How Micro and Small Enterprises Perceive Information Technology Fraud: A Study of Indonesian' Small Businesses

Diana Rahmawati
Doctoral Program in Economics
Universitas Negeri Sebelas Maret
Surakarta, Indonesia
rahmawati_diana@uny.ac.id

Ratna Yudhiyati
Department of Accounting
Universitas Negeri Yogyakarta
Yogyakarta, Indonesia
ratna.yudhiyati@uny.ac.id

Afrida Putritama
Department of Accounting
Universitas Negeri Yogyakarta
Yogyakarta, Indonesia
aputritama@uny.ac.id

***Abstract*—Micro, Small, and Medium Enterprise (MSME) managed to survive an economic downturn in many countries because of its resilience. It is much easier for MSME's owner to adjust its business and respond to the changes in markets. However, MSME also needs to admit they it has weaknesses in areas like marketing, technology, and finance. The adoption of information technology by MSMEs is generally still low because of the great hesitancy of MSME to adopt new technology. This hesitancy is understandable. Despite the usefulness of information technology, the adoption of information technology may put MSME at risk in becoming a potential victim of information technology fraud. This study explores how MSMEs perceive the risks of information technology fraud and how much their perception affected their decision in utilising information technology. The result of this study can be used to formulate necessary steps in addressing small business wariness toward information technology risks. This study hoped to provide information to develop necessary steps in introducing IT for MSMEs who still consider IT as a 'dangerous thing'.**

Keywords—small business, MSMEs, information technology, fraud risk

I. INTRODUCTION

Micro, Small, and Medium Enterprise (MSME) is one of the most important cornerstones of economy in many countries. MSME drived employment and one of the main contibutors of economic growth. Moreover, one of the discerning factors of MSME compared to its bigger counterpart is its resilience [12]. MSME is nimbler than bigger business. Important strategic decision can be decided by MSME swiftly because of its small size. This resilience was one of the main factors why MSME managed to survive economic downturn in many countries, including Indonesia.

The growth of industries requires MSME to adjust its strategies by meeting the global market needs and adopting new advances in science and technologies [12]. However, these steps can not be taken easily. Nimbleness and ability to respond customer's need in quality and innovation are some of MSME's main strengths, but MSME also have weaknesses in areas like marketing, technology, and finance [12]. MSME is usually hesitant to adopt new technology. The adoption of information technology by MSMEs is generally still low [1][7] Decision to adopt technology in MSME is also usually caused by external pressure instead of internal motivation [12].

This hesitancy can be harmful for MSME. Reference [4] explained that utilising information technology is necessary for MSME to keep competing in market, especially when technology is commonly used in the industry where it competes. Utilising technology is not about obtaining advantage anymore, but it is now about staying in competition. Global market changes rapidly and information technology is one of the most feasible ways to keep up with the changes. MSMEs which refuse to use information technology where it is commonly used in the industry will not be able to compete with their competitors.

However, the adoption of information technology may create new issues for MSME. When a business entity adopts information technology, it encounters new risks caused by security concern of the new technology used by the entity. MSME has great risk to become victim of information technology crime. MSME only has limited resources which can be dedicated for information technology security, so it is often considered as easy target by hackers and fraudsters [9].

MSME which ignore technology security risk may face several risks. The first risk is a direct financial loss, whether it is caused by theft of business' assets by fraudster or a fine from the government due to the busineness' negligence. The second risk is indirect loss, such as damage to business' reputation, disturbance in operation, theft of business' confidential information, and a blackmail where fraudster takes over access and control of enterprise information technology and asks for compensation [9]. These risks make many MSMEs become cautious in adopting information technology. Several studies found that security concern is indeed one of the main barriers for MSME in adopting information technology [7][12]13]. This continued hesitancy will make them left behind by their bigger counterparts in business competition.

MSME is a very important topic in Indonesia because of its role in sustaining economy during depression and economic downturn. Research about how to improve MSME' competitiveness in growing market is greatly sought. Most of the studies on information technology adoption by MSME in Indonesia analyzed about how far the information technology utilization by MSME or what their perception towards the utilization of information technology in general was [1][10]. They rarely address specific issue and provide further insight about each specific issue faced by MSME in information technology adoption. This study would focus on one of the

barriers faced by MSME in adopting information technology; security concern. This study would identify and analyse about how MSMEs perceive information technology risk and its influence toward business operation. We would like to know whether MSMEs think that IT fraud risk is dangerous for its business or not. We also wanted to find out whether IT security concern will make them stop using IT or not. If their answer is positive, this study would aim to find out about what can change their mind. If their answer is negative, we would like to know about what they want to do to reduce IT fraud risk in their business. By obtaining answers of these questions, this study hoped to formulate necessary steps in introducing IT for MSMEs who still consider IT as a 'dangerous thing'. This study can be used to help developing policies and fraud prevention method for MSME.

This study decided to concentrate on micro and small industries (hereafter 'small business'). Several MSMEs which represent different industries were selected as respondents for this study. This decision was made based on previous study which indicated that businesses in different industries utilise information technology differently [3].

II. Theoretical Background

A. Information Technology Fraud

Fraud is a term used to refer to any kind of method used by a person to benefit from others by using a false representation [2]. When a person deliberately deceives others for gain, it can be categorized as fraud.

Fraud can be found in any industries and any type business. However, companies using information technology have unique risks caused by the application of information technology [2]. This risk is the potential for becoming a victim of information technology fraud.

Information technology fraud is an act where a fraudster utilised information tecnology to wrongfully benefit from victims. Companies which becomes victims of information technology fraud suffer several losses, which are; (1) direct financial loss, (2) impact on reputation, (3) impact on company performance, and (4) theft of important information. There are many schemes of information technology fraud. Some commonly known examples of them are social engineering, spamming, spyware, carding, and piggy backing [11].

B. Micro, Small and Medium Enterprise

Micro, Small, and Medium Enterprise (MSME) is difficult to be defined. One of the most commonly used definition of MSME in Indonesia is provided by Law no. 20/2008 about Micro, Small, and Medium Enterprise [8].

Reference [8] provided definition of each type of enterprise. Each type of enterprise is differentiated based on the amout of its assets or turnover per year. Business whose net assets, excluding land and building, is Rp50,000,000 at most or whose turnover is Rp300,000,000 per year at most, is classified as micro enterprise. Small enterprise is business whose net asset, excluding land and building, is between Rp50,000,000 and Rp500,000,000, or whose turnover is between Rp300,000.000 and Rp 2,500,000,000 per year. Medium a business whose net asset is between Rp500,000,000 and Rp10,000,000.000 or whose turnover is between Rp2,500,000,000 and Rp50,000,000,000 per year. The enterprises should also not be a subsidiary of bigger enterprise to be qualified as MSME.

C. Previous Studies about The Use of Information Technology by MSMEs

A comprehensive study about MSME's resilience put a great importance on use of technology. The study found that most organisations who became respondents in the study admit that information technology is important in their organisation [12]. Most of them believed that information technology improves the efficiency of their operation and also their relationship with customers and suppliers. However, most MSMEs only used information technology for a single function, such as procuring or marketing, but not for an integrated supply chain activity [12]. The study also found that very few MSMEs knew and used technologies like ERP and EDI. This information showed that most MSMEs had not viewed their operations from a supply chain perspective, which could be considered as a great weakness and a waste of opportunity.

The same study also identified several barriers faced by MSMEs when they wanted to use information technology. The lack of skills in using information technology, security concerns, insufficient financial supports, and the lack of top management supports were some main barriers for MSMEs in adopting information technology [12]. Another study found similar findings related to barriers of information technology adoption by MSMEs. Reference [7] found that the lack of established regulatory system, costly initial investment, and security issues were the top three most important reasons why MSMEs hesitated to adopt information technology in Ghana. High cost of initial IT investment may be one of the reasons why some MSME top managements hesitate to support information technology adoption, as mentioned by Reference [12].

Another study about information technology adoption in Indonesia provided additional evidence that security concern, the lack of skills and high cost of infrastructure are some considerations which make MSME hesitated to use information technology. Reference [13] explained that their informants do not want to invest in IT infrastructure because it is too costly for companies at their size. The study also noted that the informants were worried of possibility of obtaining false information (namely 'hoax') which may harm their decision making. They were also worried of possibility that competitors will obtain information about their products and service through information technology, which can be classified as information leakage [13].

Based on these studies, several main factors which prevent MSMEs from adopting IT were; (1) regulation, (2) cost, and (3) security concern [7][13]. Regulation issue can be addressed by introducing new regulations which are IT-friendly for MSME. Government can also address cost issue by improving infrastructure (e.g. better and cheaper internet connection) or changing regulation (e.g. reducing import duty for IT purchase by MSME) [10]. However, few studies had addressed security concern issue.

Security issue is regarded as the greatest threat of IT usage by MSME [6]. Security issue is also a matter of perception, so it is greatly influenced by human's point of view [6]. Governments can do their best to improve security of IT, but MSMEs may not care because they still perceive IT as a 'risky thing'. Thus, this issue needs to be addressed by directly

asking MSMEs' owner about what they really need to solve their wariness of IT. This idea was also supported by previous study which found that owners and their perception are some of the most significant factor which determine IT adoption by MSME [15].

III. Research Method

A. Research Design

This study was a qualitative research which utilize thematic method. Several respondents who experienced same phenomenon were interviewed intensively and their experiences were described and analysed by summarising several important themes and conclusions. The phenomenon which became the focus of this research is small businesses' experience is using information technology.

All respondents were small businesses who had utilised any kind of information technology. However, this study emphasized on information technology fraud, so this research would focus on explaining how small businesses perceive information technology fraud, as those who had used the information technology.

B. Data Collection

Respondents of this study were selected from small businesses whose owner resided in DI Yogyakarta, Indonesia. This decision was made to enable us to interview the respondents directly, instead of conducting interview remotely. However, we believed that these respondents could represent Indonesia's small business because; (1) they sold their goods or services nationally and their customers came from all provinces in Indonesia, and (2) all MSMEs in Indonesia are properly classified nationally by Law no. 20/2008 explained in previous section, so busineses are quite similar within same category.

Respondents were selected by following several steps. First, we obtained a list of MSMEs which can be possible respondents. We combined the list of MSMEs registered in Department of Industry and Trade, DI Yogyakarta, and some unregistered MSMEs. Unregistered MSME's data was obtained from participant list of several seminar and training for MSMEs held by our institution. Second, we identified MSMEs in the list which can be classified as micro and small enterprise based on their turnover and asset. Third, we identified the small business in our list which utilised information technology in their business operation. We identified them based on public information we have about them, and we also asked some small businesses personally. Fourth, our respondents need to represent at least two types of business; trading, manufacturing, or service. Fifth, based on the updated list of possible respondents, we contacted them to ask their willingness to be our respondents. We managed to obtain five respondents for our study.

This study utilised direct interview to collect data and information from respondents. The interview was conducted for 15-30 minutes and the questions aksed during interview were based on pre-arranged interview guide. We would interview each respondent several times if we need more information. The two main questions asked in interviews were

TABLE I. Content Analysis for Respondent AH (partial)

Meaning units (*Condensation*)	**Codes**	**Categories**	**Theme**
My opinion about payment channel. Hmm, I trust the security measures provided by the online trading website and platforms (*I trust website and platform provider*)	Trust	Opinion about existing security measure	Opinion about using IT despite fraud risk
Especially those reputable companies. Those companies surely have ways and measures to prevent unwanted circumstances (*Reputable companies have ways to prevent security issues*)	Trust	Opinion about existing security measure	Opinion about using IT despite fraud risk
If there is any security issue, those companies will be questioned, and they will be in problem (*Companies will be in a problem if security issue is found*)	Trust	Opinion about existing security measure	Opinion about using IT despite fraud risk
I believed that security loopholes always exist. (*Security loopholes always exist*)	Understanding	Understanding about security issues	Understanding about IT fraud risk
In my understanding, if we designed a fully-secured system, data will not be able to go in or out. My friend told me that a fully-secured system will only be a security vault without additional value, since we can not utilise the data. (*data will have no use in a fully-secured system*)	Understanding	Understanding about security issues	Understanding about IT fraud risk
This is one of the main reasons why system designers will try their best to find a balance between system's security and benefit. This is also the reason why all systems have weaknesses and loopholes, simply because it was designed that way. If we make doors for going in and out, there will always be small holes. (*Systems always have security loopholes because it was designed that way*)	Understanding	Understanding about security issues	Understanding about IT fraud risk
We trust them, but we also need to be wary and take necessary precaution regarding online platform, such as securing password and change it regularly. (*Trust them, but still need to be wary and take precaution*)	Security precautions	Opinion about existing security measure	Opinion about using IT despite fraud risk

'what have you experienced when you use information technology in your business?' and 'what is your opinion about fraud risk which may arise when you use information technology for business?'. The second question can be separated into three different questions; (1) what is your opinion about IT fraud risk? (2) will you stop using IT because of its fraud risk? (3) what will you do about IT fraud risk in your business? The results of the interviews were documented in audio recordings and interview transcripts.

C. Data Analysis

This research utilises content analysis to analyse the data obtained from interviews. By performing the qualitative content analysis, we aimed to transform the large amount of text and data into a concise and organised summary which provide several key results [14].

First, we read and re-read the interview transcript to get a general understanding about what the respondent was talking about. We divided up the text into smaller parts whille retaining the core meaning of the text. These smaller parts are named condensed meaning unit [14]. The parts which needs to be condensed were selected by chosing statements which can answer the research questions we described in previous section.

The next step is labelling these meaning units by formulating codes. These codes were grouped into categories and these categories were classified further into themes [14]. The themes served as a foundation for describing and analysing what respondents experience and how they view the experience [5].

We started the analysis by performing it first to one of our respondents, AH. Two persons read and re-read the interview. They condensed the large text into smaller condensed meaning units, coding them, and grouping them into categories and themes *individually*. These two persons discussed their result and when they found different result, they dicussed it and make a conclusion together. The analysis of respondent AH's interview was described partially in Table 1 as an example of our content analysis process. AH was selected as the first respondent we analysed because we thought that AH provided us with the longest and most comprehensive answers to our questions. Our analysis of AH's interview produced two categories and two themes.

The codes found in AH interview was utilised as a starting point to code materials in other four interviews. However, our analysis of other interviews provided several new information and produce two additional categories. Thus, our study classified all interview materials into four categories, which can be grouped into two themes. We wrote structured descriptions about the answers of our research questions, and their analysis, based on these categories and themes.

IV. Result and Discussion

A. Respondents' Profile

Table 2 provided background and introductory information about respondents of this study. This information would be useful for analysing the result of our study.

Some respondents admitted that they had started using information technology since they started their operation. Based on our interview, all respondents had basic knowledge and experience in using information technology before they started their business, so they did not hesitate to use information technology when they started business of their own. However, two respondents admit that he did not use information technology when they started his business, despite their experience in using information technology. They adopted information technology recently, thanks to the the growing popularity of internet, e-commerce, electronic payment, and other appliance of information technology in business. This information expressed that owner's background indeed greatly influence decisions made by small business and it is also much easier for owner to implement changes in small business, as long as they are willing [12].

All respondents used information technology for marketing and receiving payment from customer, despite the industry where they operated. The most commonly used information technology is the internet-based ones, such as

TABLE II. Respondents' Profile

Respondents' Initial	Industry	How long they have used IT	How they utilise IT in business
AH	Service (lodging and hospitality)	7 years (Since the business started its operation)	• Using website for marketing, booking, and customer service. • Accepting electronic payment
MC	Manufacture (Food & Bakery)	3 years (Since the business started its operation)	• Using website and social media for marketing and receiving order. • Accepting electronic payment
BAJ	Retail	6 years (Since the business started its operation)	• Using simple database sharing system to share data with franchiser. • Accepting electronic payment • Using website for marketing
KK	Manufacture (sugar and palm sugar)	2-3 years (Since the product became well known and established)	• Accepting electronic payment • Using website for marketing • Using e-mail for communicating operation report • Using GPS and online map system for tracking shipment of products to customer.
BB	Retail (food and restaurant)	1 year (Adopt information technology recently)	• Accepting electronic payment • Using website for marketing

social media, website, and internet-based payment channel (PayPal, internet banking, mobile banking). We noticed that there were two respondents which utilise more complicated information technology, such as database and GPS tracking. This information is surprising since previous study noted that most small business only use simple information technology and rarely use interconnected information technology such as database or Business-to-Business (B2B) [12].

B. Result and Discussion

1) Small businesses' understanding about fraud risk of information technology.

Our respondents explain that their decision to use information technology was greatly influenced by a cost-benefit analysis. They compared potential benefits they can obtain and risks they may face. Regarding fraud risk of information technology, they know and understand the risks, yet they are willing to bear the risk because in their opinion, the benefit of using information technology fat outweigh the risks.

All respondents shared similar view. They were not ignorant about the possibility of becoming fraud victim due to their decision of using information technology. However, these potential problems did not stop them from utilising information technology in their businesses. This opinion was expressed in following statement from one of the respondents, AH;.

"In my understanding, if we designed a fully-secured system, data will not be able to go in or out. My friend told me that a fully-secured system will only be a security vault without additional value, since we can not utilise the data. This is one of the main reasons why system designers will try their best to find a balance between system's security and benefit. This is also the reason why all systems have weaknesses and loopholes, simply because it was designed that way. If we make doors for going in and out, there will always be small holes"

Another similar statement was provided by another respondent, MC.

"I told my friend that if we use online platform, we should not expect our data to be fully secure. We need to be ready for it to be public. That risk is the price for obtaining the advantage of online platform."

Our respondents' profile showed that they had prior knowledge of information technlogy before they start implementing it in their businesses. We concluded that initial information technology knowledge significantly influences small business decision in using information technology and how they perceive the fraud risk associated with it. This finding was supported by previous study which found that MSMEs' managers or owners who have IT-professional background or IT experience regarded IT fraud risk as a high-priority threat, compared to MSMEs' managers or owners who had no such experience [6].

2) Small Businesses' Opinion about Using Information Technology despite Security Risk.

We analysed this theme by keep the existing three categories separate because each category provided unique information. This section described each category in detail, so they were expected to provide a clear explanation about what small businesses thought about using information technology despite existing security risk.

a) Opinion about Existing Security Measure

Our study found that most of the respondents used information technology provided by third-party vendor. Respondents expressed their trust to existing security system provided by those parties. They believed that information technology provided by reputable companies had good quality and it also had adequate security measure. This attitude was explained by AH in following statements.

"I trust the security measures provided by the online trading website and platforms, especially those reputable companies. Those companies surely have ways and measures to prevent unwanted circumstances. We trust them, but we also need to be wary and take necessary precaution regarding online platform, such as securing password and change it regularly."

Most respondents expressed that they have confidence on security measures provided by vendors whom they partnered with. Our respondents also thought that the ones who held main responsibility over their IT security were the vendors who provide the technology. However, we also noticed that respondents also did not blindly trust the vendor. They understood that they also had responsibility toward their own system's security. They understood the importance of personal security measures, such as user name, password, and antivirus software.

b) Willingness to Invest

Nevertheless, small businesses' trust toward third party vendor affected their willingness to invest in security measures. As mentioned before, respondents had basic knowledge about information technology. They also understood that security cost is always cheaper than financial loss which may arise if they become a victim of information technology fraud. However, they were willing to pay the security if they felt that they need it. Most respondents believed that they did not need the additional security cost because they felt content with the current technology and they also believed that the security measures provided by vendors were adequate. They did not consider long-term benefit which could not be identified easily in their cost-benefit calculation.

This view was expressed by MC in following statement;

"I will definitely do it (improving security measures) in the future when my business had grown. I have plans to use more IT when I finally have my own shop. For now, I think everything is working well because I only use simple online banking and it is quite safe."

This finding was similar with another study which found a situation where small businesses had high dependency on third-party vendor which provide the information technology used by the small businesses [6]. Reference [6] concluded that MSME's age was the main factor which caused the dependency. However, our study did not find similar conclusion since all respondents greatly depended on third party vendors despite their difference in age. It was assumed

that business' size may have bigger influence toward high dependecy on third party provider than business' age.

c) Opinion about Routine Maintenance.

Routine maintenance is one the preventive security measures which can be used to reduce information technology fraud. Cost of preventive measures is usually much cheaper than financial loss which occur when an entity become a fraud victim [2]. However, this study found that most respondents thought that routine maintenance for security measures is not necessary.

One of the respondents, KK, expressed his opinion in following statement; "We do not perform routine maintence, so we will only perform maintenance if we encounter a problem or there is a server failure". A similar statement was provided by BB which stated; "We do not think that maintenance is necessary, since our information technology is provided by third party."

Our respondents argued that reactive maintenance, which is a maintenance performed when a problem occurs, is better than routine maintenance from a cost-benefit view. Routine maintenance is considered costly while not providing immediate benefit. Some respondents also thought that routine maintenance is not their responsibility since they used third-party online platform or software. This view was also greatly affected by their trust towards vendors and their reluctance to pay additional cost for security measure whom they assessed as adequate, which had been discussed in prior section.

V. Conclusion

This study found that small businesses which utilise information technology are usually owned by individuals who have initial knowledge and prior experience in using information technology, before they decided to implement the information technology in their businesses. They made an informed decision in adopting information technology. They had adequate knowledge about fraud risks which may arise, yet they were willing to bear the risks. They consider that the benefit of using information technology greatly outweigh the risks.

Several conclusions about how small business perceives information technology fraud were summarised from this study. This study found that most small businesses used information technology provided by third party vendor. They thought that the vendors were the one who is most responsible to provide adequate security measure for their technology. However, those businesses were not ignorant about the importance of personal security measures which need to be implemented properly, such as personal password and accounts. The trust toward third party vendor also greatly affected their reluctance to pay additional investment in security measures because they assessed that the existing security measures were adequate.

This study expanded previous literatures and research of MSMEs by analysing and describing MSMEs' opinion and how they perceive information technology fraud risk. While most previous studies discussed about barriers of IT adop tion by MSME in general, this study focused and analysed in depth one of those barriers; security concern. These findings would be beneficial to answer small business' concern toward information technology security and encourage them to adopt information technology further. Our finding about the great role of third-party vendor also can be useful for those vendors and other interested parties to design the most information technology and its additional service for MSME.

Nevertheless, this study had several limitations. First, this study did not aim to generalise its finding to all small businesses because its main aim is obtaining new insights. Thus, it is important to find further evidence to support this study's conclusions which can be generalised to all small businesses. Second, this study also did not separate our analysis based on the respondents' industries and ages. Based on our findings and previous studies, we noticed there was possibility that additional insights could be concluded if they were comparatively analysed.

Acknowledgment

This research was funded by Universitas Negeri Yogyakarta, Yogyakarta, Indonesia.

References

[1] I.A.F Ahmad and I. Sentosa, "An empirical study of e-commerce implementation among SME in Indonesia", International Journal of Independent Research and Studies, vol. 1, pp. 13-22, 2012.

[2] W. Albrecht, C. Albrecht, C. Albrecht, and M. Zimbelman, Fraud Examination. Boston: Cengage Learning, 2011.

[3] E. Brynjolfsson and L. Hitt, "Information technology as a factor of production: The role of differences among firms", Economics of Innovation and New technology, vol. 3(3-4), pp. 183-200, 1995.

[4] A. Cataldo and R. McQueen, "Strategic driver or unimportant commodity?", Industrial Engineering, vol. 46, pp. 36–41, 2014.

[5] J. W. Creswell, Qualitative Inquiry & Research Design: Choosing Among Five Approaches. Sage Publication, 2007.

[6] K. Grant, D. Edgar, A. Sukumar, and M. Meyer, "Risky business': perceptions of e-business risk by UK small and medium sized enterprise (SMEs)", International Journal of Information Management, vol. 34, pp. 99-122, 2014.

[7] F. Iddris, "Adoption e-commerce solutions in small and medium-sized enterprises in Ghana", European Journal of Business and Management, vol. 4, pp. 48-57, 2012.

[8] Law No. 20/2008 (Indonesia).

[9] S.M. Rahman and R. Lackey, "E-commerce system security for small business", International Journal of Network Security & Its Application, vol. 2, 2013.

[10] M.R. Roosdhani, P.A. Wibowo, and A. Widiastuti, "Analisis tingkat penggunaan teknologi informasi dan komunikasi pada usaha kecil menengah di Kab. Jepara (An Analysis of information technology utilisation level in small and medium enterprises at Jepara)". Jurnal Dinamika Ekonomi dan Bisnis, 2012.

[11] M.B. Romney and P.J. Steinbart, Sistem Informasi Akuntansi (Accounting Informasion System). Jakarta Selatan: Penerbit Salemba Empat, 2015.

[12] A. Gunasekaran A, B.K. Rai and, M. Griffin, "Resilience and competitiveness of small and medium size enterprises: an empirical research", International journal of production research, vol. 49(18), pp. 5489-5509, 2011.

[13] M.A. Nugroho, A. Z. Susilo, M. A. Fajar, and D. Rahmawati, "Exploratory Study of SMEs Technology Adoption Readiness Factors", Procedia Computer Science, vol. 124, pp. 329-336, 2017.

[14] C. Erlingsson and P. Brysiewicz, "A hands-on guide to doing content analysis", African Journal of Emergency Medicine, vol. 7, pp. 93-99, 2017.

[15] R. Rahayu and J. Day, "Determinant Factors of E-Commerce Adoption by SMEs in Developing Country: Evidence from Indoensia", Procedia – Social and Behavioral Science, vol. 195, pp. 142-150, 2015.