Asian Culture and History; Vol. 13, No. 2; 2021
ISSN 1916-9655 E-ISSN 1916-9663
Published by Canadian Center of Science and Education

Cyber-Security Culture towards Digital Marketing Communications among Small and Medium-Sized (SME) Entrepreneurs

Aiman Huzrin Adleena Huzaizi[1], Siti Nor Amalina Ahmad Tajuddin[2], Khairul Azam Bahari[2], Kamaruzzaman Abdul Manan[2] & Nur Nadia Abd Mubin[2]

[1] Peninsula College, The Ship Campus, Pulau Pinang, Malaysia

[2] Department of Communication and Media, Faculty of Languages and Communication, Sultan Idris Education University, Malaysia

Correspondence: Siti Nor Amalina Ahmad Tajuddin, Department of Communication and Media, Faculty of Languages and Communication, Sultan Idris Education University, Tanjong Malim, Perak, Malaysia. Tel: 605-450-6064.

Received: December 2, 2021 Accepted: December 23, 2021 Online Published: December 30, 2021

doi:10.5539/ach.v13n2p20 URL: https://doi.org/10.5539/ach.v13n2p20

Abstract

Cybersecurity is a multidisciplinary field of study that focuses on preserving and protecting data and information from a wide range of threats and dangers. This study presents a cyber-security culture for assessing the knowledge, attitude and practice towards digital marketing communications among small and medium-sized entrepreneurs. The objectives of this study were to identify the knowledge, attitudes, and practices of cyber-security culture toward digital marketing communications among small and medium-sized entrepreneurs in Selangor, as well as to look into the relationship between knowledge and practice in this area. This study utilized a quantitative methodology in the form of a survey, with respondents being selected at random from a list of numbers and from a box of random numbers. Several lists were generated using Instagram business account listings, telegram entrepreneur groups, the National Entrepreneurs Institute, and the Kuala Selangor District Council webpage for recruiting respondents. From the findings, this study found that there is a strong relationship between the level of knowledge and practices towards cybersecurity in digital marketing communications among small and medium-sized entrepreneurs. The study concluded that good knowledge of cybersecurity is crucial among entrepreneurs for them to establish good practices in managing their business.

Keywords: cyber-attacks, cybersecurity culture, digital marketing, entrepreneurs, Small and Medium-Sized (SME)

1. Introduction

1.1 Background of the Study

Initially, cyber security was described by a highly specialized technical approach that should be left to professionals (Georgiadou et al., 2020). However, in today's world of ever-increasing hazards and threats, cyber security is crucial for all users and suppliers of systems and data, from the smallest individual to the greatest enterprise and most powerful state (Ghernaouti & Wanner, 2018). Furthermore, information technology, such as mobile devices and digital apps, has altered daily living, allowing for a wide range of lifestyles in a variety of fields. As a result, individuals should be able to create their cybersecurity strategies to provide safe and secure cyberspace. The notion of a cybersecurity culture is significant in the digital world, which is often referred to as cyberspace (Da Veiga et al., 2020). The intentional and unintentional manners in which cyberspace is used from an international, national, organizational, or individual viewpoint in the context of the cyber user's attitudes, assumptions, beliefs, values, and knowledge is referred to as cybersecurity culture (Da Veiga, 2016). He further stressed that the resulting cybersecurity culture may either promote or constrain individual, organizational, and government safety, security, privacy, and civil rights in cyberspace (Da Veiga, 2016).

Cyber-attacks are rising in frequency and scope, affecting all spheres of economic activity, putting industries and enterprises in danger. As a result, our study concentrated on small and medium-sized (SME) entrepreneurs. Furthermore, growing digital technologies are spawning new businesses and offering up massive market opportunities for SMEs, but at the same time, they are also making them more vulnerable to cybersecurity

attacks. Microsoft, in cooperation with Frost & Sullivan, revealed the findings of research that estimates the potential economic damage in Malaysia as a result of cybersecurity events to be as high as US$12.2 billion (Microsoft Malaysia News Center, 2021). Due to a major shortage of technology experience and resources among entrepreneurs, more than two-thirds of small and medium-sized businesses have been victims of cyber-attacks over the year. To reap the benefits of the digital transformation, small and medium-sized (SMEs) entrepreneurs will need to properly manage cyber-risks as they connect to the digital world and progress towards new digital solutions. At a reasonable cost, a basic level of cyber-security must be given. Furthermore, cybersecurity must not become a barrier for anybody wanting to perform private or business-related activities over the Internet (Ghernaouti & Wanner, 2018).

As a result, knowledge and attitudes are two critical pillars in establishing cybersecurity culture, which will then support cybersecurity best practices (Reegård et al., 2019) which were the focus of this present study.

1.2 Problem Statement

Today's cybersecurity looks to be a never-ending cycle of an individual's increasing security and training to thwart harmful assaults, while the attacker seeks new ways to break down the networks. Cyber-attacks thus are a potential threat to a cybersecurity culture. As data usage rates and Internet consumption continue to increase, cyber awareness has become increasingly urgent. The digitization of our society has significant consequences for public security as cyber security threats and cyber-attacks raise the risk of casualties (Katsantonis et al., 2019). In terms of marketing communication, social media is much more complex than traditional marketing, such as print advertising in newspapers or magazines, television or radio commercials, billboard ads and brochures. Companies and entrepreneurs have already changed marketing strategies across digital channels such as blogs, social media, YouTube videos, pop-ups and banner advertising in today's current situation, not just to virally distribute goods or services and sustain customer relationships (Bekoglu & Onayli, 2016). But revenues have also increased and marketing costs have been reduced (Hashim et al., 2016). The COVID-19 pandemic is shifting social and business norms and forcing businesses to ramp up their digital transformation. The broader adoption of digitalization means that businesses must include cyber risk assessment, testing and training as part of the new normal, even after the pandemic has eased. Extended movement restrictions have led to a paradigm shift to remote work and 'social distance' and this has led organizations to move quickly to digital channels for continuity. Chief Executive Officers (CEOs), entrepreneurs as well as information security personnel have presented a new set of cyber security challenges, as increased use of technology means greater exposure to cyber threats (BERNAMA, 2020).

Despite the fact that more businesses have invested in security awareness training programs as well as a variety of security policies, procedures, and technical solutions, yet, incidents occur more frequently in businesses that provide training (Georgiadou et al., 2020). While the majority of employees claim to understand the company's standards and procedures, knowledge is not enough to keep hostile conduct at bay. In Malaysia, the recent study had indicated that 48 percent of cyber incidents were due to human or administration errors, with the most frequently infringed data being consumer information, 40 percent of businesses reporting a customer file leak, 35 percent were affected by ransomware attacks and malicious email link phishing (Asila, 2019). In addition to that, as cybercriminals increasingly show deep technical expertise and new special skills in the manipulation of technological and social tools, cyber-attacks are becoming more sophisticated (Katsantonis et al., 2019). In 2018, a study has been shown that there are 178 cases of data breach to date, almost a 200% jump from the recorded 63 attacks last year, according to data from the Malaysia Computer Emergency Response Team of Cyber Security Malaysia. However, a cybersecurity expert believes that the figure is alleged to be much higher as there were many unreported incidents as well (Yunus, 2021). As such, many people claim that they do not know how to secure their online system or that they do not know the implications of protection for Internet security are the key problem with these accidents (Bada et al., 2019). In response to this problem, there is a need to conduct this study on small and medium-sized entrepreneurs by assessing the level of knowledge, attitudes and practices of cyber-security culture towards digital marketing communications.

1.3 Small and Medium-Sized Entrepreneurs in Malaysia

Many scholars have agreed that in most developed nations, entrepreneurs seem to have dominated small-scale businesses (Adam & Mahadi, 2016; Hashim et al., 2016; Rahayu & Day, 2017). SMEs are the backbone of the Malaysian economy, accounting for 97.3 percent of all company establishments, 36.3 percent of total GDP, 65.5 percent of total workforces, and 17.6 percent of total exports in 2015 (SME Corp. Malaysia, 2016). SME contribution to Malaysia's service, manufacturing, and construction industries is 98.2 percent, 95.4 percent, and 87.1 percent, respectively. These figures demonstrate the importance of SMEs, which not only encompass a large

number of businesses but also serve as the key source of contributions and development to Malaysia's economy (Yuan et al., 2019). The small and medium-sized business is determined by the number of employees and/or revenue it generates. These two criteria must meet a certain standard set by the respective country to be classified as a small or medium business (Abdul Razak et al., 2018). The development of SMEs plays a critical role in Malaysia's socio-economic development strategy, particularly in the development of the Bumiputra community. Chinese entrepreneurs dominated Malaysian SMEs in the early decades of independence, leaving Malaysians and Bumiputras far behind. That condition had to change to achieve improved economic redistribution in this multi-racial country. As a result, the government has aided a significant number of Bumiputra-owned SMEs (Wok, 2007).

Due to the emergence of its economy and the dominance of trade activities, Malaysia's economic development has been intimately tied to global economic changes. In the early years of independence, resource-based products, primarily from agriculture and mining, provided 60% of total industrial growth. This contribution, however, decreased in the 1970s as non-resource-based industries, particularly electronics and textiles, grew in significance (Abdul Razak et al., 2018). They contributed little or minimally to the development and expansion of Malaysia's domestic industrial structure, according to research, and their links to the rest of the economy were weak. The strategic role and growth potential of SMEs in general, and technology-based export-oriented SMEs in particular, should be considered against this backdrop, particularly in the context of their role in accelerating Malaysia's development within the globalized economy (Wok, 2007).

1.4 Cybersecurity for Businesses

Cybercrime is now ranked as one of the world's top four economic crimes, according to the PricewaterhouseCoopers (PWC) Global Economic Crime Survey in November 2011, with 23 percent of respondents saying that they were victims of computer crime. The internet has revolutionized the management of tasks in existence, empowering them to connect with new people through social networks and the opening of new economic horizons for individuals and organizations to transact via mobile devices, including fundamental changes in the higher education system and teaching methods (Lee et al., 2017). In collaboration with Frost & Sullivan, Microsoft had released the results of its study that shows the potential economic loss in Malaysia as a result of cyber security incidents can reach an astounding US$12.2 billion. The study shows that more than half of the organizations surveyed in Malaysia have either had a cybersecurity incident as much as 17 percent and those who were not sure whether they had one because they did not conduct adequate forensics or data breach evaluation at 36 percent (Cybersecurity threats to cost organizations in Malaysia US$12.2 billion in economic losses - Microsoft Malaysia News Center, 2021). Recently, during the Movement Control Order (MCO) period from March 18 to April 7, 2020, Cybersecurity Malaysia recorded a total of 838 cyber-attacks, reflecting a whopping 82.5 percent rise compared to the same period in 2019. Regarding this, companies must be able to react quickly and decisively when a cyber-attack happens, so they must step up preparations against cyber-attacks to ensure that their operations can recover quickly (BERNAMA, 2020). Knowing what to protect is crucial to any successful cybersecurity operation. While this may seem obvious, most small firms overestimate or underestimate the importance of their data (Paulsen, 2016). Small medium-sized entrepreneurs need to be aware of the importance of having cyber security to protect their business and also to take in mind the consequences such as the business losses that might happen to them if they do not practice the culture of cyber security.

2. Methodology

A descriptive quantitative approach has been used to run the study to look at the knowledge, attitudes and practices of cyber-security culture towards digital marketing communications among small and medium-sized enterprises in Selangor. As for the study, a descriptive approach has been used due to its structured way to gain data by using a questionnaire as our instrument. The technique was less time-consuming as a result of the COVID-19 pandemic, and we were able to contact a larger number of respondents for the data gathering. The target respondents were among Small and Medium-sized (SME) entrepreneurs in Selangor. This study adopted a probability sampling method technique, which was simple random sampling. A random sample is a subset of respondents chosen at random from a larger group. At any point during the sampling process, each individual has an equal chance of being chosen for the study (DePoy & Gitlin, 2019). During the process of this data collection, several lists have been generated from the Instagram business account list, telegram entrepreneur groups, the National Entrepreneurs Institute and the Kuala Selangor District Council portal. The respondents were randomly chosen by the numbers assigned in the list that has been extracted from the website on paper and drawing the numbers on the paper randomly from the box. To identify the level of knowledge, attitudes and practices of cyber-security culture towards digital marketing communications among small and medium-sized entrepreneurs

(SMEs) in Selangor, this study used an ordinal set of questions adopted and adapted from two research instruments which were from the Security Behavior Intentions Scale (SeBIS) by Egelman and Peer (2015) and from the past study that had designed an instrument to evaluate information security awareness (Kaur & Mustafa, 2013). This study was conducted during Movement Control Order, therefore, an online survey was used as a strategy to distribute the questionnaire. A total of 500 respondents were identified and randomly contacted to participate in the study. After 3 weeks of the study period, 204 respondents managed to complete the survey. The questionnaire was divided into two main parts. Section A consists of 8 questions of demographic data. As for section B of the questionnaire, 5 points Likert scale was used to measure the level of agreement for knowledge (7 items), attitudes (11 items) and practices (7 items). This is necessary to conduct the relationship analysis for research objective two.

2.1 Method of Data Analysis

Statistical software packages for the social sciences (SPSS) version 22 was used to analyze as well as assess the level of knowledge, attitudes and practices of cyber-security culture as well as the relationship between knowledge and practice towards cyber security in digital marketing communications among small and medium-sized entrepreneurs (SMEs) in Selangor. Moreover, correlation analysis was used to measure the relationship between knowledge, attitudes and practices of cybersecurity in digital marketing communications among Selangor's SME entrepreneurs.

3. Results

Descriptive analysis of this study shows that three main elements have been explored in this study which were the level of knowledge, attitudes and practices of cyber-security culture towards digital marketing communications among small and medium-sized entrepreneurs in Selangor. It involves seven-item to measure knowledge, 11 items to measure attitude and eight items to measure practice. The respondents' demographic data will be described in this section. A detailed overview of the demographic profiles of the respondents is presented in Table 1.

Based on the data from the conducted survey, the majority of the respondents were aged between 25 to 34 years old with a percentage of 30.9%. Whereas those who were 35 to 44 years old are the second-highest respondents, which is 26.5%. While those who were between the age of 18 to 24 is at 18.6%. As for those who were at the age 45 to 54, they are at 12.7%. There was 9.8% of respondents recorded to be at 56 to 64 of age, and the least age group was 65 years of age and above with at the percentage of 1.5%. For the type of business, the highest respondents that is 30.9% will be those who were in the beauty/health industry. The second-highest percentage of the respondents were those in the food industry, which is at 22.5%. The respondents who were in the Service/Trade industry were recorded at 21.6%. While those who were in the manufacturing industry were recorded at 8.3%. 7.8% of respondents were in the agriculture industry, whereas 4.4% of respondents were involved in other types of industries. As for those who were in the technology industries, the percentage recorded was 3.9%. Finally, 0.5% falls under those who were involved in both the agriculture and food industries. Next, 57.4% of the respondents were male, and the female respondents were 42.6%. Based on the findings, we can see that those who had less than five years of experience were at 67.2 of percentage whilst those who had business experience between 5 to 10 years was recorded at 24.5%. However, 8.3% have had more than 20 years of business experience. As for the education level of the respondents, 33.3% of the respondents had a diploma, whilst 30.9% of the respondents received their high school certificates. Meanwhile, about 27.5% of the respondents hold a bachelor's degree, whilst 6.4% hold a master's degree. There were only 2.0% of the respondents who have a Ph.D. If we look at the monthly profit, 42.6% gained between RM1500 to RM2500. Meanwhile, those who gained under RM1000 were at 24.0%. From the finding, we can also see that the percentage of those who manage to gain their business profit between RM2600 to RM3500 is at 19.6%. Only 13.7% of the total respondents managed to gain RM3600 and above. Lastly, there were 77.0% of the respondents had registered with the Companies Commission of Malaysia (SSM), while 23.0% did not do so.

Table 1. Frequency distribution of age, types of business, gender, business experiences, education level, monthly business profit and their business registered under the Companies Commission of Malaysia (SSM)

Variables	Freq.	Percent
Age		
18 ± 24	38	18.6%
25 ± 34	63	30.9%
35 ± 44	54	26.5%
45 ± 54	26	12.7%
55 ± 64	20	9.8%
65 >	3	1.5%
Types of Business		
Beauty/Health	63	30.9%
Food	46	22.5%
Manufacturing	17	8.3%
Service/Trade	44	21.6%
Agriculture	16	7.8%
Agriculture and Food	1	.5%
Technology	8	3.9%
Others	9	4.4%
Gender		
Male	117	57.4%
Female	87	42.6%
Business Experience		
< 5 years	137	67.2%
5 ± 10 years	50	24.5%
> 20 years	17	8.3%
Education Level		
High School	63	30.9%
Diploma	68	33.3%
Degree	56	27.5%
Master	13	6.4%
PHD	4	2.0%
Monthly Business Profit		
< RM1000	49	24.0%
RM1500 ± RM 2500	87	42.6%
RM2600 ± RM3500	40	19.6%
RM3600 >	28	13.7%
Businesses registered under the Companies Commission of Malaysia (SSM)		
Yes	157	23.0%
No	47	77.0%

Research Objective 1 - To identify the level of knowledge, attitudes, and practices of cyber-security culture toward digital marketing communications among small and medium-sized entrepreneurs in Selangor

To achieve research objective 1, descriptive analysis was performed on all items for knowledge, attitudes and practices. In general, the findings in Table 3 reveal that 66.4% of respondents agreed that they have a positive attitude towards cybersecurity in digital marketing communications. In particular, 79.8% of respondents agreed that they have an overall knowledge about cybersecurity in digital marketing communications. Moreover, 86.8% strongly agreed that they know what they need to do to address the problem of data security at the workplace. In addition, 84.4% strongly agreed that they understand the ethical procedure to conduct business. They also strongly agreed that 83.2% of them understood the importance of data security. On the other hand, more than half of respondents (69.6%) reported that when getting a link from someone, they would open it without double-checking where it will bring them. In this instance, they need to be more careful upon receiving an unknown link from an anonymous.

Table 2. Descriptive statistics of knowledge towards cybersecurity in digital marketing communications among Small and Medium-Sized Entrepreneurs in Selangor

Item (s)	Mean	%	Std. Deviation
K1 - I know what I need to do to address the problem of data security at my workplace.	4.34	86.8	.787
K2 - The company's Internet access is a corporate resource that should only be utilized for business purposes.	4.22	84.4	.704
K3 - Phishing is the act of stealing sensitive and personal information from a user. I'm used to hearing threats like these.	4.22	84.4	.711
K4 - I understand the importance of data security.	4.16	83.2	.662
K5 - When I'm requested to update the software, I'll do it right away.	3.85	77	1.008
K6 - I just ignore and close my computer when it attempts to reboot after upgrading or installing applications.	3.72	74.4	1.215
K7 - When someone sends me a link, I open it without first double-checking where it will take me.	3.48	69.6	1.412
Total Knowledge	3.99	79.8	.660
Valid N		204	
Strongly disagree 1 - (0–20%); Disagree 2 – (21–40%); Slightly agree 3 – (31–60%); Agree 4 – (61–80%); Strongly agree 5 – (81–100%)			

Table 3 shows that respondents' attitudes of cybersecurity culture in digital marketing communications among small and medium-sized entrepreneurs. In general, the findings in Table 3 reveal that the highest number of participants (80.6%) strongly agreed that they were curious to learn how antiviral software may assist them to improve the security of their business operations followed by 79.8% of them agreed that utilizing a password-protected computer was a good idea and safer. Moreover, more than three-fourths of respondents (79%) said they were confident in detecting phishing attacks followed by 74.6% of them agreed that they were safe from malware, scareware, and spyware. Respondents, on the other hand, must have the right mindset about why the security setting was supposed to be difficult. According to 49 percent of respondents, this is to prevent the system from being attacked by the hacker.

Table 3. Descriptive statistics of small and medium-sized entrepreneurs' attitudes towards cybersecurity culture in digital marketing communications

Item (s)	Mean	%	Std. Deviation
A1 - Antivirus software is something I'm curious to learn more about.	4.03	80.6	.898
A2 - Using a password-protected computer is, in my opinion, a good idea.	3.99	79.8	.800
A3 - I am confident that I can identify phishing.	3.95	79	.892
A4 – I'm protected against malware, scareware, and spyware.	3.73	74.6	.843
A5 - No one can guess my password since it is strong enough.	3.72	74.4	.956
A6 - My method for managing sensitive data is thorough and reliable.	3.63	72.6	.930
A7 - I am aware of cybercrime and will never be a victim.	3.49	69.8	1.024
A8 - It is appropriate to share downloaded materials with a friend without paying him or her.	2.57	51.4	1.087
A9 - I don't use a complicated password since it's too difficult to remember, so I use my name or anything easy.	2.49	49.8	.965
A10 - Security settings and tools slow me down and cause me trouble.	2.45	49	.872
A11 – It's pointless to change the password because it may still be hacked.	2.45	49	.878
Total Attitude	3.32	66.4	.521
Valid N		204	
Strongly disagree 1 - (0–20%); Disagree 2 – (21–40%); Slightly agree 3 – (31–60%); Agree 4 – (61–80%); Strongly agree 5 – (81–100%)			

Finally, the findings in Table 4 present respondents' practices of cybersecurity culture in digital marketing communications among small and medium-sized entrepreneurs. Generally, the findings show that 69.6% of respondents agreed that they practiced cybersecurity in digital marketing communications. In specific, 83.8% strongly agreed that they were using the firewall system at work followed by 82.8% of them strongly agreed that they were always on alert when receiving suspicious emails. More than three-fourths of respondents (77.8%) also agreed that if their computer was hacked, they would immediately turn off their computer device. On the other hand, 44% of respondents still practiced illegal downloading such as online movies. This indicates that the respondents' level of practicing cyber security still needs to be enhanced because respondents only practice it to

protect their own business.

Based on Tables 2, 3 and 4, this analysis concludes that the level of respondents' knowledge about cyber security is high. Moreover, their level of attitude about the importance of cyber security is also positive and high. Table 4 reveals that respondents agreed with the practice of cybersecurity towards digital marketing communications in multiple situations. Their cyber security practices included using a firewall at work (M = 4.19), remaining alert on suspicious emails (M = 4.14), turning off the computer if something wrong with the mouse pointer (M = 3.89), allowing others to fix computer system vulnerability (M = 3.87) and keeping important software updated (M = 3.81). Although the findings show that respondents practiced cyber security at work for security and protection, they continued to engage in harmful practices that could lead to cybercrime (illegal downloading). Therefore, more campaigns should focus on cultivating a healthy culture of cyber security. To conclude, Research Objective 1 - To identify the level of knowledge, attitudes, and practices of cyber-security culture toward digital marketing communications among small and medium-sized entrepreneurs in Selangor is achieved.

Table 4. Descriptive statistics of practices of cybersecurity culture towards digital marketing communications among small and medium-sized entrepreneurs

Item (s)	Mean	%	Std. Deviation
P1 – I am using the firewall system at work.	4.19	83.8	.881
P2 - When it comes to suspicious emails, my practice is to be on the alert.	4.14	82.8	.926
P3 - If my mouse pointer goes on its own on the screen and clicks on a file on my desktop, I will turn off my computer device.	3.89	77.8	.932
P4 - If I discovered a security flaw on my device, I would continue doing what I was doing and trust others to fix it.	3.87	77.4	1.146
P5 - I keep track of Windows / Apple, antivirus, browser, and other software updates.	3.81	76.2	1.134
P6 - I will click an email that requires confirmation for my bank account as the bank has updated the new software.	3.56	71.2	1.570
P7 - There is no problem downloading illegal items such as online movies without having to pay.	2.20	44	.937
Total Practice	3.48	69.6	.603
Valid N		204	
Strongly disagree 1 - (0–20%); Disagree 2 – (21–40%); Slightly agree 3 – (31–60%); Agree 4 – (61–80%); Strongly agree 5 – (81–100%)			

Research Objective 2 - To examine the relationship between knowledge and practice of cyber-security culture toward digital marketing communications among small and medium-sized entrepreneurs in Selangor

The Pearson correlation analyses were used to achieve research objective two. This analysis only examined the relationship between knowledge and practices of cybersecurity culture toward digital marketing communications among small and medium-sized entrepreneurs in Selangor. Preliminary analyses were carried out to confirm that the normality and linearity assumptions were not violated.

Table 5 demonstrates that there was a strong, positive relationship between knowledge and practices with a value of r =.69, n = 204, p 0.01 of cybersecurity culture towards digital marketing communications among small and medium-sized entrepreneurs in Selangor. As a result, our second research question is answered to which respondents' knowledge is significantly correlated with the practices of cybersecurity culture toward digital marketing communications.

Table 5. Relationship between knowledge and practices using Pearson correlation coefficient

Correlations		Total Knowledge	Total Practice
Total Knowledge	Pearson Correlation	1	.687**
	Sig. (2-tailed)		.000
	N	204	204
Total Practice	Pearson Correlation	.687**	1
	Sig. (2-tailed)	.000	
	N	204	204

**. Correlation is significant at the 0.01 level (2-tailed).

4. Discussion

This study aimed to assess the level of knowledge, attitudes and practices of cyber-security culture towards digital marketing communications and to examine the relationship between knowledge and practice of cyber-security culture towards digital marketing communications among small and medium-sized entrepreneurs in Selangor. A quantitative approach in the form of a survey was used for this study. The study used a probability sampling method technique which was the simple random sampling were used in the study where several lists have been generated from Instagram business account list, telegram entrepreneur groups, the National Entrepreneurs Institute and Kuala Selangor District Council portal and the respondents were randomly chosen by the numbers assigned in the list and drawing random numbers from a box. A total of 204 respondents between the ages of 18 to 65 years of age has participated in answering the survey to make this study a success.

The study used an ordinal collection of questions developed from two research instruments: Egelman and Peer's (2015) Security Behavior Intentions Scale (SeBIS) and a previous study that developed an instrument to assess information security awareness. (Kaur & Mustafa, 2013). Preliminary analyses were performed to ensure no violation of the assumptions of normality and linearity. There was a strong, positive correlation between knowledge and practices of cyber-security culture towards digital marketing communications among small and medium-sized entrepreneurs in Selangor with the value of $r = .69$, $n = 204$, $p < 0.01$. Based on the findings, entrepreneurs must have a thorough understanding of cybersecurity in order to build sound business practices. Knowing what to defend is therefore essential for any effective cybersecurity operation. The current findings also concur with the previous study of Georgiadou et al. (2020) who suggested that cybersecurity threat is closely linked to a person's personality, behaviour, attitude, beliefs, and skills.

Furthermore, owing to a lack of detection, slow response, and inconsistent remediation practices, insider security breaches represent a higher business risk (Georgiadou et al., 2020; Ko et al., 2017). While this may seem self-evident, most small businesses exaggerate or underestimate the value of their data (Paulsen, 2016). Small and medium-sized businesses must be aware of the necessity of having cyber security to secure their businesses, as well as the implications, such as economic losses, that may occur if they do not consider cyber security.

Acknowledgments

This is a small-scale preliminary study that has been carried out as part of the Fundamental Research Grants Scheme (FRGS/1/2020/SS0/UPSI/02/5) provided by the Ministry of Education of Malaysia. The authors would like to extend their gratitude to Universiti Pendidikan Sultan Idris (UPSI) that helped in managing the grant.

References

Abdul Razak, D., Abdullah, M., & Ersoy, A. (2018). Small medium enterprises (SMEs) in Turkey and Malaysia a comparative discussion on issues and challenges. *International Journal of Business, Economics and Law*, *10*(49), 2-591.

Adam, S., & Mahadi, B. (2016). Entrepreneurial Strategy-Making Mode and Organisational Performance of Internet Business in Malaysia. *Journal of Global Business and Social Entrepreneurship (GBSE)*, *2*(4), 85-97.

Asila, J. (2019, October 17). *84% of SMEs fell victim to cyber attack last year. The Malaysian Reserve*. Retrieved from https://themalaysianreserve.com/2019/10/17/84-of-smes-fell-victim-to-cyber-attack-last-year/

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*

Bekoglu, F. B., & Onayli, C. (2016). Strategic approach in social media marketing and a study on successful Facebook cases. *European Scientific Journal*, *12*(7), 261-274. https://doi.org/10.19044/esj.2016.v12n7p261

BERNAMA. (2020) *Preparing for cyber risk assessment is the new normal - ASIACYBERX*. Retrieved 13 February 2021, from https://www.bernama.com/en/general/news_covid-19.php?id=1838281

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 1006-1015. https://doi.org/10.1109/SAI.2016.7556102

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers and Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

DePoy, E., & Gitlin, L. N. (2019). *Introduction to research E-book: Understanding and applying multiple strategies*. Elsevier Health Sciences.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd annual ACM conference on Human Factors in Computing Systems* (pp. 2873-2882). https://doi.org/10.1145/2702123.2702249

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, 1-12. https://doi.org/10.1080/08874417.2020.1845583

Ghernaouti, S., & Wanner, B. (2018). Research and Education as Key Success Factors for Developing a Cybersecurity Culture. In *Cybersecurity Best Practices* (pp. 539-552). https://doi.org/10.1007/978-3-658-21655-9_38

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 and Space*, *12*(2).

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

Kaur, J., & Mustafa, N. (2013, November). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286-290). IEEE. https://doi.org/10.1109/ICRIIS.2013.6716723

Ko, L. L., Divakaran, D. M., Liau, Y. S., & Thing, V. L. (2017). Insider threat detection and its future directions. *International Journal of Security and Networks*, *12*(3), 168-187. https://doi.org/10.1504/IJSN.2017.084391

Lee, K. G., Chong, C. W., & Ramayah, T. (2017). Website characteristics and web users' satisfaction in a higher learning institution. *International Journal of Management in Education*, *11*(3), 266-283. https://doi.org/10.1504/IJMIE.2017.084926

Microsoft Malaysia News Center. (2021). *Cybersecurity threats to cost organizations in Malaysia US$12.2 billion in economic losses.* Retrieved 13 February 2021, from https://news.microsoft.com/en-my/2018/07/12/cybersecurity-threats-to-cost-organizations-in-malaysia-us12-2-billion-in-economic-losses/

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, *49*(8), 92-97. https://doi.org/10.1109/mc.2016.223

Rahayu, R., & Day, J. (2017). E-commerce adoption by SMEs in developing countries: Evidence from Indonesia. *Eurasian Business Review*, *7*(1), 25-41. https://doi.org/10.1007/s40821-016-0044-6

Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture. *Proceedings of the 29th European Safety and Reliability Conference*, 4036-4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

SME Corp. Malaysia. (2016). *Guideline book for new SME definition*. Retrieved from http://www.smecorp.gov.my/images/pdf/Guideline_New_SME_Definition_updated.pdf

Wok, S. (2007). Malaysia at 50: Achievements and Aspirations. In S. A. Idid (Ed.), *Intellectual Discourse*, *15*(2).

Yuan, Y., Azam, S., & Tham, J. (2019). Small and Medium Size Enterprises (SMEs) in Malaysia: A Conceptual Underpinning of Capital Structure Decisions and Firm Performance. *European Journal of Social Sciences Studies*, *4*(5). http://dx.doi.org/10.46827/ejsss.v0i0.709

Yunus, R. (2021, December 12). Almost 200% increase in data breach attacks since 2018. *The Malaysian Reserve*. Retrieved 13 February 2021, from https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/