IJCCS (Indonesian Journal of Computing and Cybernetics Systems)
Vol.15, No.3, July 2021, pp. 233~244
ISSN (print): 1978-1520, ISSN (online): 2460-7258
DOI: https://doi.org/10.22146/ijccs.67010

Exploring MSMEs Cybersecurity Awareness and Risk Management : Information Security Awareness

Yerik Afrianto Singgalen*[1], Hindriyanto Dwi Purnomo[2], Irwan Sembiring[3]
[1]Universitas Katolik Indonesia Atma Jaya, Jakarta, Indonesia.
[2,3]Universitas Kristen Satya Wacana, Jawa Tengah, Indonesia.
e-mail: ***[1]yerik.afrianto@atmajaya.ac.id**, [2]hindriyanto.purnomo@uksw.edu,
[3]**irwan@uksw.edu**

Abstrak

Pemanfaatan teknologi informasi dalam manajemen Usaha Mikro Kecil Menengah (UMKM) tidak terbatas pada performa dan produktivas usaha, melainkan juga pada aspek keamanan data dan transaksi menggunakan pelbagai aplikasi berbasis mobile, website, maupun dekstop. Artikel ini menawarkan gagasan untuk mengeksplorasi kesadaran cybersecurity serta manajemen risiko dari pelaku UMKM yang mengadopsi teknologi informasi. Metode penelitian yang digunakan ialah kualitatif dengan pendekatan studi kasus pada bisnis Coffeeshop X dan bisnis Souvenir Y di Kota Salatiga, Jawa Tengah, Indonesia. Teknik pengambilan data menggunakan wawancara mendalam, observasi dan studi dokumen. Hasil penelitian ini menunjukkan bahwa Cybersecurity Awareness khususnya kesadaran keamanan informasi dapat ditinjau berdasarkan pengetahuan, sikap dan perilaku. Sedangkan, risiko dapat dikelola berdasarkan supply risk, operational risk, dan customer risk. Adapun, persoalan Cybersecurity Awareness dan Risk Management pada UMKM bersifat holistik dan tidak dapat digeneralisir, sehingga perlu ditinjau secara kontesktual berdasarkan studi kasus. Dalam konteks Coffeeshop X dan Souvenir Y, tingkatan Cybersecurity Awareness (pengetahuan, sikap, perilaku) tidak sama.. Selain itu, pengelolaan risiko lebih dominan pada dimensi customer risk, dibandingkan dengan supply risk dan operational risk.

Kata kunci*—Cybersecurity, Manajemen Risiko, UMKM, Keamanan Informasi*

Abstract

The use of information technology in the management of Micro, Small, and Medium Enterprises (MSMEs) is not limited to business performance and productivity but also aspects of data security and transactions using various mobile, website, and desktop-based applications. This article offers an idea to explore cybersecurity awareness and risk management of MSME actors who adopt information technology. The research method used is qualitative with a case study approach in the Coffeeshop X business and the Y Souvenir business in Salatiga City, Central Java, Indonesia. The data collection technique used in-depth interviews, observation, and document studies. These findings indicate that Cybersecurity Awareness, especially information security awareness, can be reviewed based on knowledge, attitudes, and behavior. Risk management can be review based on supply risk, operational risk, and customer risk. Cybersecurity Awareness and Risk Management in MSMEs is holistic and cannot be generalized, so it needs to be discussed contextually based on case studies. In the context of Coffeeshop X and Souvenir Y, the level of Cybersecurity Awareness (knowledge, attitude, behavior) is not always linear. In addition, risk management is more dominant in the customer risk dimension, compared to supply risk and operational risk.

Keywords— *Cybersecurity, Risk Management, SMEs, Information Security*

Received June 24th,2021; Revised July 21th, 2021; Accepted July 30th, 2021

1. INTRODUCTION

Cybersecurity awareness among Micro, Small, and Medium Enterprises (MSMEs) in Indonesia is a context and a fundamental issue in analyzing the development of e-commerce based on an entrepreneurial perspective [1]. Previous research describes the Cybersecurity component for companies divided into several segments: analyze, defend, detect, revival, oversight, and development, which must be interpreted and applied to adapt to the development of cybercrime that is detrimental to system users [2]. The attacker's existence in the virtual space becomes a smooth and a catalyst for application developers as defenders to improve application performance and security. Cybersecurity has a holistic scope, such as operation security, communication security, information security, physical security, and military security [3]. This article offers an idea to explore cybersecurity awareness and risk management of perpetrators (MSMEs) who use e-Commerce applications and digital transaction support applications that are more specific in discussing information security.

Information security is one of the essential components of cybersecurity [4]. In the Control Objective for Information and Related Technology (COBIT) framework, information security is crucial in maintaining company privacy, especially data that cannot be published [5]. In addition to COBIT, the ISO/IEC 27001 framework also evaluates the information security component of information systems used by institutions [6], [7]. Information Security is one aspect of vulnerability that needs to be estimated using various methods or approaches [8]. In the context of information security vulnerabilities, good governance is required to classify multiple risks that can potentially cause harm to companies and government institutions [9]. Therefore, information security is one of the essential issues accommodated in policies to anticipate criminal acts or misuse of data detrimental to institutions and the public [10]. The discussion in this article explicitly describes the perspective of MSME actors to maintain business continuity and protect confidential data or information.

Information security awareness is influenced by knowledge, attitude, and behavior [11]. In the context of knowledge, system users can consider information security before using digital devices as a means of business transactions or digital marketing platforms [12]. Knowledge of the capacity and capability of technology devices and the information systems used is a form of information security awareness that prevents incidents due to negligence in maintaining information security. Meanwhile, information security components that need to be evaluated are trusted in application repositories, misconceptions about application testing, security and agreement messages, pirated applications, and adoption of security control [13]. The various losses caused by the behavior of system users can be classified into three characteristics, namely good, neutral, and bad behavior. Therefore, private and public sector institutions need to manage information security, risks, incidents, assets and optimize system access controllers [14]. It shows that the discussion of information security awareness can be done by identifying system users' knowledge, attitudes, and behavior. Implicitly, matters related to knowledge, attitudes, and behavior of system users. In this case, MSME actors in the Coffeeshop and Souvenir business sector will be discussed with risk management strategies to obtain an overview of anticipatory steps for MSME actors to respond to incidents due to negligence in maintaining confidential data or information.

This article offers an idea to outline cybersecurity awareness and risk management by limiting the scope of the discussion to information security awareness. Contextually, the system users who are the unit of observation of this research are limited to SMEs in the Coffeeshop and Souvenir business sectors. Implicitly, information security awareness will be studied based on knowledge, attitudes, behavior, and business risk management to maintain business continuity and protect confidential data or information. Furthermore, the novelty of this research is the

reconstruction of the model that connects cybersecurity and risk management to realize information security resilience based on the MSME business scale.

2. METHODS

The research method used is a qualitative method with a case study approach to MSME actors in the Coffeeshop and Souvenir business sectors. As an effort to maintain the privacy of MSME actors and the MSME brand, this study uses the initials of the Coffeeshop business identity and the Souvenir business to become the Coffeeshop X business and the Souvenir Y business. Meanwhile, the location of this research is in Salatiga City, Central Java Province, Indonesia. The considerations for adopting a qualitative method and a case study approach are as follows. First, the perspective of MSME actors in the Coffeeshop and Souvenir business sector accumulates from various dimensions related to educational, economic, and socio-cultural backgrounds. The knowledge, attitudes, and behavior of system users describe complex processes or dynamics. Second, information security awareness is a private consideration for MSME actors in the Coffeeshop and Souvenir business sector to manage risks that can cause business losses. Third, the output of this study is the result of a description of the thoughts of MSME actors in the Coffeeshop and Souvenir business sector, which is communicated with the results of previous studies to present novelty and contribute to scientific developments in the field of cybersecurity and risk management.

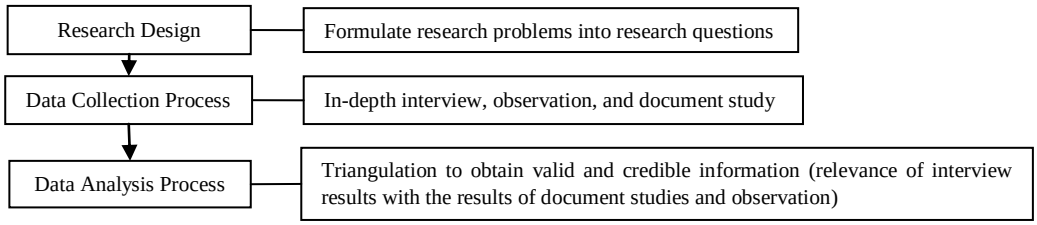

Figure 1. Research Stages

Figure 1 represents the stages of this research. In the first stage, the formulation of the research problem is converted into a research question: first, how is the awareness of Coffeeshop X and Souvenirshop Y entrepreneurs towards information security?; second, how is information security risk management at Coffeeshop X and Souvenirshop Y? based on the formulation of this problem, the data collection process was carried out by conducting in-depth interviews, observations, and document studies. After obtaining the required data and information, the triangulation process is used to analyze the relevance between in-depth interviews, observation, and document studies results. The key informants involved in the in-depth interview process have the following qualification standards. First, the informant is an MSME actor in the Coffeeshop and Souvenir business sector. Second, informants use information technology for product marketing and digital transactions. Third, MSME actors in the Coffeeshop and Souvenir business sectors have adopted information technology for product marketing and digital transactions for more than three years. Based on these qualification standards, in-depth interviews were conducted with the owners and employees of the Coffeeshop X business and the Souvenir Y business. The key informant from the Coffeeshop X business was VN, while the key informant from the Souvenir Y business was RRK. Observations technique were applied by observing the MP application process by owners and employees in managing digital transaction data (Coffeeshop X business) and using IN and WA applications for marketing and digital transactions (Souvenir Y business). Meanwhile, the study of documents related to the Coffeeshop X business transaction data and the Souvenir Y business is confidential.

The triangulation technique is used to obtain valid and credible data as a factual representation of the study on cybersecurity and risk management. Specifically, the triangulation technique is a process of validating the results of in-depth interviews, observations, and document studies to maintain the coherence and correspondence of the data studied in this study. In addition, triangulation techniques consider the relevance of the content to the context of research related to information security awareness based on aspects of knowledge, attitudes, and behavior of system users. In this case, Coffeeshop X business owners and employees (as key informants) use the MP application, and business owners and employees Souvenir Y (as a key informant) uses the IN application for product marketing.

3. RESULTS AND DISCUSSION

3.1 Cybersecurity Awareness : Information Security Awareness

Cybersecurity is a popular topic among academics and practitioners to optimize system performance to be used safely, effectively, and efficiently. The development of Cybersecurity studies can be traced based explicitly on the dimensions of operation security [15], *communication security* [16], *information security* [17], *physical security* [18], [19], *and military security* [20]. In the context of this research, the study on Cybersecurity is focused on Information Security Awareness of the owners and employees of the Coffeeshop X and Souvenir Y businesses. The information security awareness in the context of Coffeeshop X and Souvenir Y businesses can be seen in Table 1 below.

Table 1 Information Security Awareness of Coffeeshop X and Souvenir Y Employee

yber Security Awareness	**Description**	**Coffeshop X**	**Souvenir Y**
Knowledge	*Cyber Crime (Unauthorized access to computer system and service, illegal contents, data forgery, cyber espionge, cyber sabotage and extortion, cracking, cybercrime against government)* [21]	Medium	Low
	Cyber Security (Operation, Communication, Information, Physical, Military) [3]	Medium	Low
Attitude	*Employees Attitude towards Cybersecuiry* [22]	Low	Medium
	Privacy Attitude [23]	Low	Medium
Behavior	*Risky Online Behaviours*[22]	Low	Medium
	Secure Behaviour [23]	Low	Medium

Source: Empirical Data (Processed)

Table 1 results from data processing interviews with owners and employees regarding information security awareness by owners and employees of the Coffeeshop X business and the Y Souvenir business. In the Coffeeshop X and Souvenir Y business context, both owners and employees have knowledge that can be categorized as a medium. However, the attitude of system users regarding Cybersecurity and protection of private matters is still relatively low. In addition, the behavior of system users related to Cybersecurity, risky online behavior, and secure behavior is still relatively low. Based on the results of interviews with Coffeeshop X business employees, the vulnerability aspect that affects the attitudes and behavior of system users is trust in teamwork empowerment. It is following the results of interviews with OI:

"We have to admit that our understanding of cybercrime and cybersecurity is still minimal because we do not have an educational background in information technology. However, we are aware of several things related to the rise of cases of data loss due to being stolen by hackers, fraud through websites that are intentionally created to trap users, and other cases. Such information makes us more alert to limit the use of hardware that has installed the MP application, specifically to serve orders and payments. The MP application is a website-based information system that can be used on Smartphone devices with low specifications and is directly connected to the business owner's account. Each employee has created an account and password, and employee number of monitoring the work

schedule and transaction services directly by the business owner. At work, we trust each other. So, we can take turns serving the ordering and payment processes effectively and efficiently, without having to make consumers wait any longer."

Based on the results of interviews with OI as the owner of the Coffeeshop X business, it can be seen that digital technology operations for transactions and marketing are part of the self-taught learning process, the results of discussions, and participation in informal education. In the Coffeeshop X business context, the barista has a dual role as an employee in charge of serving digital transactions (orders and payments) and an employee who mixes drinks according to consumer demand. Especially for food products, baristas only make reservations on the MP application. In contrast, the provision of food according to consumer demand will be prepared by the kitchen (chef and assistant chef). The barista's dual role in handling food and beverage transaction services demands talent in action and knowledge of the features of a capable MP application. Baristas who have experience operating MP applications will share knowledge with other employees to reduce the risk of fraud and conflicts due to misunderstandings due to errors or negligence of system users when using the MP application.

In the Coffeeshop X business context, team performance is one of the benchmarks for improving business performance. Trust between the owner and the barista as an employee who handles the payment process for food and beverage products plays an essential role in determining the continuity of teamwork in the Coffeeshop X business. Therefore, one form of controlling employee performance to reduce problems arising from vulnerability is the policy of creating employee accounts in the MP application. Thus, the owner can monitor the process of recording purchase transactions based on employee accounts and ask for personal accountability if there is a discrepancy in the audit results between the recorded digital transactions reported and the attached purchase notes (printed). The obstacle identified from the barista's dual role as an employee in charge of mixing coffee and recording digital transactions (orders and payments) at Coffeeshop X is information security awareness that affects the effectiveness and efficiency of digital and manual transaction services. The money storage (cash machine) and MP application hardware (tablet) are located on the same table as the coffee maker without strict supervision, relying only on trust. The barista account is in an operational condition, so irresponsible people can misuse it. In addition, the MP application is a website-based information system that employees can access from personal smartphones by entering the username and password that the owner as the administrator has created. It indicates a high risk of misuse of system user accounts so that it requires attitudes and behaviors that are aware of data or information security.

In terms of quantity, the barista on duty is limited to two people by changing working hours. Consumers who want to order or pay for food and beverage products must wait in front of the cashier until the barista is ready to record digital transactions (orders and payments). The barista does not provide an order confirmation question in the payment process according to the table number but based on the characteristics of the food and beverage product ordered previously. It can cause a technical error, namely the customer's reservation code being swapped, so it takes 10-15 minutes to solve the problem. Meanwhile, other customers have to stay in line or are asked to wait until the issue is resolved or one of the baristas on duty is ready to serve the ordering process manually. Based on the business conditions of Coffeeshop X, it can be seen that knowledge about information security is moderate, but attitudes and behavior are still relatively low (low). Ignorance of private information can be hacked and cause harm to employees and the workplace through various means such as hacking, phishing, and malware [15]. The possibility of data loss is very high if the device that has installed a digital transaction recording application is also used to access social media and other websites [24]. In addition, to optimize business performance, the risks of various business activities related to information security awareness of system users need to be increased [25]. Business performance relies heavily on data to measure sales achievement based on the targeted period, so the data security structure is written in the Standard Operational Procedure and must be applied by every system

user [26]. Cybersecurity, especially Information Security Awareness for coffee shop business SMEs (owners and employees), shows that business information security awareness (knowledge, attitudes, and behavior) needs to be optimized to minimize the risk of cybercrime that harms the business.

In the context of the MSME business Souvenir Y, digital marketing using the IN social media application has an essential role in supporting the sustainability of the Souvenir Y business. Business owners can do product marketing independently by documenting souvenirs based on price and size characteristics using smartphone devices. Meanwhile, customer trust in the Souvenir Y business is mobilized by the availability of information in reviews or testimonials from consumers who have a history of purchasing transactions with the Souvenir Y business before. On the other hand, Souvenir Y's knowledge of Cybersecurity and Cyber Crime is still relatively low. Based on the results of interviews with Souvenir Y business owners, it can be seen that the inadequate knowledge of Cybersecurity and Cyber Crime Souvenir Y is caused by educational backgrounds that are not related to information technology. In addition, the attention of business owners is more dominant on business opportunities and market segmentation, compared to the vulnerability of data or business information from digital applications. This is following the results of interviews with RRK:

"I don't know much about Cybersecurity because I'm not an IT kid, but I know a little about Cyber Crime, such as hacking, phishing, and carding. There is currently enough information about crime in the virtual space, easy to access, just input keywords in the search engine (google). We can know things related to cybercrime and how to anticipate it. After knowing this information, I was careful when accessing websites with many advertisements, so I didn't get trapped like my colleague whose WA business account was hacked because my friend was told to input a code from a prized SMS. A friend of mine clicked on a link from an online gambling website because he thought he would get a prize, but his social media account was actually hacked. I take the experience of my colleagues as a lesson, so I have to be more vigilant. I marketed souvenir products using the IN social media application, regarding product quality, packaging, and delivery processes, it can be seen from consumers' comments. Orders can be made via WA, and we will deal when it has been fully transferred. I will send the goods if in doubt, don't order. The souvenirs that I sell have their uniqueness, so if you're not interested, that's okay. So that the souvenirs I sell are famous, purchases that should be manual, I asked them to provide testimonials on business social media accounts to trust each other, no tricks. Personally, this business account means a lot because consumer reviews are non-repeatable."

Based on the results of interviews with key informants, namely RRK as the owner of the Souvenir Y business, it can be seen that knowledge about Cybersecurity and Cyber Crime is still relatively low. Nevertheless, the attitude and behavior of using the system for product marketing through IN social media can be categorized as a medium. As a social media account owner for the Souvenir Y business, the password for account security is updated regularly. Furthermore, all emails and passwords from business social media accounts have been recorded manually as an anticipatory form of various risks of losing or forgetting passwords. In addition, hardware or Smartphones used for business are different from smartphones used for personal purposes, thus avoiding multiple potential personal omissions that harm Souvenir Y's business. It shows that knowledge about Cybersecurity and Cyber Crime that is not deep does not always indicate the same attitude and behavior. In the Souvenir Y business context, attitudes and behaviors regarding information or data security awareness can be categorized as a medium stage. Souvenir Y owners always pay attention to the security of social media accounts used to market Souvenir Y products. In addition, the trigger for information security awareness has a relationship with the characteristics of the business being run, where consumer confidence in Souvenir Y's business processes lies in buyer reviews of the products sold. In online shops, several previous studies have shown that consumer satisfaction is influenced by the quality of services applied by online shop entrepreneurs [27]. Therefore, online shop owners must implement quality promotional strategies through websites and social media [28]. Consumer confidence in online business activities is influenced by service quality [29] and ease of transaction [30]. In addition, consumer perceptions of previous transaction history also affect consumer confidence [31].

3.2 Cybersecurity Awareness : Risk Management for Information Security Issues

Cybersecurity awareness has a significant relationship with risk management for business information security [23]. [32] Shows that the risks related to Cybersecurity that need to be managed in a business are as follows: partner trust; information theft; insufficient protection of cargo in transit; plant malfunctioning; counterfeit products; failure of IT equipment; product specification fraud; manipulation of data; poor cryptographic decisions; insufficient protection of cargo in transit. It shows that the components related to Cybersecurity awareness in the business realm are holistic and need to be studied contextually. The Sources of risk in the Coffeeshop business can be analyzed based on supply risk, operational risk, and customer risk. The Customer risk aspect is dominant in the Coffeeshop business because of the business characteristics that rely on services and food or beverage products. Some factors influence consumers to choose coffeeshop characteristics based on location, cost, atmosphere, facilities, food, and beverages. Consumer perceptions of the services provided by coffee shop owners and employees also affect consumer loyalty and willingness to pay [33]. Therefore, the product marketing management applied by the Coffeeshop Business manager must be representative of product quality, as well as consumer preferences. Meanwhile, the authentication of food and beverage products and services that reflect the characteristics of a coffee shop is an essential part of attracting consumers' attention. Based on the features of the Coffeeshop business, the concept of risk management based on aspects of supply risk, operational risk, and customer risk becomes relevant.

In addition to coffee shops, the concept of risk management based on aspects of supply risk, operational risk, and customer risk is also relevant to the characteristics of the souvenir business. Souvenir business can be managed individually, group, or professional business entity [34]. Raw materials and the features of Souvenir products also vary according to consumer preferences. Product marketing can be applied conventionally and digitally depending on the financial capabilities of the business owner [35]. Finally, souvenir products relate to the memories or socio-cultural identity of the people in an area or country. The Souvenir business offers material aspects and cultural aspects, namely the value attached to the Souvenir product [36]. Thus, the Souvenir business entrepreneur seeks to manage various risks related to supply risk, operational risk, and customer risk, as shown in Table 2 below.

Table 2 Source of Risk and Risk Management

Business	Source of Risk	Coffeeshop X	Souvenir Y
Supply Risk	Theft of Vendor Credential	✓	×
	Modification of the Source code through Malware	×	×
	Supply of Compromised Software	×	×
	Breach from the Vendor Network	×	×
	Inaccessibility of Supplier	×	×
Operational Risk	Failure to detect coding errors	×	×
	Product specification fraud	✓	✓
	Data Theft	✓	✓
Customer Risk	Manipulation of Data	✓	✓
	Unauthorized access to customer's data	✓	✓
	Fraudulent communication	✓	✓
	Information Sabottage	✓	✓
	Unauthorized payment gateways	✓	✓
	Intellectual Property Theft	✓	×

Source : Modified Sources of Cyber Security Risk [32]

Table 2 is a source of risks related to Cyber Security in a business context. In Coffeeshop X's business, risk management strategies for Cyber Security can be analyzed from three aspects: supply risk, operational risk, and customer risk. Expressly, risk management for supply risk is limited to the risk management of vendor credential theft. Meanwhile, risk management for operational risk is limited to product specification fraud and data theft risk management. Meanwhile, risk management for customer risk is risk management for cases of

data manipulation, unauthorized access to customer data, false communications, information sabotage, unauthorized payment gateways, and intellectual property theft. Coffeeshop X's business has business processes that involve vendors as suppliers of raw materials. Meanwhile, information regarding the vendor's credentials is confidential, so the risk of disseminating vendor information needs to be anticipated. The Coffeeshop X business seeks to protect member data as permanent consumers and transaction history by consumers. Purchase data is confidential, which is only used by the owner of the Coffeeshop X business. In addition, original product specifications, in this case, raw materials and seasonings for the manufacture of specialty drinks and food products belonging to the Coffeeshop X business, are also confidential. There are rules for baristas in recording payment transactions via cash or transfer to a predetermined account number.

Furthermore, employees are required to print receipts to be audited by the business owner for the bookkeeping process. In addition, access to consumer data related to purchase history is limited by the Coffeeshop X business owner as of the MP application administrator. Matters related to the brand logo and gastronomy of food and beverage products commercialized by the Coffeeshop X business are intellectual property that is legal or protected by law. Thus, the customer risk management of Coffeeshop X's business is more dominant than supply risk and operational risk.Dalam konteks manajemen risiko untuk bisnis Souvenir Y, pengelolaan risiko yang berhubungan dengan *Cyber Security* dapat terbatas pada aspek *operational risk*, dan *customer risk.* Aspek *Supply risk* tidak tersedia, karena proses bisnis Souvenir Y ditangani secara mandiri (level mikro) dimulai dari pembelian bahan baku hingga produksi. Meskipun demikian, bisnis *Souvenir Y* memiliki manajemen risiko yang berhubungan dengan *operational risk* khususnya manajemen risiko kasus penipuan spesifikasi produk dan pencurian data pelanggan dari smartphone pribadi. Apabila akun media sosial dari *Smartphone* diretas, pemilik bisnis Souvenir Y telah menyiapkan backup data manual (hasil screenshot percakapan digital). Selanjutnya, manajemen risiko yang berhubungan dengan *customer risk* ialah manajemen risiko terjadinya kasus manipulasi data produk atau data transaksi, akses tidak sah ke data pelanggan atau akun yang diretas, komunikasi palsu mengatasnamakan pemilik akun bisnis *Souvenir Y,* serta sabotase informasi tentang nomor rekening bisnis *Souvenir Y.* Pemilik bisnis Souvenir Y selalu memberikan pernyataan atau pengumuman yang diposting pada akun media sosial terkait dengan keabsahan akun, agar konsumen tidak dijebak oleh kasus penipuan oleh oknum yang meniru akun media sosial busines *Souvenir Y.* Kendala yang dimiliki oleh pemilik bisnis *Souvenir Y* ialah keterbatasan modal finansial untuk mengurus legalitas produk menjadi hak kekayaan intelektual yang dilindungi hukum. Berdasarkan hasil identifikasi proses bisnis *Souvenir Y,* dapat diketahui bahwa manajemen *customer risk* lebih dominan dibandingkan dengan *operational risk.*

This study shows a fundamental difference between the risk management of the Coffeeshop X business and the Souvenir Y business. The risk management of the Coffeeshop X business is procedural and complex because it involves more than one system user. Meanwhile, the business process for marketing is carried out by the owner, while the production of food and beverages is explicitly handled by the kitchen (chef and assistant chef). Furthermore, the brewing and reservation sections are operated by the barista who doubles as an admin. It is different from the Souvenir business risk management, which is managed at the micro-level. It emphasizes the security of consumer data and information accumulated in the Souvenir Y business digital communication media (WA applications and IN social media). Case studies on Coffeeshop X and Souvenir Y in risk management show that the customer risk aspect is dominant, compared to the supplier risk and operational risk aspects. Thus it can be seen that the study of risk management related to information security awareness in MSMEs cannot be generalized and needs to be reviewed contextually based on business characteristics, products, market segmentation, business processes, number of workers, and technology used.

3.3 Engange Cybersecurity Awareness and Risk Management for Information Security Resilience in MSMEs

This study offers a model for realizing information security resilience by linking cybersecurity awareness and risk management in learning information security resilience for Micro, Small, and Medium Enterprises (MSMEs). The construction of ideas for designing models is interpreted based on various negligence of business actors in understanding business processes and the needs of technology tools. In addition, the dominance of socio-cultural aspects in the economic dimension, especially in business, has led to the indecisiveness of system access mobility based on user authority. Also, through Coffeeshop X and Souvenirshop Y, the use of information technology tends to follow the trend or popularity of the market without understanding the scale of the business and the business processes involved. In addition, employees who work at Coffeeshop X and Souvenirshop Y can access the system without any usage restrictions based on authority so that they are vulnerable to abuse.

In Micro, Small, and Medium Enterprises (MSMEs), professional teamwork tends to be weak because the working relationship is dominated by mutual trust between business owners and working employees. Therefore, a professional attitude in administrative matters needs to be applied as a work culture by reminding various aspects of information security vulnerabilities that may occur and the risk of employee negligence on business continuity. In the context of Coffeeshop X and Souvenirshop Y, a work culture that relies on social values needs to be balanced with the value of professionalism that adheres to the business system. It is necessary to reduce business obstacles caused by the lack of awareness about cybersecurity without proper risk management. This study offers a constructive idea to realize information security resilience in MSMEs, as shown in Figure 2.

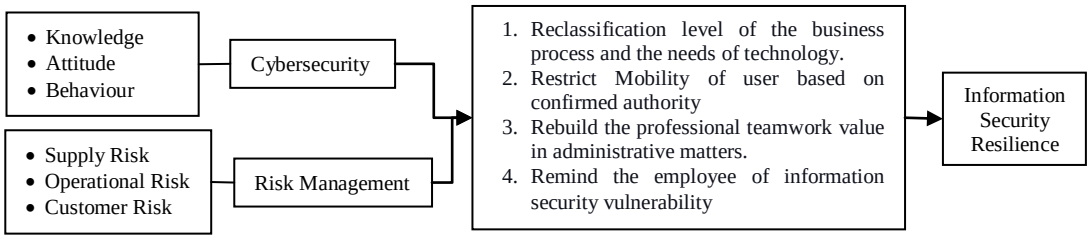

Figure 2. Information Security Resilience Model for MSMEs
Source : Reconstructed from Empirical Data

Figure 1 is a recommendation from this research for efforts to maintain information security based on the results of cybersecurity and risk management analysis, namely: first, reclassification of business security levels based on the characteristics of technology devices used to support business processes; second, limiting the mobility of system users based on the employee's authority which the business owner has validated; third, rebuilding the value of professional teamwork in administrative matters; fourth, remind employees regularly about the vulnerability aspects of business information security. These four things are reconstructed from the results of the Coffeeshop X and Souvenirshop Y case studies. Previous studies examining cybersecurity and risk management in the MSME sector have not presented a contextual idea regarding maintaining business information security based on business characteristics. Through this study, the description of the Coffeeshop and Souvenirshop business processes that are managed independently or based on a team needs to pay attention to the resilience of information security caused by weak knowledge, attitudes, and behavior. Moreover, running a business by ignoring the risk of information security in supply, operational, and customer aspects.

The limitation in this research is the reconstruction of ideas that rely on micro and small-scale businesses from a holistic study of MSMEs. In addition, the adoption of qualitative methods as an approach that prioritizes the depth of information has ignored the generalization of the MSME business. However, this research has succeeded in capturing the characteristics of

MSME businesses in Indonesia, especially on the micro and small scale, which still shows gaps in previous research. The recommendation for further research is to compare the results of this study by connecting aspects of cybersecurity, risk management aspects with the business model canvas in case studies that represent the characteristics of Micro, Small, and Medium Enterprises in Indonesia. Thus, this kind of research can contribute to the development of science in business system security that connects information technology, information systems, economics, and MSMEs.

4. CONCLUSIONS

This research shows that team-managed businesses have a higher vulnerability than individual-managed businesses. Based on case studies on MSME Coffeeshop X and Souvenir Y, the use of information systems for recording transactions and product marketing involving more than one system user has a higher level of vulnerability than information systems for transactions processing and product marketing operated by one person. According to the aspects of knowledge, attitude, and behavior, the classification of information security awareness shows that the level of expertise about Cybersecurity and Cyber Crime at a low or medium level is not always the same as the level of attitude and behavior of system users. It shows that the level of knowledge, attitudes, and behavior about information security awareness is highly dependent on product characteristics, business processes, and the number of system users. Furthermore, risk management at Coffeeshop X and Souvenir Y is very dominant in customer risk compared to supplier risk and operational risk. Thus it can be seen that the study of risk management related to information security awareness in MSMEs cannot be generalized and needs to be reviewed contextually based on business characteristics, products, market segmentation, business processes, number of workers, and technology used. This study offers an idea to overcome this problem, namely by considering the following four aspects: first, reclassification of business security levels based on the characteristics of technology devices used to support business processes; second, limiting the mobility of system users based on the employee's authority which the business owner has validated; third, rebuilding the value of professional teamwork in administrative matters; fourth, remind employees regularly about the vulnerability aspects of business information security. Thus, information security resilience is realized for business continuity.

ACKNOWLEDGEMENTS

I want to thank all the informants who have participated in this research. I also thank the Atma Jaya Catholic University of Indonesia and Satya Wacana Christian University.

REFERENCES

[1] G. Rahmadi and A. Raf'ie Pratama, "Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia," *Automata*, vol. 1, no. 2, pp. 1–7, 2020, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/15399.

[2] S. F. Aboelfotoh and N. A. Hikal, "A review of cyber-security measuring and assessment methods for modern enterprises," *Int. J. Informatics Vis.*, vol. 3, no. 2, pp. 157–176, 2019, doi: 10.30630/joiv.3.2.239.

[3] F. Anwar, B. U. I. Khan, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A comprehensive insight into game theory in relevance to cyber security," *Indones. J. Electr. Eng. Informatics*, vol. 8, no. 1, pp. 189–203, 2020, doi: 10.11591/ijeei.v8i1.1810.

[4] S. Aritonang, H. Yulieanto, and D. D. A. Rajab, "Internet Eavesdropping : Information Security Challenge in the Cyberspace," *J. Pertahanan*, vol. 4, no. 1, pp. 61–75, 2018,

[Online]. Available: http://jurnal.idu.ac.id/index.php/DefenseJournal/article/view/253/pdf4.

[5] F. T. Riadi, A. D. Manuputty, and A. Saputra, "Evaluasi Manajemen Risiko Keamanan Informasi Dengan Menggunakan COBIT 5 Subdomain EDM03 (Ensure Risk Optimisation) (Studi Kasus : Satuan Organisasi XYZ – Lembaga ABC)," *JUTEI*, vol. 3, no. 1, pp. 1–10, 2018, doi: 10.21460/jutei.2018.12.53.

[6] A. Z. Maingak and L. D. Harsono, "Information Security Assessment Using Iso / Iec 27001 : 2013 Standard," *Trikonomika*, vol. 17, no. 1, pp. 28–37, 2018, [Online]. Available: http://journal.unpas.ac.id/index.php/trikonomika/article/view/1138/618.

[7] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)," *Bull. Comput. Sci. Electr. Eng.*, vol. 1, no. 1, pp. 1–11, 2020, doi: 10.25008/bcsee.v1i1.2.

[8] P. D. Ibnugraha, L. E. Nugroho, and P. I. Santosa, "An approach for risk estimation in information security using text mining and jaccard method," *Bull. Electr. Eng. Informatics*, vol. 7, no. 3, pp. 393–399, 2018, doi: 10.11591/eei.v7i3.847.

[9] I. G. N. Mantra, "The Modeling of Information Security Classification With Risk Value Assesment Factor to Good Information Governance on The Indonesia Higher Education Sector," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 3, no. 1, pp. 12–22, 2016.

[10] W. B. W. Ismail, R. A. T. R. Ahmad, S. Widyarto, and K. A. Ghani, "A generic framework for information security policy development," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 2017-Decem, no. September, pp. 19–21, 2017, doi: 10.1109/EECSI.2017.8239132.

[11] Dafid and Dorie, "Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 11–20, 2020, doi: 10.35957/jatisi.v7i1.296.

[12] I. R. Munthe and I. Purnama, "Uji Tingkat Kesadaran Keamanan Informasi Pengguna Smartphone (Studi Kasus: Amik Labuhan Batu)," *J. Tek. Inf. dan Komput.*, vol. 2, no. 2, pp. 156–165, 2019, doi: 10.37600/tekinkom.v2i2.113.

[13] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *J. Sist. Inf. Bisnis*, vol. 8, no. 2, pp. 115–122, 2018, doi: 10.21456/vol8iss2pp1-8.

[14] D. C. Islami and K. B. I. H. Candiwan, "Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia," *J. INKOM*, vol. 10, no. 1, pp. 1–8, 2016, doi: 10.14203/j.inkom.428.

[15] A. D. Smith and W. T. Rupp, "Issues in cybersecurity: Understanding the potential risks associated with hackers/crackers," *Inf. Manag. Comput. Secur.*, vol. 10, no. 4, pp. 178–183, 2002, doi: 10.1108/09685220210436976.

[16] A. S. Firdaos, "Sistem Pengamanan dan Pemantau Sepeda Motor Menggunakan NFC (Near Field Communication) dan GPS (Global Positioning System) Security and Monitoring System in Motorcycle Using NFC (Near Field Communication) and GPS (Global Positioning System)," vol. 5, no. 1, 2017.

[17] R. Z. Yousif, S. W. Kareem, and S. M. Abdalwahid, "Enhancing Approach for Information Security in Hadoop," *Polytech. J.*, vol. 10, no. 1, pp. 81–87, 2020, doi: 10.25156/ptj.v10n1y2020.pp81-87.

[18] D. Efstathiou, "A collaborative physical layer security scheme," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 3, pp. 1924–1934, 2019, doi: 10.11591/ijece.v9i3.pp1924-1934.

[19] P. T. Tin, D. H. Ha, M. Tran, and T. T. Trang, "Physical security layer with friendly jammer in half-duplex relaying networks over rayleigh fading channel: Intercept probability analysis," *Bull. Electr. Eng. Informatics*, vol. 9, no. 4, pp. 1694–1700, 2020, doi: 10.11591/eei.v9i4.2249.

[20] Sumantri, "The Urgency of National Security Council (NSC) in the Context of Cyber Security as a Sub System of National Security to Protect State and People," *J. Soc. Polit.*

Sci., vol. 1, no. 1, pp. 71–75, 2020.
[21] S. S. Aulianisa and I. Indirwan, "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia," *Lex Sci. Law Rev.*, vol. 4, no. 1, pp. 33–48, 2020, doi: 10.15294/lesrev.v4i1.38197.
[22] L. Hadington, "Employees Attitude towards Cyber Security and Risky Online Behaviours : An Empirical Assessment in the United Kingdom," *Int. J. Cyber Criminol.*, vol. 11, no. 1, pp. 262–274, 2018, doi: 10.5281/zenodo.495776.
[23] T. Halevi, N. Memon, and J. Lewis, "Cultural and psychological factors in cyber-security," *J. Mob. Multimed.*, vol. 13, no. 1–2, pp. 43–56, 2017.
[24] F. Kwarto and M. Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *J. Akunt. Bisnis*, vol. 11, no. 2, pp. 99–110, 2018, doi: 10.30813/jab.v11i2.1382.
[25] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: a review and research agenda," *Supply Chain Manag.*, vol. 25, no. 2, pp. 223–240, 2020, doi: 10.1108/SCM-10-2018-0357.
[26] M. S. Ansari, "Information System Security (Cyber Security)," *J. Inform.*, vol. 2, no. 1, pp. 189–197, 2016, doi: 10.31311/ji.v2i1.60.
[27] A. Setiyanigrum and H. Hidayat, "Service Quality dan Kepuasan Konsumen : Studi Empiris dan Implikasinya pada Toko Online," *J. Ilm. Manaj.*, vol. 6, no. 2, pp. 247–260, 2016.
[28] R. Rachmatullah and R. Yanto, "Sistem Penjualan Online Spare Part Mobil di Toko Citra Abadi Motor Semarang," *Indones. J. Netw. Secur.*, vol. 5, no. 3, pp. 56–62, 2016.
[29] R. R. Febriani and B. Sudaryanto, "Pengaruh Brand Image dan Kualitas Layanan Terhadap Kepercayaan dan Keputusan Pembelian pada Toko Online (Studi Pada Konsumen OLX.co.id di Kota Semarang)," *Diponegoro J. Manag.*, vol. 7, no. 2, pp. 1–11, 2018.
[30] F. Alwafi and R. H. Magnadi, "Pengaruh Persepsi Keamanan, Kemudahan Bertransaksi, Kepercayaan terhadap Toko dan Pengalaman Berbelanja terhadap Minat Beli Secara Online pada Situs Jual Beli tokopedia.com," *Diponegoro J. Manag.*, vol. 5, no. 2, pp. 1–15, 2016.
[31] A. Mohansyah and R. Parani, "Digital Online Dan Trust Dalam Hubungan Antara Tokopedia Dengan Penguna Layanan," *J. Lontar*, vol. 6, no. 1, pp. 58–68, 2018.
[32] S. Pandey, R. K. Singh, A. Gunasekaran, and A. Kaushik, "Cyber security risks in globalized supply chains: conceptual framework," *J. Glob. Oper. Strateg. Sourc.*, vol. 13, no. 1, pp. 103–128, 2020, doi: 10.1108/JGOSS-05-2019-0042.
[33] M. Setiawardani, "Peran Servicescape Terhadap Peningkatan Loyalitas Pelanggan (Kajian Empiris terhadap Pelanggan Yumaju Coffee)," *J. Ris. Bisnis dan Inov.*, vol. 7, no. 1, pp. 10–21, 2021.
[34] E. Irawan, "Analisis Faktor – Faktor Yang Mempengaruhi Pendapatan Anggota Kelompok Sadar Wisata Pada Usaha Industri Kecil Kerajinan Souvenir Di Kota Mataram," *J. Ekon. dan Bisnis Indones.*, vol. 2, no. 1, pp. 1–10, 2017, doi: 10.37673/jebi.v2i1.47.
[35] A. T. Novitasari, "Pelatihan Membuat Kerajinan Souvenir Rangka Besi untuk Meningkatkan Keterampilan Berwirausaha," *JAPI*, vol. 5, no. 2, pp. 124–131, 2020.
[36] D. Islamiyati and C. Chairy, "the Influence of Memorable Souvenirs Shopping Experience and Place Identity on Revisit Intention (the Case of Yogyakarta)," *J. Muara Ilmu Ekon. dan Bisnis*, vol. 5, no. 1, pp. 205–213, 2021, doi: 10.24912/jmieb.v5i1.11054.