has the authority to bring the cybersecurity issues in action. In assistance, the Prime Minister's Department also adopted the Malaysian Communications and Multimedia Act 1998, Defamation Act 1957 and the Sedition Act 1948 to monitor the cyber activities that could threaten national security. NCSA will be the sole agency in coordinating all agencies managing cybersecurity threats by assigning cybersecurity expertise under one parent agency. Such coordination enables national cybersecurity monitored thoroughly and effectively [4,15].

The government also allocated the RM1 billion in 2018 on the digital fields through the implementation of the National Fiberisation and Connectivity Plan (NFCP) to promote the digital economy. This agenda also called corporation such as Celcom and Axiata to channel RM150 million financial assistance indoor to accelerate digital adoption across Malaysian SMEs delivers to the embrace the digital economy policy.

Such agency like the Malaysian Communication and Multimedia Commission (MCMC), Cybersecurity Malaysia (CSM), Majlis Keselamatan Negara, Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), NACSA and academicians in the area of specialisation of computing and networking work hard towards a trusted digital economy and a safer cybersecurity environment in Malaysia. They are succeeding, but there is a need to do more, especially in deterrence and rapid response in case of any attacks.

At the same time, SMEs Corporation Malaysia works together to promote awareness to entrepreneur and spur the spirit of digitalisation in their businesses. The independent coordination of policymaker, academicians, entrepreneur and users in promoting and adopting the digital pace play a vital role to continue leading the safe paths for the Malaysian economic development.

2.1 Theoretical Framework: Theory Grand Strategy

The concept of grand strategy has been extended to describe a multi-tiered strategy in general, including strategic thinking at the level of corporations and political parties [14]. Generally, grand strategy refers to the collection of plans and policies that comprise the state's deliberate effort to harness economic tools together to advance that state's national interest. Grand strategy is the art of reconciling ends and means. It involves purposive action — what leaders think and want. It is elaborated on how the world works and what is or ought to be their states' roles in that world. It is embodied in policy and practice: government action and reaction in response to real threats and opportunities. Grand strategy lends itself to vigorous interpretive academic debates, yet it is so realistic that practitioners, current and former, can and must contribute for it to be correctly understood. Grand strategy is a useful way of a blending of real-world experience of the practitioner.

In business, a grand strategy is a general term for a broad statement of strategic action. A grand strategy states the means that will be used to achieve long-term objectives. Examples of grand business strategies that can be customised for a specific company include concentration, market development, product development and innovation (www.wikipedia.com). Grand strategy is essential for the study of cyber policy because it can provide a framework on how prevailing policy strategy fits into related issues [10] such as digital branding strategy with a cybersecurity strategy. This model will be projected as a trajectory of strategic planning for secured digital towards cybersecurity policy.

3. Methodology

The qualitative research enables and empowers the researcher to uncover and understand what goes on behind any of the lesser-known scenario or circumstances specific issues. For this study, unstructured in-depth interview and content analysis [1] will be utilised to answer the research questions. The interview question focuses on digital branding and cybersecurity strategy. The face-to-face interviews conducted with a mutual agreement by two policymakers from Cybersecurity Malaysia labelled as informant 1 and 2 in data analysis; informant from academicians' expertise in law and media marked as informant 2 and 3.

As mentioned by Lipiäinen and Karjaluoto [3] digital development has now been ongoing for some time, and it is the right time to slow down and learn from those who have been able to harness digitisation successfully. Document analysis will be a governmental document, annual report, acts, marketing plan and business development paperwork.

Qualitative data analysis uses unstructured measurement in line with the qualitative studies techniques untypically rigid on data analysis as long as it provides a systematic and complete set to ensure data been analysed thematically and consistently [1,7]. Therefore, researchers refer to coding tables supported by NVIVO software to explore key themes, sub-themes and categories such as digital branding and cybersecurity strategies justified with the reasons, the factors and the impact of the theme described by the informant.

4. Results and Discussion

This analysis is based on the objective of the study which to identify the secured digital branding strategies and cybersecurity strategy for policymakers and company. The preliminary data had shown that the main strategy for digital branding is humanity and technical.

According to the respondent:

Humanity is one of the defence strategies. Through behaviour, we can confront digital anonymous. Users were responsible for vulnerability.

(Informant 1)

Trust is credence in dealing with the online transaction. If you doubt on pop-up, information, seller, then don't buy it. Don't click it…

(Informant 3)

We have the brand manual on how to do digital branding. Brand identity and its relationship is the main element in digital branding…

(Informant 2)

Respondent highlighted trust is an important spark to start branding. Data has also shown that technology is a part of the essential strategy to defence the threats. Respondent said:

Generally, we can't control businesses from selling and purchasing; e-commerce; information grazing, *but we tried to filter and screening, blocked the potential threats that could harm them.*

(Informant 1)

Another respondent supports it:

Toward these issues, we have planned to bring out the national security upward by gathering the technical expertise to formulate the umbrella strategy for country and region as it becomes the prior agenda in this digital era.

(Informant 4)

As followed,

We controlled the space by imposed the penalty to cybercrime. The Malaysian Communications and Multimedia Commission Act (1998) still relevant regulator for the communications and multimedia industry in Malaysia.

(Informant 3)

According to the respondent, there are preferably controlled the technical advances and law enforcement rather than controlling the keyboard of unknown and anonymous users. The duality themes presented is an umbrella strategy for parties [8].

In digital branding, trust is a significant predictor in the humanity aspects,). Consumers may turn to trusted and trustworthy brands as an indication in online. Even more, it was suggested that humanity trust leading the laws on digital trust and cybersecurity to minimise the risk and to prepare for future unforeseen. Besides, the technicality advances, also the central concern of cybersecurity strategy that could protect cyberspace. there is a call for improvising the secured cyberspace improvement in Malaysia. To be protected, the initiative should be channelled consistently as a threat is emerging and continuously existing [2,8].

5. Conclusion

As consumers become savvy about the Internet, the digital revolution has taken place the companies' approaches to handling consumers. The passion for digital branding has tended to look at the practical resource usages and profit, while overlooked the activities would trigger invisible threats. In reviewing the findings, it is essential to highlight that while the company eager to explore the hidden opportunity of the digital aura, the success of such eagerness partly depends on company surveillance to face the realities of the boundless market and ultimately from extensive exposure from the government initiatives. With the countless of a new tactic of cybercrimes, advancement in Internet applications and variations of a medium in social media that offered the opportunity to explore the hidden market, yet it delegates a new potential threat to the company and Malaysian cybersecurity, massive amendment in Acts should be taken seriously to prevent it concerning the development of businesses in Malaysia.

Acknowledgement

This article paycheck to the Fundamental Research Grant Scheme for Racer. Warmest acknowledgements to UUM to grant research on The Exploration of Link Between Digital Branding Strategy with Malaysia Cyber Security Strategy: A Development of Grand Strategy Model, S/O code: 14438.

References

[1] Creswell, John W., and Cheryl N. Poth. Qualitative inquiry and research design: Choosing among five approaches. Sage publications, 2016.

[2] Gohwong, Srirath Goi. "The Cyber-attacks and digital economy in Malaysia during 1997-2016." PSAKU International Journal of Interdisciplinary Research (PSAKUIJIR) Vol 5 (2016). https://doi.org/10.12778/235108618X15452373185688

[3] Lipiäinen, Heini Sisko Maarit, and Heikki Karjaluoto. "Industrial branding in the digital age." Journal of Business & Industrial Marketing 30, no. 6 (2015): 733-741. https://doi.org/10.1108/JBIM-04-2013-0089

[4] Mat Razali, N. A. Keselamatan siber dan cabarannya. Utusan Online. (June 16, 2017).

[5] Rowley, Jennifer. "Online branding strategies of UK fashion retailers." *Internet research* 19, no. 3 (2009): 348-369. https://doi.org/10.1108/10662240910965397

[6] Karake-Shalhoub, Zeinab, and Lubna Al Qasimi. *Cyber law and cyber security in developing and emerging economies*. Edward Elgar Publishing, 2010.

[7] Strauss, Anselm, and Juliet Corbin. "Basics of qualitative research techniques." (1998).

[8] Ganesin, A., L. Supayah, and Jamaludin Ibrahim. "An overview of cyber security in Malaysia." *Arabian Journal of Business and Management Review (Kuwait Chapter)* 6, no. 4 (2016): 12-20. https://doi.org/10.12816/0036698

[9] Tan, A. "Deputy prime minister outlines Malaysia's digital efforts, noting that the digital economy will account for one-fifth of the country's GDP by 2020". (2017).

[10] Weber, Valentin. "Linking cyber strategy with grand strategy: the case of the United States." *Journal of Cyber Policy* 3, no. 2 (2018): 236-257. https://doi.org/10.1080/23738871.2018.1511741
[11] CyberSecurity Malaysia. www.cybersecurity.my/data/content_files/46/1634.pdf (Cyber Security Annual Report). 2020.
[12] Edelman, David C. "Branding in the digital age." *Harvard business review* 88, no. 12 (2010): 62-69.
[13] Ministry of Communications. "National Cyber Security Strategy to be implemented middle of this year - DPM". 3 April 2019.
[14] Heuser, Beatrice. *The evolution of strategy: thinking war from antiquity to the present*. Cambridge University Press: Cambridge, 2010.
[15] Malaysian Communications and Multimedia Commission. www.mcmc.gov.my/.../communications-and-multimedia-act-1998-reprint-200 Communications and Multimedia Act 1998). 2019.