The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1477-996X.htm

Received 25 March 2021
Revised 29 April 2021
14 May 2021
Accepted 14 May 2021

What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case

Ratna Yudhiyati and Afrida Putritama
Accounting Program, Faculty of Economics, Universitas Negeri Yogyakarta, Yogyakarta, Indonesia, and

Diana Rahmawati
Doctoral Program in Economics, Universitas Sebelas Maret, Surakarta, Indonesia

Abstract

Purpose – This study aims to identify and analyse the issues faced by internet-based small businesses in developing countries regarding cybersecurity and document how these businesses address the risks.

Design/methodology/approach – This study used the qualitative method. Respondents were internet-based small businesses selected by using theoretical sampling. Data were collected by using interviews and observations. The validity of the analysis was ensured by using triangulation and member checking.

Findings – This study reveals that small businesses managed to identify the loss of physical and monetary assets as possible damage. However, only a few businesses identified loss of intangible assets as possible cyber risks. Most small businesses had used basic cybersecurity measures to protect data access and some primary business activities. Unfortunately, they rarely take initiatives in preventing and early detecting cyber risks.

Research limitations/implications – Findings of this study cannot be generalised as it aims to obtain new insights and document unexplored findings. Thus, if this study's findings are going to be generalised, it is necessary to conduct an additional study. Secondly, this study did not assess how far small business had fulfilled the relevant information security framework as assessment required additional research, and this study only aimed to map the current situation in small businesses.

Practical implications – This study emphasised the importance of identifying valuable assets or resources when implementing cybersecurity measures. Focusing on security measures to protect identified assets from cyber risk will make the efforts more efficient and effective than using standardised cybersecurity measures. Third-party developers can also use this study to understand small businesses' current cybersecurity implementation and their characters to design online platforms that suit these needs. Governments can also design educational activities that address small businesses' lack of knowledge.

Originality/value – Most studies which focus on small businesses and information technology (IT) usually only discuss how they use IT. This study also brings new contributions by focusing on developing countries and specifically addresses internet-based technology cyber risk faced by e-commerce businesses. The qualitative method is used as most studies in e-commerce adoption were positivistic in nature, and inductive-based studies were rarely found on the topic.

Keywords Qualitative study, Developing countries, Small business, Cybersecurity risk, Security measures

Paper type Research paper

This study was funded by Faculty of Economics, Universitas Negeri Yogyakarta, Indonesia.

Journal of Information, Communication and Ethics in Society
Vol. 19 No. 4, 2021
pp. 446-462
© Emerald Publishing Limited
1477-996X
DOI 10.1108/JICES-03-2021-0035

1. Introduction

The widespread use of mobile and cloud technology supported by growing internet coverage significantly transformed how people performed their activities. Smartphones and other connected devices allow people to obtain information quickly and to perform business transactions remotely. However, the growth of these technologies also brought new and unique security issues to users of the technologies (Sukumar and Edgar, 2009; Saleem *et al.*, 2017). The rapid growth of connected devices is also not followed by similar advances in security measures against cybersecurity attacks (Saleem *et al.*, 2017).

There had been a noticeable increase in cybersecurity attacks for the past few years, primarily because of the unsatisfying growth of security measures. While large enterprises had always been a popular target for hackers, there was a noticeable increase in attacks targeting small businesses for the past few years. It was estimated that 43% of recorded cybersecurity attacks targeted small businesses in 2015 (Symantec, 2016). Most small businesses tended to be vulnerable to cybersecurity attacks because they do not have adequate funds or human resources, which can be allocated to cybersecurity duties, and those who have tend to underappreciate cybersecurity threats (Rahman and Lackey, 2013; Saleem *et al.*, 2017). This behaviour can create negative impacts on small businesses in the future if the proper security measures are not implemented.

Cybersecurity risk is identified as one of the main concerns for small businesses in using information technology (IT) (Iddris, 2012; Grant *et al.*, 2014; Nugroho *et al.*, 2017). This concern is reasonable because cybersecurity incident in an organisation will be costly and negatively affect an organisation's operation and reputation (Kaušpadienė *et al.*, 2019). However, small businesses' decision to adopt IT is greatly influenced by the environment or external pressures (Perdana, 2011; Kurnia *et al.*, 2015). Small businesses in many countries are forced to start using IT to fulfil customer's demands or compete against competitors. Thus, they are put in a situation where they must implement IT despite being a potential victim of a cybersecurity attack, which they have difficulties preventing.

Only a few studies explored how small businesses respond to cybersecurity risks as the studies that focus on small businesses and IT usually only discuss how small businesses use IT (Berry and Berry, 2018). However, there were several noteworthy exceptions. Kaušpadienė, Ramanauskaitė and Čenys (Kaušpadienė *et al.*, 2019) assessed existing information security frameworks to evaluate their suitability for small and medium enterprises (SMEs) and defined which criteria are the most relevant for SMEs. Several studies focused on identifying what SMEs had done regarding cybersecurity risks and decisions (Yildirim *et al.*, 2011; Osborn and Simpson, 2017; Berry and Berry, 2018).

However, most of these studies were conducted in developed countries, and the difference in infrastructure, market and other landscapes between developed and developing countries may make these previous findings inapplicable in developing countries (Kabanda *et al.*, 2018). A study about IT adoption in Indonesia provided additional evidence that security concern is one factor that makes SMEs hesitant to use IT (Maryeni *et al.*, 2012; Nugroho *et al.*, 2017). Unfortunately, security concern is usually only one of the topics discussed in SME e-commerce adoption studies and additional studies that focus on how small businesses responded to this wariness was lacking. Kabanda *et al.* (2018) addressed this issue by exploring how South African small businesses perceive cybersecurity risk, and the study found that small businesses cybersecurity practice was influenced by budget, management support and attitudes. Unfortunately, this study was the only one that we found.

Other important topics that are rarely explored are the rising popularity of the internet of things and internet-based technology on small businesses, especially considering the growing e-commerce industry. Existing studies mostly focus on IT as a whole and rarely analysed the unique impacts and security risks created by the usage of these technologies in small businesses.

This study seeks to identify and analyse how Indonesian small businesses that operate in the digital market perceive cybersecurity risk. We selected Indonesia as a country to represent developing countries' small businesses as e-commerce transactions are gaining widespread use in Indonesia, and its vast population provides an excellent opportunity for growth of e-commerce business (Budiono *et al.*, 2018). The number of internet-based small businesses in Indonesia had also grown significantly for the past few years. Thus, it is crucial to understand how much Indonesian small businesses understood cybersecurity risk and what they had done to address the risk. The research questions addressed are:

RQ1. How do small businesses in developing countries that have used the internet in their operation view cybersecurity risk?

RQ2. How do small businesses in developing countries that have used the internet in their operation respond to cybersecurity risk?

This study used qualitative methods as most e-commerce adoption studies were positivistic in nature, and inductive-based studies were rarely found on the topic (Kabanda and Brown, 2017). New findings that can be found from the qualitative study will be helpful for both decision-makers and researchers to design policies or advice for small businesses in overcoming cyber risks in current digital markets.

2. Literature review

2.1 Defining small businesses

The term of small business is difficult to be defined. One of the most used definitions of small business in Indonesia is provided by Law (*Undang-undang*) number 20/2008. The law classifies small businesses into three groups, which are micro, small and medium enterprises (MSMEs). Each type of enterprise is classified based on the total value of its assets or turnover per year. Micro-enterprise is a business whose net assets, excluding land and building, is Rp 50,000,000 at most or whose turnover is Rp 300,000,000 per year at most. A small enterprise is a business whose net asset, excluding land and building, is between Rp 50,000,000 and Rp 500,000,000, or whose turnover is between Rp 300,000,000 and Rp 2,500,000,000 per year. Medium enterprise is a business whose net asset is between Rp 500,000,000 and Rp 10,000,000,000 or whose turnover is between Rp 2,500,000,000 and Rp 50,000,000,000 per year. The enterprises should also not be a subsidiary of bigger enterprise to be qualified as MSME.

2.2 Previous studies about the use of information technology by small business

A comprehensive study about small businesses' resilience put great importance on the use of technology. Most small businesses acknowledge the importance of IT, and especially about improving their operation's efficiency and maintaining a relationship with customers and suppliers (Gunasekaran *et al.*, 2011). However, most small businesses only used IT for a single function, such as procuring or marketing, but not for an integrated supply chain activity (Gunasekaran *et al.*, 2011). Another study also found that most small businesses in developing and least developed countries mostly use websites for marketing purpose (Kabanda and Brown, 2017). However, despite only using information system for retailing activity, these small businesses have advantages compared to traditional local businesses as they can reduce their cost structures by using the information system, specifically internet-based system (Lee and Cheung, 2004).

Many studies identified small business' challenges in adopting IT. The lack of established regulatory systems, costly initial investment and security issues were identified as the top three most important reasons why small businesses hesitated to adopt IT in Ghana (Iddris, 2012). Similar findings were found in Indonesia. Nugroho *et al.* (2017) found that security concern, the lack of skills and the high cost of infrastructure are some barriers that make Indonesian small businesses hesitate to use IT. Indonesian small businesses reasoned that IT infrastructure is too costly for companies of their size. The study also noted that respondents were worried that technology exposure would expose them to false information (namely "hoax"), which may harm their decision-making. They were also worried about the possibility that competitors would obtain information about their products and service through IT, which can be classified as information leakage (Nugroho *et al.*, 2017).

Based on these studies, several main factors that prevent small businesses from adopting IT were regulation, cost and security concerns (Iddris, 2012; Nugroho *et al.*, 2017). The regulation issue can be addressed by introducing new regulations that are IT-friendly for small businesses. The government can also address cost issues by improving infrastructure (e.g. better and cheaper internet connection) or changing regulation (e.g. reducing import duty for IT purchase by small businesses) (Roosdhani *et al.*, 2012). However, few studies had addressed the security concern issue.

The security issue is regarded as the greatest threat to IT usage by small businesses (Grant *et al.*, 2014). The security issue is also a matter of perception, so it is greatly influenced by the human's perspective (Grant *et al.*, 2014). Governments can do their best to improve IT security, but small businesses may not care because they still perceive IT as a "risky thing". Thus, this issue needs to be addressed by directly asking small businesses' owners what they need to solve their IT issues. This idea was also supported by a previous study, which found that owners and their perception are some of the most significant factors which determined IT adoption by MSME and the success of the adoption (Rahayu and Day, 2015).

Kabanda *et al.* (2018) is one of the rare studies that specifically address small business attitude to cybersecurity risk. The study found how small business perceived cybersecurity risk was influenced by budget constraints, management support and general attitude to cybersecurity risk (Kabanda *et al.*, 2018). These three factors tend to affect cybersecurity implementation in small businesses negatively.

2.3 Information security framework

An information security framework is a guideline used by organisations to design an information security management strategy. The lack of proper security strategy may lead to inefficient use of resources spent for cybersecurity implementation (Kauspadiene *et al.*, 2017). Thus, selecting an appropriate information security framework is an important decision for adequately addressing cybersecurity risk.

Several organisations and studies introduced some information security management frameworks for the past few years. Unfortunately, most security frameworks are not fully compatible with small businesses as most of them are too complicated to be applied by small businesses that have limited resources (Kaušpadienė *et al.*, 2019). One of the information security frameworks applicable for small businesses is the SABSA information security framework.

Sherwood Applied Business Security Architecture (SABSA) model is applicable for small businesses because the model provides an adjustable and scalable guideline instead of a list of requirements. SABSA model consists of six layers, representing a different stakeholder's view in an information security architecture model (Sherwood *et al.*, 1995). The six layers are as follows:

(1) The business view, which focuses on the business owner's interpretation.

(2) The architect's view, which focuses on grand vision and high-level description
(3) The designer's view, which consists of a logical structure derived from the architect's vision.
(4) The builder's view, which focuses on how the logical structure is turned into a technology model.
(5) The trademan's view, which focuses on combining and installing various products with different purposes to function properly.
(6) The service manager's view, which focuses on the manager who uses and maintain the information system.

The business view is also termed contextual security architecture. It is an important foundation of an information system architecture that describes the business requirements for achieving a secure system (Sherwood *et al.*, 1995). Business needs should drive the information and communications technology vendor to design the applications and system that answer the businesses' needs instead of otherwise. The business view is the primary concern of small businesses as this is an information system architecture's aspect where the business owner has complete control.

SABSA model asked business owners to ask themselves of six issues. The issues are:

(1) *what* (what assets to be protected and what the business needs for information security);
(2) *why* (the risks which drive the needs for business security);
(3) *how* (business operations and transactions that need to be protected);
(4) *who* (insiders and business partners who are involved in securing the information system);
(5) *where* (location-related aspects of business security); and
(6) *when* (time-related aspects of business security which need to be considered to suit the business' needs) (Sherwood *et al.*, 1995).

Answers to these questions indicate that a business has a strong idea about their cybersecurity needs, while the absence of responses may indicate a lack of proper foundation. Thus, it is an interesting topic to find out whether small businesses had a general idea about these issues or not.

3. Research methodology

3.1 Research design and questions

This study is a comparative case study that used the qualitative method. The case study approach is used when researchers seek to comprehend dynamics within single settings (Eisenhardt, 1989). An important initial step of a case study is defining initial research questions. These questions can evolve as new findings are found, but a starting point is necessary (Agee, 2009).

There are five initial questions addressed in this study. The five questions were derived from the six questions guidelines of the SABSA information security framework, excluding the *where* part of the question guideline. This part was excluded as our population is mobile and internet-using small businesses whose operation is not limited by geographical location. Our initial research questions are as follows.

- What are situations and losses which can be considered as cybersecurity risks by small businesses?

- Why do small businesses use security countermeasures?

- How do small businesses secure their operations from cybersecurity risk?

- Who are regarded as relevant individuals by small businesses regarding their cybersecurity?

- How long are small businesses willing to let an identified cybersecurity risk exist in their system?

3.2 Data collection

The population of this study is a group of Indonesian small businesses that use internet-based technology to market or provide goods or services for their customers. Small businesses that only use offline, local area network or extranet-based technologies were not considered as part of this study's population. Small businesses that only use internet-based technologies for activities not directly related to marketing and selling goods or services (such as cashless payment) were also excluded. Some examples of internet-based technologies used by small businesses which make them included as our population are as follows, but not limited to:

- Using social media (such Facebook or Instagram), online marketing websites (such as OLX.co.id) or other online advertisements (such as Google AdSense) to receive orders from customers. Then, sellers contact customers directly by using other communication methods.
- Using virtual marketplaces (such as Bukalapak, Tokopedia and Shopee) or other third-party applications (such as GoJek and Grab), which act as a mediator to receive customers' orders, communicate with customers and process customers' payments.
- Using the company's own website to receive orders, process transactions, receive payments and communicate with customers.

Samples were selected using theoretical sampling, a method commonly used in qualitative studies (Eisenhardt, 1989). The sampling strategy used in this study is *criterion* strategy, where researchers defined a list of criteria, and all cases that meet them are selected as samples (Creswell and Poth, 2018). Sample size did not matter much in this study as selecting samples that fulfil the defined criteria is the essential part of the sampling process. Qualitative studies tend to have a great range of sample sizes which depend on the type of study (Creswell and Poth, 2018).

Respondents for this study were selected by following several steps. Firstly, we obtained a list of small businesses which used IT in their operation. The list was derived based on the attendance list of a seminar for small businesses held by us. The seminar was training for small businesses to address cybersecurity risks held in Yogyakarta, Indonesia. Secondly, we identified small businesses which used internet-based technology based on questionnaires they filled in the seminar. Thirdly, we selected possible respondents based on the list by considering two criteria: there should be at least two respondents for each type of small business defined in Law (*Undang-undang*) number 20/2008 about MSME in Indonesia, which are micro enterprise, small enterprise and medium enterprise; and technologies used by the selected respondents should represent as many examples of internet-based technology as possible. Fourthly, we contacted possible respondents to ask their willingness to be our respondents. We managed to obtain six respondents for our study, which fulfilled the listed criteria and expressed a willingness to collaborate. The six respondents consist of two businesses for each category of MSMEs.

This study combined interviews and observations to collect research data. The interviews were conducted based on a pre-arranged interview guide. The interview guides were developed by involving several stakeholders, which is an effort to improve qualitative research questions in thoughtful and interactive ways (Agee, 2009). Stakeholders involved in the question development step were professionals, academics and other internet-based small businesses that were not considered respondents. They were invited to a focus group discussion where their opinions and advice help us in arranging the interview guide. The interview was conducted for 15–30 min per session, and we interviewed some respondents several times when we needed additional information. The results of the interviews were documented in audio recordings and interview transcripts.

Observations were used by observing how the respondents' website, social media page, virtual shop or other similar accounts were used by both respondents (business owners) and their customers. We asked respondents to show us how they used their online platforms, and we observed customers' activity in the respondent' online platforms by checking customers' reviews, comments and messages in the online platforms. We used observation data to confirm some findings obtained from interview. For example, when a respondent mentioned that he regarded reputation and customer's satisfaction as valuable assets, we checked his online market platform to analyse how he responded to customer's reviews and feedbacks. Prompt and welcoming replies will confirm his statement, while slow or no replies will motivate us to question him further.

3.3 Data analysis

This research used content analysis to analyse the data obtained from interviews. Content analysis can analyse the text data obtained in a case study research (Kohlbacher, 2006). The validity of the analysis was maintained by using triangulation and member checking; two validity procedures were used when analysing qualitative inquiry (Creswell and Miller, 2000). Two different persons made interview transcripts for each respondent. The transcripts were later reviewed together, and any discrepancies were settled. After finalising the transcripts, we sent the final interview transcript to respective respondents to confirm whether we managed to write their inquiry result correctly or not. The data analysis process of the finalised transcripts was performed by two different researchers separately. These researchers discussed the results of their individual analysis and discussed them together to find a joint conclusion if they found any differences.

Firstly, we read interview transcripts a few times to get a general idea of what the respondents were talking. We identified and selected statements in the interview transcripts, which can answer the research questions described in the previous section. The statements were divided into smaller parts while retaining the core meaning of the text, which are called condensed meaning units (Erlingsson and Brysiewicz, 2017).

The next step is labelling these units by putting code for each of them to identify various respondents' idea who have similar gist. We used hierarchical coding where similar codes are clustered together to create more general, higher-level codes (Cassell and Symon, 2004). This study defined higher-level codes as categories that are expected to start providing answers for the research questions (Erlingsson and Brysiewicz, 2017). These category names are short, but they are factual sounding, compared to codes with little meanings for people who do not read the interview transcripts. This study continued to group categories into themes. We identified five initial themes at the beginning of this study derived from the five initial questions.

Findings and conclusions derived from the interviews were cross-checked to our observation results. We compiled a table of tabulated evidence to keep track of evidence supporting our conclusions. We wrote structured descriptions about the answers to our research questions and their analysis based on these pieces of evidence.

4. Result and discussion

4.1 Respondents' profile

Table 1 described some background information of our respondents. This information would be useful for analysing the results of our study.

All respondents use internet-based technology for marketing purposes. The popularity is reasonable as online presence allows businesses to expand their market in cheaper ways than physical presence. The popularity applies to both businesses that sell products and services. We also noticed that two respondents who have the highest turnover prefer to have their own website to conduct their business instead of using websites or online platforms provided by third party. It can be inferred that bigger-size small businesses have better resources than smaller-size businesses. Unfortunately, a relationship between businesses' size and their decision to use technologies cannot be summarised, and any conclusion requires further testing.

4.2 Findings and analysis

4.2.1 Theme 1: situations and losses which can be considered as cybersecurity risks by small businesses. All respondents acknowledged that using internet-based technology provides a big chance for hackers to target them. They understood that there is no fully secured IT. This opinion was expressed in the following statement from one of the respondents, KA.

> I realised that using online platforms, such as websites, social media, Line or WhatsApp, for selling products bears risks. No matter how advanced information technologies are, they will be obsolete one day. It is also similar to security measures. We had used firewalls and verification code for securing transactions, but they can not ensure that our system will be 100% safe from hackers. – KA

Unfortunately, despite knowing that *there are risks* in using internet-based technology, most respondents admit that they did not know for sure *what* the risks are. When respondents were asked to list some possible ways for hackers to deceive them, steal data or disrupt their system, they admit that they can only list few ways they almost fell victim to.

Their answers can be grouped into two groups. Firstly, respondents mentioned cybersecurity attacks whose main objective is disrupting or damaging respondents' IT itself. Secondly, respondents also identified attacks that seek to disrupt their operation or stealing resources by using their internet-based technologies, but these attacks did not damage the technology itself.

The cybersecurity attacks which respondents had experienced are described in detail in Table 2.

Table 2 showed that four respondents had experiences in being targeted by cybersecurity attacks. There is no recognisable pattern of attacks. It is understandable that KA, being a bigger-size business compared to other respondents, was targeted more

Table 1.
Respondents' profile

Respondent's initial	Business activity	Turnover per year	Internet-based technologies used in business
KA	Manufacturing and selling products	Rp 3bn	Using the company's own website for advertising, receiving order and keeping track of inventory
BB	Service	Rp 360m	Using the company's own website for advertising and receiving order form customers
AH	Service	Rp 180m	Using an advertisement website to publish information about the business to potential customers
AB	Selling products	Rp 72m	• Using social media for advertising • Using virtual marketplaces for advertising, receiving order and processing payments from customers
JA	Selling products	Rp 48m	• Using social media for advertising • Using virtual marketplaces for advertising, receiving order and processing payments from customers
WJ	Manufacturing and selling products	Rp 10m	• Using social media for advertising and purchasing raw materials from suppliers • Using virtual marketplaces for advertising, receiving order and processing payments from customers

frequently by various attacks. However, JA admitted being targeted several times, which is more frequent than other bigger respondents, excluding KA. Thus, we cannot conclude that bigger-size businesses are targeted more frequently by cybersecurity attacks than smaller-size businesses.

Another important point is respondents recognising that hackers can use their system to target their customers instead of themselves. Respondents realise a considerable risk of customer's dissatisfaction and loss of trust, which may affect their business in the long term. Respondents who admit to being a victim of this kind of attack were KA and BB. BB specifically mentioned the threat of losing customer's trust because of this attack.

> If our website has good security, customers will feel secure and willing to use the website. However, if they do not trust the company's website, the website will be obsolete, and our business suffers. – BB

Respondents who raised this wariness over losing customers' trust were only KA, BB and AB. It can be determined that KA and BB have a high awareness of this issue because they were our only respondents who use their own website for business. They have higher control of their own website compared to other respondents who use third-party platforms.

Table 2.
Respondents' experience in being targeted by cybersecurity attacks

Group	Group description	Cybersecurity attacks identified	Respondents
1	Attacks whose main objective is disrupting or damaging respondents' IT itself	Virus, hacked website and hacked accounts	KA, JA
2	Attacks which seek to disrupt their operation or stealing resources by using their internet-based technologies, but these attacks did not damage the technology itself	Fake payment, website impersonating and fake order	KA, BB, JA, AH

Thus, customers are more likely to hold them accountable than other businesses that use platforms provided by a third party. Another respondent, AB, also expressed the importance of providing testimonies and other efforts to ensure the customer's trust in the business. However, the respondent admitted that it did not think that insecure social media will damage its reputation as it only uses social media and virtual marketplace instead of the company's own website.

Summarising our respondents' answers, we can identify what the small businesses thought and perceive regarding two aspects of the information security framework. The summary is explained in Table 3.

Most respondents identified the loss of computers or cost, which need to be paid to solve the security issue caused by hacker attacks, computer virus or worm, as online risks. The only respondent who did not feel threatened by a possible loss of assets caused by online risk is respondent WJ. The respondent admitted that she thought the business is too small, and the risk was very low to be targeted by those issues. A lax attitude to cybersecurity risks is commonly found in small businesses when they consider themselves to be too small to be concerned (Paulsen, 2016; Kabanda *et al.*, 2018). Our finding shows that there is a variety of cybersecurity awareness among small businesses. It is possible that this different level of cyber risk awareness was influenced by their size and exposure to mobile and internet-based technology (Rahmawati *et al.*, 2019).

The summary explained in Table 3 also showed that our respondents could identify *what* assets need to be protected from cybersecurity risks, though the identified assets were still too general. Proper identification of assets that need to be protected is an important step in implementing cybersecurity measures. Unfortunately, most small businesses simply follow existing security guidelines instead of actively selecting which assets they want to protect (Paulsen, 2016).

4.2.2 Theme 2: Why small businesses use security countermeasures? Respondents' decision to use internet-based technology was greatly affected by several factors. Firstly, respondents considered the possible benefits of using internet-based technology. All respondents mentioned practicality, market expansion, improving existing operations, keeping with competitors and flexibility as the main benefits of using internet-based technology. Secondly, respondents measured possible cost and risks which may arise from using internet-based technologies. Risks were considered as possible costs or loss of money, which may happen in the future. Thirdly, respondents considered other factors that may affect their decision, whether positively or negatively.

The summary of respondents' consideration in using and selecting the internet-based technologies to be used is described in Table 4.

Framework aspect	Description	Summary	Respondents
What	What are the situations and losses which can be considered as cybersecurity risks by small businesses?	a. Loss of asset (hardware and monetary)	a. KA, BB, AH, JA, AH
		b. Customer's trust in the business	b. KA, BB, AB
Why	Why do small businesses use security countermeasures?	c. Understanding the existence of online risk	c. All respondents
		d. Technical damage	d. KA, BB, AH, JA, AH

Table 3. *What* and *why* aspects of information security framework for business owner

Two additional factors that need to be considered in deciding to use internet-based technology and *what* technology to use are ease of use and how prevalent the technology is among the targeted market. The two factors are often related. Small businesses often selected internet-based technologies because their targeted customers use those technologies. An example of this consideration is Instagram as the most popular social media used for selling and marketing products than other social media. Their ease of use often causes the popularity of respective technologies. Most respondents explained that the platform, website or online features were selected based on how comfortable they feel. The platform or website should be easy to maintain and used by people with little knowledge of technology.

> My most important considerations in selecting information technology are ease of use, its security, and the cost needs to be paid for using it. – KA

Cybersecurity risk is a possible risk or cost, which may incur for the small business. Small businesses need to use internet-based technologies to obtain benefits, including competing against competitors. They need to bear the possible loss of using the selected technology. Security measures are used to reduce possible loss and relevant online risks. If possible, respondents tended to select internet-based technologies that provide the best security possible. Unfortunately, respondents also considered other factors, and security was not the top priority for our respondents.

Based on our respondents' answers, we can identify additional findings of what the small businesses thought and why they thought they needed to use security measures. The summary is explained in Table 5.

4.2.3 Theme 3: How small businesses secure their operations from cybersecurity risks? All respondents admit that they had taken some security measures to address cybersecurity risks. These security measures can be classified into three groups. The first group consists of security measures that focus on protecting the technology itself and prevent hackers from accessing it, such as firewall, antivirus and account passwords. All respondents used this measure, and other studies also found that it is the type of security measure most used by small businesses (Valli *et al.*, 2014).

The next group consists of policies, procedures and habits practiced by respondents whose objective is minimising cybersecurity breaches. The last type of security measure commonly used by our respondents is documentation. All respondents explained that they record all their transactions as completely as possible. They believed that comparing these records with their bank accounts would be very useful for finding issues. Unfortunately, maintaining a complete record of transactions is costly, so available resources greatly influence the quality of the records.

Table 4. Respondents' considerations in using and selecting internet-based technologies

No.	Classification	Consideration	Respondents
1	Possible benefits	Practical	KA, AB, WJ, JA
		Improving operation	KA, BB
		Expanding market	BB, WJ, JA
		Competing against competitor	All respondents
2	Possible loss	Cost, online risks	All respondents
3	Other consideration	Ease of use	KA, BB, WJ
		Security	KA
		Commonly used	AB, BB, WJ, JA

Table 6 provides a summary of measures performed by our respondents to address cybersecurity risks.

Our respondents admit that security measures were selected based on their limited knowledge, and they admit that they lack adequate knowledge. They expressed their disappointment that the government and other stakeholders consider cybersecurity an unimportant issue for small businesses. One of our respondents mentioned the following statement.

> Unfortunately, I never get any information or training about cyber risks from government, such as the Ministry of Trade. They may think that cyber risk is less important for small businesses like us. – BB

Based on our respondents' answers, we can identify what processes need to be protected and how to protect them in small businesses' opinions. The summary is explained in Table 7.

Table 7 identified that only some respondents managed to identify how they plan to protect themselves from cybersecurity risks. Unfortunately, most respondents relied heavily on third-party providers to secure the internet-based technologies they used. A detailed explanation is provided in Theme 4.

Table 5. *Why* aspects of information security framework for business owner (additional finding)

Framework aspect	Description	Summary	Respondents
Why	Why do small businesses use security countermeasures?	Reducing possible cost Losing against competitor	KA, BB KA, AB, BB

Table 6. Cyber risk countermeasures used by respondents

Group	Group description	Countermeasures performed	Relevant business process
1	Security measures which focus on protecting the technology itself and prevent hackers to access it	Security software, account login and password	Login and accessing data Hardware protection
2	Policies, procedures and habits practices by respondents whose objective is minimizing cybersecurity breaches	a. Standard operating procedures (SOPs) for receiving order, communicating with customers and processing payment b. Segregating duties between order receiving and payment processing c. Policies of changing password regularly d. SOPs for employees in using the business' IT	a.1 Receiving customer's order a.2 Communicating with customers b. Receiving customer's payment c. Login and accessing data d.1 Login and accessing data d.2 Hardware protection
3	Documentation	• Recording transactions automatically by using the online sales platform • Recording transactions manually	Maintaining accuracy of data

4.2.4 Theme 4: Who are the relevant individuals considered by small businesses regarding their cybersecurity? Customers, competitors and colleagues were essential in small businesses' decisions in using internet-based technologies. Most small businesses use existing internet-based technologies or services provided by third-party developers. Respondents also admitted that they selected technologies that are commonly used and trusted by their targeted customers. Thus, they tended to select internet-based technologies that were similar to those used by colleagues and competitors so customers can easily compare their technologies. If small businesses use a similar technology to those considered secure by society, other customers tend to trust the business website or virtual market, despite never performing a transaction with the respective business.

Another critical stakeholder regarding small businesses' cybersecurity is third-party developers. Most respondents used existing internet-based applications, websites or virtual marketplaces to conduct their business. The respondents who have their own website hire their website developer to provide maintenance and upgrade, while they only have small and limited control towards their own website. This dependency included the security maintenance and countermeasures of their technologies.

> The ones responsible for routine maintenance and security systems are marketplace administrator and social media administrator. I believed that the administrators had provided the necessary security and maintenance. – AB

This dependency is concerning as cyber risk is an internal control issue for a company (Smith *et al.*, 2019). Businesses are supposed to have control over their data, especially confidential data. High reliance of small businesses on third-party providers implied that small businesses need to select providers that can be trusted and are capable of securing their data.

Our findings showed that the government is expected to have a significant role in small businesses' cyber risk countermeasures. Some respondents expressed their hope in the government to provide them guidelines or support in combating cyber risks. KA and AB confessed that they would rely on law enforcement if they became victims of cybersecurity attacks. Some respondents also admit their disappointment that the Indonesian Government did not educate them on the importance of cybersecurity risk for small e-commerce businesses, as explained in Theme 3 analysis. A previous study found that small businesses are inclined to dutifully follow their government's policy in cybersecurity (Kabanda *et al.*, 2018). Thus, governments' policies or requirements about cybersecurity measures can improve the cybersecurity implementation in small businesses.

Framework aspect	Description	Summary	Respondents
How	How do small businesses secure their operations from cybersecurity risk?	a. Physical protection (protecting data and system access) b. Policies for receiving order, communicating with customers and processing payment c. Policies for employees in using the business IT (protecting the technology's hardware) d. Keeping proper business transaction (Maintaining accuracy of data)	a. KA, BB, JA b. KA, AB, BB c. BB d. WJ, JA

Table 7.
How aspect of information security framework for business owner

Based on our respondents' answers, we can identify stakeholders who influence small businesses' decisions regarding their technology and its respective security measures. The summary is explained in Table 8.

4.2.5 Theme 5: How long small businesses are willing to let an identified cybersecurity risk exist in their system? Many studies advised businesses to design security measures to prevent or early detect any existing security risks as preventing and detecting risks are less costly than detecting risks after they damage businesses' operation. Unfortunately, this attitude was almost not found in our respondents. All respondents explained that they did not think that routine maintenance was necessary and only inform third-party developers if they found any security issues. Some preventive measures they took were access protection and security policies. However, the only early detective measure was documentation, and it was only performed by two respondents, as discussed in Table 7. These attitudes indicated that respondents had a long time tolerance regarding cyber-attacks.

> We may consider routine maintenance when our business has grown significantly. For now, we do not think that that routine maintenance is necessary. We will face any issues when we find them. – BB

Unfortunately, this lax attitude was shared by other small businesses from different countries. Valli *et al.* (2014) found that only 40% of Western Australian small businesses implemented basic cybersecurity measures, such as firewall, virus scanner and other similar measures. Of this number, only 59% admit that they update their security software regularly (Valli *et al.*, 2014).

Based on our respondents' answers, we can identify the small businesses' time-tolerance regarding cybersecurity attacks. The summary is explained in Table 9.

5. Conclusion

Identifying important assets that need to be protected is an important step in cybersecurity implementation. Most respondents managed to identify possible monetary loss and system damage as possible cyber risk damage. Unfortunately, only some respondents managed to identify reputation and customer's trust towards the business as potential loss from cybersecurity attacks. They planned to address possible issues of technical damage and

Table 8. *Who* aspect of information security framework for business owner

Framework aspect	Description	Summary	Respondents
Who	Who are regarded as relevant individuals by small businesses regarding their cybersecurity?	Customers Competitors Colleagues Developers Government	All respondents All respondents All respondents All respondents KA, AB

Table 9. *When* aspect of information security framework for business owner

Framework aspect	Description	Summary	Respondents
When	How long small businesses are willing to let an identified cybersecurity risk exist in their system?	a. Security issues are only addressed when they are found b. Routine maintenance is unnecessary	a. All respondents b. All respondents

other additional costs which may arise if they became victims of cyber-attacks. Another significant risk they want to avoid is losing against competitors as secure technologies are important for customers in the current internet-based information system.

Most small businesses had used cybersecurity measures at a certain level. These security measures can be classified into three groups: security measures that focus on protecting the technology itself and preventing hackers from accessing it; measures that focus on policies, procedures and habits practiced by respondents whose objective is to minimise cybersecurity breaches; and the last type is documentation. Important business processes they wanted to protect were data access, receiving and processing customers' orders, processing payment receipts and recording business transactions.

Customers, competitors, colleagues and developers are important people who influence small businesses' decisions in selecting internet-based technologies and their security measures. However, the potential of government role in small businesses' cybersecurity implementation in Indonesia should not be overlooked. Currently, respondents thought that the Indonesian Government did not provide much help in educating small businesses about cyber risk, but they still hope that the government can help them in other aspects. Small businesses also much relied on third-party developers who design internet-based technologies used by most small businesses.

Unfortunately, small businesses rarely take initiative in preventing and early detecting cybersecurity attacks. They thought that routine maintenance and upgrade of their systems was an unnecessary additional cost and preferred to rely on third-party developers to update the security of their systems. These attitudes indicated their acceptance of slow response to cybersecurity countermeasures.

This study improved previous studies by identifying and analysing what small businesses thought about cybersecurity risks and their attitudes towards cybersecurity measures. While most previous studies discussed barriers and issues of small businesses' IT adoption in general, this study focused specifically on one of those barriers, the security concern. These findings would be beneficial to map and analyse how far internet-based small businesses had fulfilled the information security framework and assess their readiness to combat cyber risks.

This study advised internet-based small businesses to identify data, resources or assets that are important but were also threatened by cyber risk. This list will differ among businesses and depends on their activity. However, some assets are commonly important to all internet-based businesses, such as online platform access, monetary resources and reputation. Small businesses need to focus on using security measures that secure these assets instead of using standardised security measures. This focus will enable small businesses to implement cybersecurity measures more effectively and efficiently as each business has different needs and priorities.

Governments can use our findings to design training or educational activities that address specific small businesses' lack of knowledge or their weaknesses in cybersecurity implementation. Third-party developers and other interested parties can also use our findings to design the online platform that suits their targeted small businesses based on the small businesses' cybersecurity situation explained in the article.

6. Limitation and future research

This study had several limitations that need to be considered if this study's findings are used for future studies or decision-making. Firstly, we did not aim to generalise our findings to small businesses as our objective was to obtain new insights. Thus, it is necessary to conduct an additional study if this study's findings will be generalised. Secondly, this study did not assess how far small businesses had fulfilled the relevant information security framework as assessment required additional research, and this study only aimed to map the current situation in small businesses.

References

Agee, J. (2009), "Developing qualitative research questions: a reflective process", *International Journal of Qualitative Studies in Education*, Vol. 22 No. 4, pp. 431-447.

Berry, C.T. and Berry, R.L. (2018), "An initial assessment of small business risk management approaches for cyber security threats", *International Journal of Business Continuity and Risk Management*, Vol. 8 No. 1, pp. 1-10.

Budiono, F.L., Lau, S. and Tibben, W. (2018), "Cloud computing adoption for e-commerce in developing countries: contributing factors and its implication for Indonesia", *Pacific Asia Conference on Information Systems (PACIS) 2018*.

Cassell, C. and Symon, G. (2004), *Essential Guide to Qualitative Methods in Organizational Research*, Sage Publications Ltd, London.

Creswell, J.W. and Miller, D.L. (2000), "Determining validity in qualitative inquiry", *Theory into Practice*, Vol. 39 No. 3, pp. 124-130.

Creswell, J.W. and Poth, C.N. (2018), "Qualitative inquiry and choosing among five approaches".

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550, doi: 10.1016/s0140-6736(16)30010-1.

Erlingsson, C. and Brysiewicz, P. (2017), "A hands-on guide to doing content analysis", *African Journal of Emergency Medicine*, Vol. 7 No. 3, pp. 93-99.

Grant, K., Edgar, D., Sukumar, A. and Meyer, M. (2014), "Risky business: perceptions of e-business risk by UK small and medium sized enterprises (SMEs)", *International Journal of Information Management*, Vol. 34 No. 2, pp. 99-122.

Gunasekaran, A., Rai, B.K. and Griffin, M. (2011), "Resilience and competitiveness of small and medium size enterprises : an empirical research", *International Journal of Production Research*, Vol. 49 No. 18, pp. 5489-5509.

Iddris, F. (2012), "Adoption of e-commerce solutions in small and medium-sized enterprises in Ghana", *European Journal of Business and Management*, Vol. 4 No. 10, pp. 2222-2839, available at: http://pakacademicsearch.com/pdf-files/ech/517/48-57_Vol_4,_No_10_(2012).pdf

Kabanda, S. and Brown, I. (2017), "A structuration analysis of small and medium enterprise (SME) adoption of e-commerce: the case of Tanzania", *Telematics and Informatics*, Vol. 34 No. 4, pp. 118-132.

Kabanda, S., Tanner, M. and Kent, C. (2018), "Exploring SME cybersecurity practices in developing countries", *Journal of Organizational Computing and Electronic Commerce*, Vol. 28 No. 3, pp. 269-282.

Kaušpadienė, L., Ramanauskaitė, S. and Čenys, A. (2019), "Information security management framework suitability estimation for small and medium enterprise", *Technological and Economic Development of Economy*, Vol. 25 No. 5, pp. 979-997.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S. and Ramanauskaite, S. (2017), "High-level self-sustaining information security management framework", *Baltic Journal of Modern Computing*, Vol. 5 No. 1, pp. 107-123.

Kohlbacher, F. (2006), "The use of qualitative content analysis in case study research", *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, Vol. 7 No. 1, available at: https://epub.wu.ac.at/5315/.

Kurnia, S., Choudrie, J., Mahbubur, R.M. and Alzougool, B. (2015), "E-commerce technology adoption: a Malaysian grocery SME retail sector study", *Journal of Business Research*, Vol. 68 No. 9, pp. 1906-1918.

Lee, M.K.O. and Cheung, C.M.K. (2004), "Internet retailing adoption by small-to-medium sized enterprises (SMEs): a multiple-case study", *Information Systems Frontiers*, Vol. 6 No. 4, pp. 385-397.

Maryeni, Y.Y., Govindaraju, R., Prihartono, B. and Sudirman, I. (2012), "Technological and organisational factors influencing the e-commerce adoption by Indonesian SMEs", *2012 IEEE International Conference on Management of Innovation and Technology (ICMIT)*, pp. 436-441.

Nugroho, M.A., Susilo, A.Z., Fajar, M.A. and Rahmawati, D. (2017), "Exploratory study of SMEs technology adoption readiness factors", *Procedia Computer Science*, Vol. 124, pp. 329-336.

Osborn, E. and Simpson, A. (2017), "On small-scale IT users' system architectures and cyber security: a UK case study", *Computers and Security*, Vol. 70, doi: 10.1016/j.cose.2017.05.001.

Paulsen, C. (2016), "Cybersecuring small businesses", *Computer*, Vol. 49 No. 8, pp. 92-97, doi: 10.1109/MC.2016.223.

Perdana, A. (2011), "Isomorfisma dalam adopsi teknologi informasi pada usaha mikro, kecil dan menengah (UMKM)", *Seminar Nasional Aplikasi Teknologi Informasi 2011*, doi: 10.2139/ssrn.1916479.

Rahayu, R. and Day, J. (2015), "Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia", *Procedia – Social and Behavioral Sciences*, Vol. 195, pp. 142-150.

Rahman, S.S.M. and Lackey, R. (2013), "E-Commerce systems security for small businesses", *International Journal of Network Security and Its Applications*, Vol. 5 No. 2, pp. 193-210.

Rahmawati, D., Yudhiyati, R. and Putritama, A. (2019), "How micro and small enterprises perceive information technology fraud: a study of Indonesian' small businesses", *5th International Conference on Computing Engineering and Design, ICCED 2019*.

Roosdhani, M.R., Wibowo, P.A. and Widiastuti, A. (2012), "Informasi dan komunikasi pada usaha kecil", *Jurnal Dinamika Ekonomi Dan Bisnis*, Vol. 9 No. 2, pp. 89-104.

Saleem, J., Adebisi, B., Ande, R. and Hammoudeh, M. (2017), "A state of the art survey – impact of cyber attacks on SME's", *ACM International Conference Proceeding Series*.

Sherwood, J., Clark, A. and Lynas, D. (1995), "Enterprise security architecture", *SABSA*, White Pape, doi: 10.1201/9781439833032.ch188.

Smith, K.T., Jones, A., Johnson, L. and Smith, L.M. (2019), "Examination of cybercrime and its effects on corporate stock value", *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 1, pp. 42-60.

Sukumar, A. and Edgar, D. (2009), "E-Business, SMEs and risks: towards a research agenda", *International Journal of Management Innovation Systems*, Vol. 1 No. 2, doi: 10.5296/ijmis.v1i2.113.

Symantec (2016), "Internet security threat report", doi: 10.1016/S1353-4858(05)00194-7.

Valli, C., Martinus, I. and Johnstone, M. (2014), "Small to medium enterprise cyber security awareness: an initial survey of Western Australian business", *Proceedings of the International Conference on Security and Management (SAM)*, 2020(July), p. 1.

Yildirim, E.Y., Akalp, G., Aytac, S. and Bayram, N. (2011), "Factors influencing information security management in small- and medium-sized enterprises: a case study from Turkey", *International Journal of Information Management*, Vol. 31 No. 4, pp. 360-365, doi: 10.1016/j.ijinfomgt.2010.10.006.

Corresponding author
Ratna Yudhiyati can be contacted at: ratna.yudhiyati@uny.ac.id