Eduvest – Journal of Universal Studies
Volume 5 Number 02, February, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

ANALYSIS OF THE MATURITY LEVEL OF CYBER SECURITY IN THE CONTEXT OF PERSONAL DATA PROTECTION FOR MSMES IN DEPOK CITY

Catur Agus Sulistyo[1], Gerry Firmansyah[2], Budi Tjahjono[3], Agung Mulyo Widodo[4]
Universitas Esa Unggul, Indonesia [1,2,3,4]
Email: kabul.abbasy@student.esaunggul.ac.id

ABSTRACT

This research explores the cybersecurity maturity level in the context of personal data protection for Micro, Small, and Medium Enterprises (MSMEs) in Depok City, Indonesia. The increased use of digital technology by MSMEs has raised concerns about personal data security and the vulnerability to cyberattacks. This study aims to develop an assessment tool that MSMEs can use to evaluate their compliance with the Personal Data Protection (PDP) Law and measure their readiness to face cybersecurity challenges. Through a combination of qualitative and quantitative methods, the study analyzes MSMEs' preparedness for cybersecurity and compliance with the PDP Law. The results reveal that while 60.2% of MSMEs manage personal data, a significant 93.5% have not complied with the PDP Law, exposing them to potential financial losses and cyber risks. The research emphasizes the need for MSMEs to adopt a simple yet effective cybersecurity framework to ensure data protection and compliance.

KEYWORDS *Cybersecurity, Personal Data Protection, MSMEs, Compliance*

INTRODUCTION

Data leaks generally involve personal data, and in accordance with the mandate of Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection (UU PDP), personal data must be protected. Protection of personal data is one of the human rights, so it is necessary to provide a legal basis to obtain security for personal data, based on the 1945 Constitution of the Republic of Indonesia (UU PDP, 2022).

Personal data according to Article 1 of the PDP Law is data about an individual who is identified or can be identified individually or in combination with other information either directly or indirectly through electronic or non-electronic systems.

How to cite: Catur Agus Sulistyo, et al. (2025). Analysis of The Maturity Level of Cyber Security in The Context of Personal Data Protection for MSMEs in Depok City. Journal Eduvest. *Vol 5*(2): 2155-2171
E-ISSN: 2775-3727

Every Person (individual or corporation), Public Agency and International Organization that manages or performs electronic processing of personal data, must perform personal data processing in accordance with the principles of Personal Data Protection including limited and specific, legally valid and transparent, and in accordance with its purpose. In addition to guaranteeing the rights of Personal Data Subjects and ensuring accuracy, completeness, non-misleading, up-to-date and accountable, Personal Data must be secured from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction and/or deletion of Personal Data.

As stated in "Chapter VIII Administrative Sanctions" and "Chapter XIV Criminal Provisions" of the PDP Law, negligence in the management or processing of Personal Data that results in failure of Personal Data Protection can be threatened with administrative sanctions in the form of a fine of up to 2% of annual revenue and criminal sanctions in the form of imprisonment, fines, and/or license revocation up to corporate dissolution. Then in "Chapter XV Transitional Provisions" Article 74, Personal Data Controller, Personal Data Processor, and other parties related to the processing of Personal Data, must adjust to the provisions of Personal Data processing based on the PDP Law no later than 2 (two) years from the enactment on October 17, 2022.(Pratama, 2024)

The Coordinating Minister for Economic Affairs, Airlangga Hartanto, said that the role of 65.5 million Micro, Small and Medium Enterprises (MSMEs) is very large in national economic recovery through a contribution of 61% to Indonesia's Gross Domestic Product (GDP) (Press Release of the Coordinating Ministry for Economic Affairs, 2023). Then based on data from the Indonesian E-Commerce Association (idEA), there are 19 million MSMEs that utilize digital technology (Digital MSMEs) or 29.5% of the total MSME population (Hidranto, 2022). This number will continue to be increased by the government until it is expected to reach 30 million Digital MSMEs in 2024 so that it can have implications for digital economic growth in Indonesia of Rp 4,531 trillion in 2030 (Kumparan.com, 2022).

The increased use of digital technology in MSMEs to support business activities provides benefits including reaching a larger number of consumers, making it easier to monitor business activities, increasing revenue and reducing marketing, logistics and shipping costs (Kominfo, 2022). The use of technology and adjusting to market demand will not make the business stagnant or even abandoned by customers (Gracia, 2022). In utilizing technology, Digital MSMEs certainly also manage personal data including employee data, customer data, provider data, transaction data and others so that they must comply with the provisions in the PDP Law in order to avoid administrative and criminal sanctions (Simbolon, 2022). Therefore, as one of the parties that are part of the implementation of electronic

systems, MSMEs have used electronic systems or ICT to help run their business operations, so that the policies in the Personal Data Protection Law must be directly complied with. Referring to Article 35 of the Personal Data Protection Law, digital MSMEs as parties controlling personal data are obliged to maintain the security of personal data from the owners of the stored personal data including the confidentiality of personal data from their local and international partners (Pratama, 2024).

Based on traffic anomalies during 2023, the trend data for cyber attacks in Indonesia is 403,990,813 anomalies. The highest cyber attack anomaly recorded is the Generic Trojan RAT type, which indicates backdoor communication activity to the malicious domain which is indicated as a command and control server belonging to the threat actor. Then there are also Advanced Persistent Threats (APT) activities totaling 4,001,905 activities and 1,011,209 ransomware activities. Of the total 1,762 incident indication notifications that have been sent by the National Cyber and Crypto Agency (BSSN) during 2023, the most notifications are Traffic Anomalies. Meanwhile, through the Cyber Threat Intelligent service, there were 347 suspected cyber incidents, of which the type of incident was suspected to be a data breach. Based on reports received from stakeholders in the cyber complaint service, 1,417 complaints were obtained with the largest complaint category being Cybercrime at 86% (BSSN, 2023). The increasing application of digitalization by MSMEs has a risk impact in the form of cyber attacks by malicious actors, because MSMEs are easy targets considering that they do not have good planning and readiness related to cyber security (Bountouni, et al, 2023). The risk impacts of cyber attacks include reputational, legal, operational and financial impacts (Sarri A, et al, 2021).

Digital MSMEs as part of the Electronic System Operator (PSE) must comply with the PDP Law policy which requires them to ensure the security of personal data, so that if they cannot ensure the security of the processed personal data, there will be administrative and criminal sanctions, while the derivative rules of the PDP Law that regulate technical matters clearly and in detail have not yet been issued (Simbolon, 2022).

Based on the background description above, this research aims to design assessment tools for PDP implementation and Information Security in MSMEs that are simple but meet compliance and security criteria. Simple means that it is easy to understand and can be done by MSME actors themselves through the self-assessment method.

MSMEs as a 61% contributor to GDP with a total of 65.5 million business units, with 19 million of them being digital MSMEs, are vulnerable to sanctions for the implementation of the PDP Law, because MSMEs are likely to manage personal

data in the form of customer data. MSMEs are also at risk from cyber attacks because they do not have good planning and readiness from cyber threats.

This research aims to develop and implement an assessment tool for the implementation of Personal Data Protection (PDP) and Information Security for MSMEs in Depok City. The problems formulated include the form and application of the assessment tool as well as the readiness of MSMEs towards the implementation of the PDP Law and cyber threats. This research is expected to provide theoretical benefits by adding academic knowledge about cybersecurity maturity and MSME readiness towards the PDP Law, as well as practical benefits for MSMEs to measure their level of readiness. This research is limited to the development and simulation of assessment tools for MSMEs in Depok City.

RESEARCH METHOD

This research utilizes a methodology that involves theoretical review and design validation through experiments on a sample. The theoretical review included analyzing the literature related to information security in SMEs and its impact on personal data security. The research stages included designing an information security assessment framework based on the results of the theoretical review and experiments involving the creation of compliance and security audit controls through a study of literature as well as data collection from SMEs in Depok City to measure the maturity level of their readiness for the implementation of the PDP Law.

The object of this research is MSMEs in Depok City, which number 11,429 companies with a total workforce of 27,158 people. MSMEs in this city contribute 3.3 trillion rupiah in revenue. The focus of this research is to develop an assessment tool that can be used by MSMEs to ensure their readiness to face personal data security challenges and cyber threats.

This research adopted two main methods: qualitative and quantitative. Qualitative methods are used to describe phenomena through observation and document analysis from various sources such as books, journals, and articles. Meanwhile, the quantitative method focuses on collecting and analyzing numerical data to understand the relationship between variables and measure the readiness of MSMEs towards the implementation of the PDP Law through statistical analysis.

RESULT AND DISCUSSION

Creation of Compliance and Security Audit Controls

Increasingly complex cyber incidents due to the proliferation of crime in the digital age have become a serious threat to individuals and organizations, both public and private. Many companies choose not to disclose data leaks for fear of breaking the law and damaging reputations. To address these risks, the

implementation of a cybersecurity maturity model is important, helping companies measure their capabilities and improve security through evaluating the implementation of existing frameworks. Security standards such as CIS, ISO, NIST and others are used to assess and manage cybersecurity.

Security gaps often arise due to a company's unpreparedness in the face of cyberattacks, which can be exploited by attackers to harm the company. Therefore, implementing security mechanisms that comply with proven standards and frameworks is key to protecting corporate assets, especially data. A cybersecurity maturity assessment, including compliance with personal data protection regulations, enables companies to improve efficiency and performance by minimizing security gaps.

In the context of MSMEs, a cybersecurity maturity assessment aims to understand the actual condition of the security policies implemented, especially regarding the management of information and communication technology (ICT) and the protection of personal data. Therefore, a specific framework is needed that MSMEs can use to assess their level of compliance and strengthen their cybersecurity in accordance with applicable regulations.

Comparison of Security Framework with Literature Review

As an initial step to find out an overview of data sources in the form of standards / frameworks and also regulations related to cybersecurity and protection of personal data that will be used as a basis for mapping cybersecurity framework activities, then in Table 4.1 a comparison is made using the *literature review* technique by looking for similarities (*compare*), dissimilarities (*contrast*), views (*criticize*), compare (*synthesize*), and *summarize (summarize*). The frameworks to be compared are *CIS Controls v8 IG1 for Small and Medium Sized Enterprises* (CIS SME) and *NISTIR 7621 Revision 1 Small Business Information Security* (NISTIR SBIS).

Table 1. Comparison of Framework Standards with *Literature Review*

Methods Comparison	**Standard/Framework**	
	CIS SME	**NISTIR SBIS**
Compare	a. This guide is a security management framework for improving ICT security in small and medium-sized enterprises. b. This guide is a guideline that can be referred to by every small and medium-sized company with the technical requirements of each standard/framework as part of the data/information security compliance program.	
Contrast	1. This recommended course of action for cybersecurity provides specific and actionable	1. A framework-based approach to risk management that consists of three core parts: the framework, the levels of application of the

	ways to stop the most common attacks on systems and networks. *CIS Control v8* for small and medium-sized enterprises provides a solution that meets global standards and is one of the best practices for securing information technology systems and data from cyberattacks. 2. Consists of eighteen (18) controls which are divided into 153 *safeguards* (subcontrols) which are separated into 6 phases for basic *safeguards* which later need to be upgraded.	framework, and the framework profile. Each component has strong links to common cybersecurity activities in the critical infrastructure sector. Developed as a reference guide on cybersecurity for small businesses by presenting the basics of small business information security programs in non-technical language. 2. The framework has stages consisting of 5 (five) functions, categories, and subcategories with reference information of other related safety standards. Each subcategory can control the compliance defined in each organization.
Criticize	1. Prioritize and focus on a number of simple activities, in contrast to other control frameworks. 2. It has been vetted by a broad community of government and industry practitioners. The implementation of these controls is critical for organizations, both large and small.	1. The resource management that guides the preparation of the SMKI, which consists of four core areas and each subcategory of reference information, can be used as a control / recommendation to improve the steps of the mapping activities / programs. 2. The maturity level assessment illustrates the extent to which an organization implements cybersecurity risk management practices that are integrated throughout the organization.
Synthesize	This international standard framework is used as a measure of organizational information security management, with stages and flows tailored to achieve a predetermined level of maturity.	
Summarize	This structured information security standard/framework consists of a set of controls that meet global standards. It is one of the best practices for securing information technology	A structured cybersecurity standard/framework consists of five main functions: identification, protection, detection, response, and recovery. Each section has reference information that can be used as a control function to improve the organization's management of the

	systems and data from cyberattacks.	People, Process, and Technology components.

Based on the results of the comparison of security standards/frameworks in table 1 above, it can be concluded that in the selection of the basic framework, CIS SME is more appropriate and in accordance with the needs of the cybersecurity maturity framework for MSMEs. CIS SME prioritizes and focuses on a number of simple activities, compared to other control frameworks.

Content Analysis

The next analytical approach used in this research is content analysis. This method was used to identify the characteristics of the conceptual standards/framework and to present the data from the research analysis. Content analysis is a research methodology for understanding the content of messages, which are often unstructured, including text, images, symbols, and audio data (Gheyle, et al, 2017). In this context, content analysis is also a technique for making replicable and valid inferences by considering the context. It can reveal hidden meanings in texts, allowing in-depth exploration of documented information. There are six stages in content analysis research. While the first four stages can be used in any order, in this study, all six stages were used sequentially, depending on the situation and conditions that developed during the research (Krippendorff, 2004).

Content analysis is a method used in this research to identify the characteristics of a conceptual standard or framework, as well as present data from the analysis. This method helps to understand the content of often unstructured messages, including text, images, and audio data, and can reveal hidden meanings in texts. In this research, there are six stages of content analysis that are carried out sequentially, adjusted to the situation and conditions of the research.

The first stage, unitizing, involves identifying the messages or components that form the basis for defining the population and describing the sample. In this context, unitizing involves collecting data consisting of activities in cybersecurity standards/frameworks, such as the Cybersecurity Guidelines for small and medium-sized enterprises and the PDP Law.

The second stage, sampling, aims to simplify the research by limiting observations to a representative summary of the population. In this study, the entire population of selected cybersecurity standard/framework activities was used to provide a comprehensive understanding and in-depth analysis.

The third stage, coding, converts unstructured text into structured text categorized according to the referenced standard/framework. This process involves coding each activity in the standard/framework, which is then grouped according to

the process. For example, the CIS SME model refers to CIS Controls v8 IG1 for small and medium-sized companies.

The fourth stage, reducing, is the process of managing data so that it can be represented more efficiently, especially when dealing with large amounts of data. The MECE method is used to ensure that classification results do not overlap, and activities are grouped based on similar meaning or purpose.

The fifth stage, abductively inferring, summarizes the data from the cybersecurity guidelines and regulations studied into an integrated concept of the cybersecurity maturity framework, which is visualized in the activity distribution of the cybersecurity maturity model.

The final stage, naratting, develops text that translates the identified categories to answer the research questions. The resulting categories define cybersecurity maturity from various aspects, with nomenclature developed based on the existing categories, and where necessary, expanded by the chunk up method to avoid overly narrow definitions.

Compilation of Questionnaire

The preparation stage of the audit checklist is an audit stage carried out to create questions used in conducting compliance audits. The questions are compiled based on the cybersecurity framework from the content analysis at the previous stage, which is a total of 21 questions. These 21 questions are activities in the cybersecurity framework.

From the list of questions that have been made, there is an assessment of the selection of available answer options. The assessment of the answer options is designed by considering the assessment set by the Systems Security Engineering-Capability Maturity Model (SSE-CMM). In each question, there are 4 answer options with the highest weighted value of 4 for the answer "Yes", the middle value is 2 for the answer "Sometimes / partly", and the lowest value is 0 for the answers "No" and "Don't Know". The list of audit questions for respondents can be seen in Appendix 3.

Data Retrieval

Respondents are MSME players in Depok City and its surroundings. According to data from the West Java Central Bureau of Statistics, the number of small and micro industries in Depok City in 2022 was 11429 business units. With a sample size of 108 respondents, the *margin of error* is 9.6%. Data collection is done online using google form with a link at the address https://forms.gle/ayMmySZot4DJEhkS7. The MSME cybersecurity maturity level survey form is prepared based on the cybersecurity framework design that has been made.

The selection of respondents was conducted by the Depok City Cooperative and Microenterprise Office, which sent a survey link to the fostered groups in each sub-district. Each sub-district appointed 10 respondents from 11 sub-districts in Depok City. The sample selection used the Slovin formula with individual sampling units and sampling frames in the form of: MSMEs, located in Depok, using electronic/digital devices, connected to the network/internet, and managing personal data.

Then the question is made in simple language and the respondent simply chooses one of the answers, whose options are:

- Yes
- Partially/sometimes
- No
- Don't know

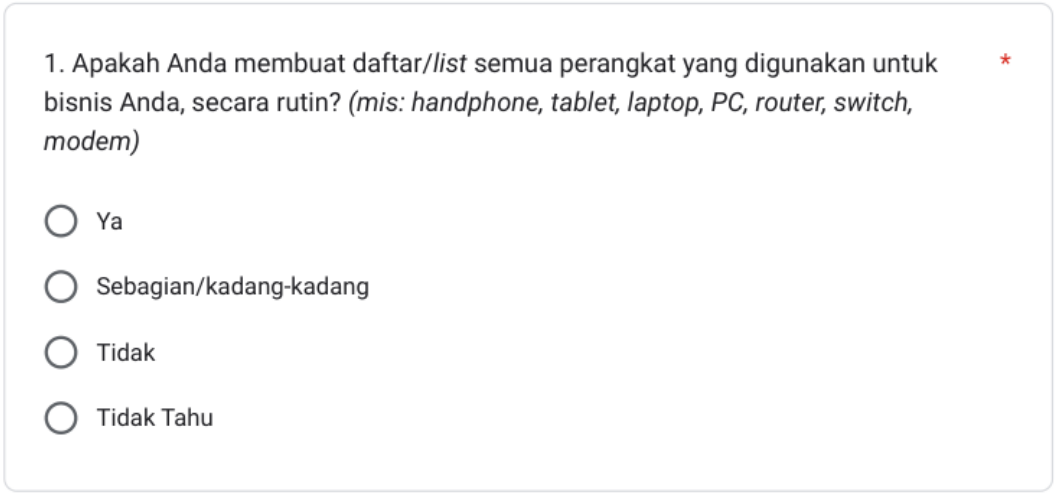
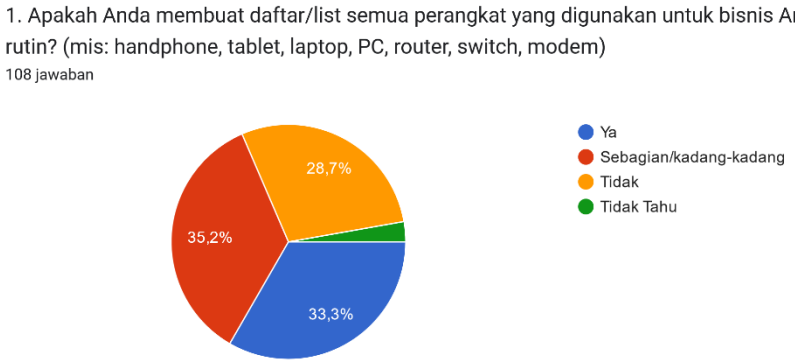
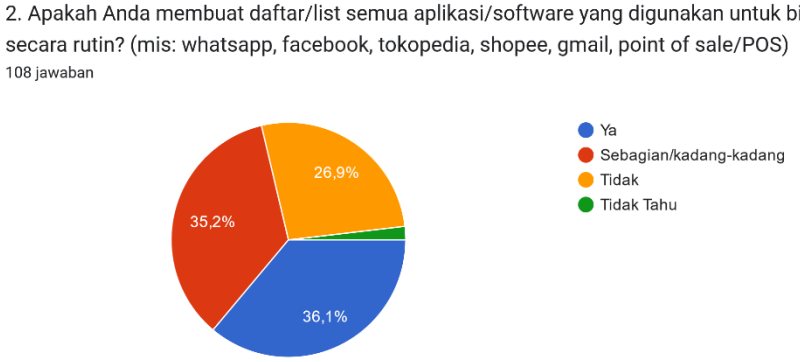
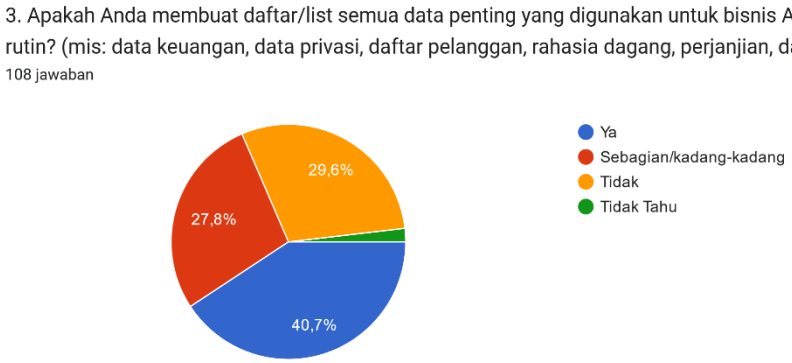


Figure 1. Survey questions

The percentage of answers from respondents for each question is as follows:







Maturity Level Measurement

The measurement of cybersecurity maturity level in the context of personal data protection involves respondents from micro, small and medium enterprises located in Depok City and its surroundings. The distribution of the survey link was carried out through the Depok City Cooperative and Micro Business Office, so that it is hoped that the results of the survey can describe the actual conditions, by being distributed to MSME communities that are assisted by the Depok City Government.

The measurement result is the average obtained by the respondent. The measurement value is obtained from the number of "Yes" and "Partly/Sometimes" answers multiplied by the multiplier factor.

Table 2. Survey Simulation Results

No.	Question	Yes	Sb	Td	TT
1	Do you make a list of all devices used for your business, on a regular basis? (e.g. mobile phones, tablets, laptops, PCs, routers, switches, modems)	36	38	31	3
2	Do you make a list of all applications/software used for your business, on a regular basis? (ex: whatsapp,	39	38	29	2

	facebook, tokopedia, shopee, gmail, point of sale/POS)				
3	Do you make a list of all important data used for your business, on a regular basis? (e.g. financial data, privacy data, customer lists, trade secrets, agreements, sensitive data)	44	30	32	2
4	Do you list all accounts (username & password) used for your business including access to devices and wifi and applications, on a regular basis? (including employee accounts)	47	25	34	2
5	Do you use antivirus on all devices used for your business?	37	35	32	4
6	Do you use a firewall to protect all devices used for your business?	15	30	46	17
7	Do you only download apps from trusted and authorized sources like Google Play or Apple App Store and not pirated ones?	99	2	0	7
8	Do you always update applications/software and firmware on devices used for your business when there is a new version?	58	34	10	6
9	Do you limit the use of thumb drives for file transfer across all devices used for your business?	48	22	28	10
10	Do you use strong passwords (a combination of uppercase, lowercase, numbers, and symbols) that are different for each of your business accounts and devices?	85	15	7	1
11	Do you use 2-step authentication (2FA) for all your business accounts and devices?	33	27	30	18
12	Do you regularly change passwords for all your business accounts and devices?	23	33	48	4
13	Do you back up your business critical data regularly and separately from the devices used for your business (PC, laptop, tablet or mobile phone)?	36	43	25	4
14	**Do you store customer or employee personal data, such as names, addresses or phone numbers?**	**65**	**26**	**17**	**0**
15	Have you asked and gotten permission from all your customers before storing their personal data?	54	33	18	3
16	Have you provided all customers with information on how their personal data will be used and stored?	46	25	34	3
17	Have you informed your customers of their rights regarding their personal data, such as the right to access and delete their data?	31	22	46	9
18	Does your MSME have a written privacy policy?	20	27	49	12

19	Have you ever experienced or known of a customer or employee personal data leak?	9	7	78	14
20	Have you created steps to take in the event of a security incident such as data theft or account breach?	21	17	47	23
21	Do you or your employees know or have you had training on cybersecurity? (e.g. how to recognize and avoid phishing)	13	7	72	16

Analysis of MSME Cybersecurity Maturity Level

The MSME cybersecurity maturity level based on the framework has 6 (six) phases, namely: inventory, device protection, account protection, data protection, incident response and security awareness. The analysis of each phase is explained as follows:

c. Inventory Phase

In the hardware inventory reflected in question number one on the survey, there are only 36 people or 33.3% who answered "Yes", this means that 66.7% of the devices used for business are still not recorded. Unrecorded devices allow devices that can be utilized by "attackers" to exploit existing systems. Meanwhile, application inventory is only carried out by 36.1% of MSMEs. Not yet recorded applications allow vulnerabilities because the application is not updated to the "*patch*" or the latest version. For data collection of important data in business, only 40.7% and accounts 43.5%. Knowing the list of important data will make it easier and efficient for company resources in an effort to secure important data. And unmanaged company accounts can be used by irresponsible parties to access resources in the company.

d. Device Protection Phase

In the phase of protecting devices against malware threats by installing antivirus/antimalware, there are only 34.3%, and only 13.9% have installed a firewall. The absence of antimalware and firewalls makes MSMEs very vulnerable to cyber attacks. Protection of applications has a fairly good value, namely from the use of applications downloaded from trusted sources as much as 91.7%. Although there are only 53.7% of MSMEs that always update their software and firmware. However, it should be noted that only 44.4% limit file transfers.

e. Account Protection Phase

The use of strong and different passwords for each account has been done by 78.7% of the respondents. However, only 30.6% have enabled 2-step authentication (2FA). Even only 21.3% routinely change passwords regularly. This certainly brings vulnerability to accounts that may have been leaked to irresponsible parties.

f. Data Protection Phase

In the data protection phase there are only 33.3% who make *backup* copies of data that are separate from the main device, this allows data vulnerabilities to be lost in the event of an incident.

g. Incident Response Phase

In the incident response phase there are only 19.4% who have created steps that need to be taken in the event of a security incident.

h. Security Awareness Phase

In the security awareness phase, only 12% have participated in or know about cyber security. This means that 88% of MSMEs are vulnerable to attacks that use *social engineering* techniques.

Analysis of Compliance with Personal Data Protection

There are 60.2% of respondents who manage personal data, and there are only 50% who have obtained permission from the personal data owner before storing their personal data. A total of 42.6% of data owners are informed of how their personal data is used and stored and only 28.7% know their rights to access and delete their personal data. Also, only 18.5% have a written personal data policy. Out of a total of 108 respondents, there are only 7 respondents or 6.5% who fulfill the compliance control of the PDP Law.

Analysis of Impact on MSMEs

i. Cyber Security Impact

Of the 108 respondents, there were only 8 MSMEs or 7.4% who achieved scores above 50 but still did not reach 60. The maturity level measurement tool in this study is a simplification of the cybersecurity framework which aims to make it easier for MSMEs to self-assess the controls or questions given. Achieving a perfect score on this tool is not the ultimate goal of cybersecurity activities, but is a prefix/bridge to start implementing cyber/information security in accordance with existing security standards, for example by implementing cybersecurity standards based on *CIS Controls Version 8 Implementation Group 1* which contains 56 security subcontrols or so-called *safeguards*. These 56 security subcontrols are activities that must be implemented by every company to defend against cyberattacks in general, and are the minimum standard of information security.

Based on the survey results, the following results were obtained:

- 7.4% of respondents scored 50-59
- 17.6% of respondents scored 40-49
- 34.3% of respondents scored 30-39
- 40.7% of respondents scored less than 30

The value obtained by MSMEs shows that there are still many cyber/information security controls that have not been implemented, so cyber incidents including data leaks are still very likely to occur.

j. Impact of PDP Law Compliance

There are 60.2% of respondents who manage personal data, but there are only 6.5% who fulfill the compliance control of the PDP Law, or there are 93.5% who have not complied. If it is assumed (based on BPS data in 2022) that there are 11,429 MSMEs in Depok City with annual revenue of IDR 3,337,444,325,000.00 with 60.2 percent managing personal data and 93.5 percent not complying with the PDP Law, it is estimated that there is a potential *loss/cost* for MSMEs in Depok City of:

IDR 3,337,444,325,000.00 x 60.2% x 93.5% x 2% = IDR 37,570,945,744.255

CONCLUSION

The study concluded that 60.2% of MSMEs in Depok City manage personal data, but 93.5% of them have not complied with the Personal Data Protection Law (PDP). As a result, potential losses for MSMEs in the city could reach IDR 37.57 billion. Furthermore, MSMEs in Depok are also vulnerable to cyberattacks, with only 7.4% of the 108 respondents achieving a score above 50 in the security audit, yet remaining below 60, indicating significant vulnerability.

To address these risks, MSMEs need to be equipped with knowledge of cybersecurity and implementation of an easy-to-implement security maturity framework, referring to international standards such as NISTIR SBIS and CIS SME. The cyber security audit for MSMEs has been designed with 15 questions covering aspects of data protection and compliance with the PDP Law. The distribution of activities in this cybersecurity framework shows that most activities come from a combination of the NCSC SME and CIS SME models.

The suggestion for MSMEs is to use the resulting framework to assess and improve cybersecurity and comply with the PDP Law. Stakeholders are expected to provide assistance to MSMEs in implementing information security standards. For future research, it is recommended to develop more cyber maturity frameworks that are easy to implement, so that MSMEs have more options to improve their security standards.

REFERENCES

Antunes et al, (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. J. Cybersecur. Priv. 2021, 1, 219–238.

Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2022," 2023.

Barker. E. Recommendation for Key Management – Part 1: General. NIST Spec. Publ. 800-57, no. May, pp. 1–142, 2016, [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.

Bountouni, N., Koussouris, S., Vasileiou, A., Kazazis, S. A. (2023, April). A Holistic Framework for Safeguarding of SMEs: A Case Study. Publish in: 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN).

Creswell, J. W., Creswell, J. D. (2017). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.

Fitzgerald (2017). Auditing Cyber Security: Evaluating Risk and Auditing Controls. Isaca, 2017.

Gheyle, N., Jacobs,T., "Content Analysis: a short overview," Intern. Res. note. Retrievedfrom https//www. Res. net/profile/Niels_Gheyle/publication/321977528_Content_Analysis_a_short_overview/links/5a3bee680f7e9b10e23bb2f9/C ontent-Analysis-a-short-overview. pdf, no. December, 2017, doi: 10.13140/RG.2.2.33689.31841.

Gracia, S. (2022). KemenKopUKM Perkuat Transformasi Digital UMKM. Stabilitas.Id. https://www.stabilitas.id/kemenkopukm-perkuat-transformasi-digital-umkm/

Hidranto, Firman (2022). UMKM Naik Kelas, UMKM Go Digital. https://indonesia.go.id/kategori/editorial/4618/umkm-naik-kelas-umkm-go-digital?lang=1

Hisbuloh, M. H. (2022). Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi. Jurnal Hukum UNISSULA.

ISO/IEC (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001

Jäntti, M. (2020). Studying Data Privacy Management in Small and Medium-Sized IT Companies.

Junior et al, (2023). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity

Kadeni, Srijani, N. (2020). Peran Umkm (Usaha Mikro Kecil Menengah) Dalam Meningkatkan Kesejahteraan Masyarakat. Quilibrium, Volume 8, Nomor 2, Juli 2020.

Kim, S., Nelson, J. G., Williams, R. S., Mixed-basis band-structure interpolation scheme applied to the fluorite-structure compounds NiSi2, AuAl2, AuGa2, and AuIn2, vol. 31, no. 6. 1985.

Kominfo (2022) .Transformasi Digital UMKM Jadi Prioritas Penguatan Fondasi Ekonomi. https://www.kominfo.go.id/content/detail/40915/transformasi-digital-umkm-jadi-prioritas-penguatan-fondasi-ekonomi/0/berita

Kosutic, D. (2012). 9 Steps to Cybersecurity The Manager's Information Security Strategy Manual. EPPS Services Ltd, 2012.

Krippendorff, K., "Reliability in content analysis: Some common misconceptions and recommendations," Hum. Commun. Res., vol. 30, no. 3, pp. 411–433, 2004, doi: 10.1093/hcr/30.3.411.

Kumparan.com (2022). Potensi Ekonomi Digital Indonesia Tembus Rp 4.531 Triliun di 2030. https://kumparan.com/kumparanbisnis/potensi-ekonomi-digital-indonesia-tembus-rp-4-531-triliun-di-2030-1yROcQEzYFo/full

Mirza, M. M. (2019). Audit Keamanan Sistem Informasi pada Dinas Komunikasi dan Informatika Kabupaten Bogor Menggunakan Standar ISO/IEC 27001:2013 dan COBIT 5.

Pratama, R. B. A. (2024). Perlindungan Hukum UMKM Internasional Untuk Kesejahteraan Masyarakat Berdasarkan Keadilan Sosial. Jurnal Ilmu Hukum, Vol.8 No.1, April 2024.

Pratiwi, F. (2020). Pengertian Audit : Manfaat, Jenis, dan Cara Melakukannya. https://www.harmony.co.id/blog/pengertian-audit-manfaat-jenis-dan-cara-melakukannya/

Republik Indonesia,"UU Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," 2022.

Sabillon, R. Serra-Ruiz, J., Cavaller, V., Cano, J. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). doi:10.1109/INCISCOS.2017.20

Sarno, R., Iffano, I. (2009) Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press, 2009.

Sarri, A., Paggio, V., & Bafoutsou, G. (2021). Cybersecurity for SMEs: Challenges and Recommendations.

Setiawati, I., Widyartati, P. Pengaruh Strategi Pemasaran Online Terhadap Peningkatan Laba Umkm. Strategi Komunikasi Pemasaran, 20, 2017, 1–5.

Shidiq, U. & Choiri, M., Metode Penelitian Kualitatif di Bidang Pendidikan, vol. 53, no. 9. 2019

Shojaifar et al, (2020). SMEs' Confidentiality Concerns for Security Information Sharing

SIARAN PERS No. HM.4.6/303/SET.M.EKON.3/08/2023 (2023). Dorong UMKM Naik Kelas dan Go Export, Pemerintah Siapkan Ekosistem Pembiayaan yang Terintegrasi. https://www.ekon.go.id/publikasi/detail/5318/dorong-umkm-naik-kelas-dan-go-export-pemerintah-siapkan-ekosistem-pembiayaan-yang-terintegrasif

SIARAN PERS No. HM.4.6/88/SET.M.EKON.3/04/2021. Dukungan Pemerintah Bagi UMKM Agar Pulih di Masa Pandemi. https://ekon.go.id/publikasi/detail/2939/dukungan-pemerintah-bagi-umkm-agar-pulih-di-masa-pandemi

Simbolon, V. A. (2022). Bagaimana Nasib Pelaku UMKM Digital Pasca UU PDP Disahkan? kumparan.com https://kumparan.com/user-27112022045905/bagaimana-nasib-pelaku-umkm-digital-pasca-uu-pdp-disahkan-1zL12M0m3dR/2

Solms, R. V., Niekerk, J. V. From information security to cyber security. Computer &Security., vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

Uprichard, E. (2013). Sampling: bridging probability and non-probability designs. International Journal of Asocial Research Methodology, 16 (1), pp. 1–11.

Whitman, M. E., Mattord, H. J. (2012). Principles of Information Security (Fourth Edition). Boston: Course Technology, 2012.

Wallang, et al, (2022). Cyber Security In Small And Medium Enterprises (SMEs): What's Good Or Bad?