Journal of Theoretical and Applied Information Technology
15th March 2021. Vol.99. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBER CRIME RISK CONTROL IN NON-BANKING ORGANIZATIONS

FORD LUMBAN GAOL[1], ANANDA DESSI BUDIANSA[2], AND YOHANES PAUL WENIKO[3] , TOKURO MATSUO[4]

[1]Computer Science Department, BINUS Graduate Program – Doctor of Computer Science, Bina Nusantara University, Jakarta11480, Indonesia
[2] Information System Management Departement BINUS Graduate Program - *Master of Information Systems*, Bina Nusantara University, Jakarta, 11480, Indonesia
[3] Information System Management Departement BINUS Graduate Program - *Master of Information Systems*, Bina Nusantara University, Jakarta, 11480, Indonesia
[4]Advanced Institute of Industrial Technology, Japan, City University of Macau, Macau, Asia University, Taiwan,
Email: fgaol@binus.edu; ananda.budiansa@binus.ac.id; yohanes.weniko@binus.ac.id, matsuo@tokuro.net

ABSTRACT

Cybercrime has become the main concern of an agency or business nowadays. It says that 71 percent of organizational threats occur because of the failure of the company to monitor the software, according to the Global Risk Management Report. Though 74% is disputed because there is no updating of the IT system. This research focuses on Indonesia and, according to the Patroli Siber website, 815 cases of offensive material have been disseminated, followed by web fraud in as many as 530 cases, unauthorized access in 104 cases, data theft in 36 cases, device reduction in 17 cases and data manipulation in as many as 54 cases. For 1361 instances, Whatsapp Social Media was ranked first in social media, followed by Intsagram 1288 instances, Facebook 596 instances, and email 108 instances. This research is also carried out in order to provide input to non-bank organizations to take future preventive steps against the risk of cybercrime. The outcome found that for non-bank organisations, there are certain steps that need to be taken in risk reduction.

Keywords: *Risk Mitigation, Cyber Crime, Cyber Threats, Non-Banking Organization,*

I. INTRODUCTION

Cybercrime is a perplexing society today. Global Risk Management's survey outcome addresses that cyber risk in Global Risk is the Big 10. From the smallest thing in the firm, cyber danger is inflicted. It says that 71 percent of organizational threats occur because of the failure of the company to monitor the software, according to the Global Risk Management Report. Although 74% is disputed because the IT system is not updated [1]. PWC noted that there has been a substantial rise in security incidents in the company or individuals over the last 5 years. In 2016, the highest graph was 69% and then there was a promising fall, but there was a 7 percent rise from 2018, which was 44 percent to 51 percent in 2019 [2].

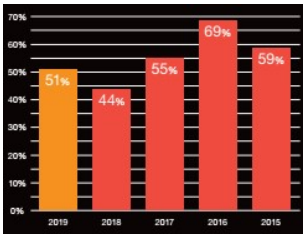

Figure 1: PWC Cybercrime Survey [2]

The perceived impact of the respondents who had witnessed a cyber incident was also reported by PWC. The emphasis is on certain important things, which is that the company's vital infrastructure becomes unavailable for a long time, the loss of the financial side, sensitive information is lost, personal data loss organization [2].

Journal of Theoretical and Applied Information Technology
15th March 2021. Vol.99. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As a special project, Kaspersky developed a platform that provides a wide range of information resources, from intelligence to emerging threats, risk reduction techniques to advisory and investigation services. Kaspersky shows a survey on the Dashboard portal as shown below [3]

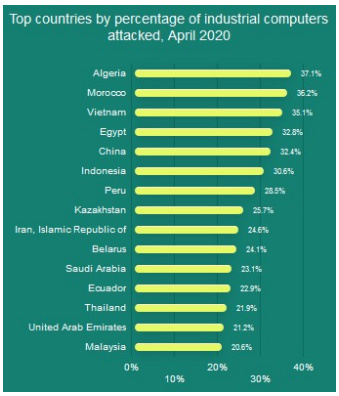

Figure 2: Top 10 Countries of Industrial Computers Attacked [3]

Indonesia is the sixth nation with a computer system that is targeted by cybercrime, according to Kaspersky, which is 30.6% of 16.3 % of the world's computer systems that are compromised by cybercrime. Indonesia took fifth position after Vietnam in January 2019, but the percentage of attacks on the systems did not decrease. This shows that Indonesia is still unable to deal with cybercrime [3]

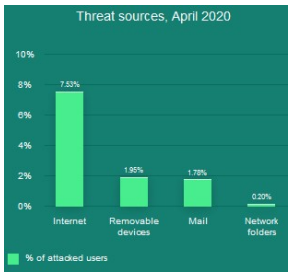

Figure 3: Threat Sources [3]

It appears from the above image that the Internet, composed of hardware, Flash disk, and Email, is the main source of cybercrime [3].

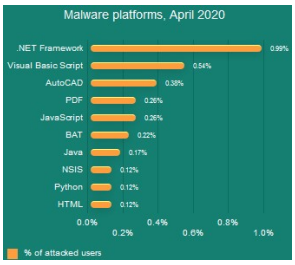

Figure 4: Malware Platform [3]

Kaspersky claims the main carriers of malware come from the .NET Framework. The use of this mechanism is commonly used in Indonesia's application system, so Indonesia still ranks sixth among the top 10 countries whose system is under attack [3].

In developing a portal named "Cyber Police", the police of the Republic of Indonesia paid more attention to cybercrime. There was a spread of provocative content of 815 cases in the portal reported during 2020, followed by online fraud in as many as 530 cases, unauthorized access in 104 cases, data theft in 36 cases, device reduction in 17 cases and data manipulation in as many as 54 cases [4]

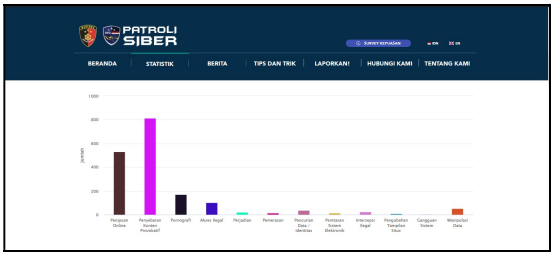

Figure 5: Types of Cyber Crimes Reported by The Public to Police [4]

The Indonesian Crime Patterns map reported in the Cyber Patrol as of February had 513 cases, decreased to 469 cases in March 2020 and decreased to 460 cases back in April 2020 [4].

Figure 6: Indonesia's Cybercrime Trend of 2020 [4]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

For 1361 cases, Whatsapp Social Network was ranked first after breakdown for each category of channel, followed by Intsagram 1288 cases, Facebook 596 cases, and email 108 cases[4].

Fig 7. Reported Platform Type [4]

In an organisation or business, cybercrime has become the primary focus. The right to privacy is given to any mechanism that runs both business and individuals. For now, there is security that we hope will not be able to cope with cybercrime. The best move to defend against cybercrime is to take cybercrime prevention steps. The bank organization, since it is not anything new in the world of banking, will look more prepared to face this cybercrime. As for non-bank organizations, cybercrime is a new thing, especially for fairly small organizations. Not all companies can cope with cybercrime, which is going to happen. This research is therefore focused on Indonesia and is being carried out to provide input to non-bank organizations to take future preventive steps against the risk of cybercrime.

II. LITERATUR REVIEW

2.1 Organisations of non-Banks

Non-bank organizations are business organizations that perform financial activities directly or indirectly through activities to collect community funds and distribute productive activities back to the community. Groups of non-bank institutions include 1) an insurance firm that provides services to estimate risk losses, benefit losses and legal liability. 2)TASPEN (Saving Insurance Pension) is a legal agency administering and running a pension scheme. 3) Save loan cooperative, which is a legal body that raises mutual funds and loans back to members or societies. 4) Stock Exchange/Place of sale and purchase of securities in the capital market, which is a legal body offering facilities for the sale and purchase of securities. (5) Factoring Firm, a business entity which carries out financing activities in the form of the purchase or transfer and management of receivables. (6) Venture capital firm, which is a company the funding of which is made available by a company to its business partners where the financing is made up of a capital spokesperson. 7) Pawnshop, which is an undertaking which lends funds with the assurance of moving goods to its customers. 8) Leasing company, which is a company that provides consumers with buying services in instalments. [5]

2.2 Cyber Crime

Cyber is derived from the technique of the Greek word that has software arts or abilities. It is possible to view criminality as a crime. Cybercrime is a crime committed by a corporation or organization's information system. Crimes committed centered on the use of cyber space is an interconnected space by the use of a network to conduct everyday activities. Positive and negative results can be achieved in the growth of cyberspace. Cybercrime is caused by this negative effect. There are several types of cyber threats, namely: 1) hardware threats that attack hardware triggered by some installation activities of the system. 2) software threats that attack software. This threat is triggered by the incorporation of tools used to carry out information theft, destruction and exploitation activities; (3) data/information risks arising from the distribution of such interest-based data/information activities [6].

According to PWC Cyber treats sources as follow: 1) employees/internals with unintended deeds, 2) criminal groups, 3) hackers, 4) the number of emerging technology, 5) statutory/regulatory criteria are the most commonly found in a business [2].

Different sources of cyber threats include international intelligence, disappointment, investigative reporters, terrorist organisations, hacker operations, and organized crime gangs. Potentially, the possibility of crime is the failure of data information systems, military operations and other intrusion using computer networks and the Internet [6].

2.3 Mitigation of Risk

In anticipation of the possibility of potential damages, risk reduction is an intervention or initial reaction. Risk mitigation strategies require the implementation of risk management mitigation plans to manage or minimize risk to an appropriate level. Once a strategy is adopted, in order to determine its efficacy, it is constantly monitored. 1) risk detection, which is to recognize the risk that may occur in the operating phase, is step-by-step in reducing risk. It is the first step in the process of risk management, 2) determining the effect of an impact assessment resulting from the defined risk, 3) risk prioritization, which is to make risk objectives based on the evaluation of the risk effect that has been carried out. 4) Risk reduction, which is to refresh mitigation based on the risk objectives that have been identified, is the objective of forming the basis for the allocation of significant resources. Actions drawn up need to be regularly monitored to assess the efficacy of the preventive measures against the risks that arise [7].

The risk reduction phase requires the creation of mitigation strategies aimed at managing, removing or reducing risk to an acceptable level. When a strategy has been adopted, its effectiveness should be tracked with the goal of revising the course of action if necessary [8]

2.4 Abbreviations and Acronyms

Table 1: Abbreviations

No	Abbrevations	Meaning
1	PWC	Price Waterhouse Coopers
2	TASPEN	Tabungan dan Asuransi Pegawai Negeri (Savings and Insurance for Civil Servants)

III. METHODOLOGY AND RESOURCES

3.1 Resources and Methods

The literature obtained from many sources, such as papers, journals, the Internet and lecture materials, is used to perform research.

Information protection risk analysis has been studied for a long period of time from the audit viewpoint, according to Sumner (2009) [12] and Rossi (2015) [13]. The most popular approach is to create a collection of checklists to verify the security elements in place and to determine the results of the evaluations on the basis of the auditor's judgment. A matrix-based approach methodology proposed by Goel & Chen (2005) [10] for information security risk analysis was applied for the purpose of this research.

The matrix approach model has enabled a wide range of quantitative analysis to be developed. This approach correlates the organization's assets, vulnerabilities, risks, and controls, and evaluates the value of various controls relating to the organization's assets. The assets of the company are defined as items of value it needs to secure. Properties, such as data and networks, may be tangible and intangible, such as credibility and confidence. The process of assessment was expressed in a risk matrix that shows the risk elements found and their relationships. This paper provides a systematic proposal for the study of quantitative risks.

As a model and observation scenario, the analysis utilized a medium-sized technology company (< 150 employees) dedicated to software growth. The purpose of the study is to provide a realistic model that small and medium enterprises should imitate.

3.2 Systems

In the IT system sampled, there are multiple layers of software technologies included:

- Operational and growth software instruments.
- Accounting and management applications and repositories for internal operations.
- Control of applications or virtual servers operating clients.

The system environment is a client/server architecture consisting of an SQL database (2012 above) designed for Visual Studio .NET (C#, C++) with programming language. Source code, executable program files, data files for development and creation, prototype and completed application code are included in the main platform.

Data development files including of source code, compiled libraries, stored procedures and tables are stored on the Seaget NAS that linked with HP server running on Windows 2019 operating systems and running the SQL 2016 R2 database engine. The code for the program is shared between the various HP servers running Windows 2019. On the separated areas in

Indonesia island, the main building houses local servers was established. A group of virtual servers running Windows 2019 and hosted in a remote Data Centers in Singapore and Bangkok run Executables/Production Systems.

In the Peninsula Islands, users are physically put in one spot. Their personal computers are physically linked with a wide area of the network (WAN). Using the VPN tunnel, programmers connect them to the development field. Operating on the South East Asia regions, there is a business unit that covers more than 100 industries that range from Manufacturing to the hospital. In this unit, access is required to administrative records, sales, production, financial backlogs, and email services. Many trusted Windows Sever 2019-managed domains are run by the business network. There is control of base on the Dashboard of the System.

3.3 Actual Threats Detection

As part of their vision and intent, cyber risk analysis protects a company that adopts IT from a broad spectrum of threats to ensure business continuity, mitigate harm and optimize return on investment and opportunities. The organization's significant assets are any mechanism that supports information systems and networks [13]. Risk identification would allow management to create controls to minimize the risk and impact of hazards associated with vulnerability and cyber security threats. Marcus & John (2000)[13] mentioned that in predicting threats, successful awareness requires:

- Identification and description of the institution's information properties.
- Development of a framework for risk assessment to identify vulnerabilities and existing security threats and to evaluate risks on a specified scale.
- Proposing methods of planning and evaluation that mitigate the risks and hazards described in the risk analysis report.
- Readiness of a Recommendation Report detailing the results to promote the concept of an information security structure tailored to the organization's evidence.

As mentioned by Wang & Chao, a converse-thinking strategy is used by current risk management systems to develop theoretical strategies to mitigate the likelihood of security breaches at a reduced cost[13]. The same authors argue that risk evaluation helps defenders, as presented in Table 2, to define effective countermeasures in conjunction with three separate defensive strategies relevant to the security strategy of the organization.

Table 2: Defensive techniques associated with the Secure of organizations

	Cost of defense	
Contra measures	**Maximum**	**Minimum**
Lower the residual risk		✓
Defend against as many threats as possible	✓	
Display the total amount of avenues of attack	✓	

3.4 Effective Risk Management

Effective risk management must necessarily be aware of the factors that can impact the business, namely:

- What ought to be covered,
- What resources are considered critical and what resources are considered critical and
- If any detrimental effect is reduced by the steps adopted to protect or avoid.

Threats are related to potential factors with a possible adverse effect on the data to the degree that vulnerabilities or shortcomings in the controls that protect them are present in the properties that may be affected. This latter meaning is summarized in the word vulnerability, which puts the organization at risk if the threat is exploited. This risk will be the product of the study of their probability of occurrence and impact on the safe properties.

In other instances, in the absence of a threat to a system, no system can be vulnerable and no unsafe circumstance occurs for an entity, subject or system unless the object, subject or system is exposed to and vulnerable to the potential action that such a threat poses. In other words, there is no danger or independent vulnerability, because situations conceptually defined separately are collectively conditioned for methodological purposes and for a better understanding of risk[13].

The definition of danger typically refers to a system's latent threat or external potential risk; statistically defined as the likelihood within certain circumstances and for a given exposure to time of reaching a level of occurrence of a certain extent. The emergence of threats and the identification of vulnerability needs constant attention from information security professionals due to the inclusion of new assets and poses a

constant challenge to achieving effective information protection [14, 15].

3.5 General Computing Environment Threats

A danger is any aspect that compromises the security of information or computing assets by utilizing or exploiting a vulnerability. Threats emerge from the presence of bugs, irrespective of whether a system's protection is compromised or not. In order to identify risks to a given computer system, it is important to consider each of the threats and vulnerabilities that can damage resources once risks and resources are established and how their harm or failure can impact the organization [17].

There is a clear relation between danger and vulnerability, as already described, to the degree that if one does not exist, the other does not exist either. Typically, emerging risks are split according to their scope:

- Ecological catastrophe (Physical Protection).
- Machine risks (Logical Defense).
- Vulnerability from networks (Telecommunication).
- Risks to individuals (Insiders-Outsiders).

Threats have been defined by looking at the enterprise, the parent corporation, and the market in order to develop our Information Security Defense Matrix. This instrument serves as a defense-in-depth checklist at each point and starts to answer the following questions [18]:

- Specify the threat by asking if an intruder might raise a threat.
- Will anyone have the opportunity for a vulnerability to be exploited?
- Will there be a tradition that exploitation is successful?
- Does anyone have a track record of targeting your industry?

3.6 Assessment of Threats

To perform a risk assessment, the level of risk calculated by previously specified risk criteria during the analysis process must be evaluated. A practical qualitative technique was used for risk. The first stage of the analysis is to classify or evaluate the properties to be covered.

3.7 Description of Effect

If an asset is the target of a hazard, it is not affected with the same effect across all its dimensions. Once it has been determined that a threat will affect an asset, in the event of an active threat, it is necessary to estimate the potential effects. Impact is described as the changes that may occur in the outcomes of one or more goals if the risk materializes, according to Valero. The danger effect is calculated on a cardinal scale between 0 and 9 for this work. As suggested by Caralli (2007) [16], the following levels were used to assess the magnitude of the impact.

Table 3: Impact Scoping

Magnitude of Impact	Impact Definition
Strong [9]	The exploration of vulnerability (1) a highly expensive loss of making realistic assets or resources can result; (2) the intent, reputation or interest of an individual can be significantly breached, harmed or impeded.
Moderate [3]	Vulnerability (1) is responsible for causing the expensive loss of tangible assets or resources; (2) is liable to infringe, harm or obstruct an entity's intent, reputation or interest.
Weak [1]	Exercising a weakness (1) can lead to the loss of some valuable resources or assets; (2) may have a serious impact on the purpose, credibility or interest of the entity.

IV. CRITERIA FOR RISK ASSESSMENT

4.1 Risks that related with System

Computer manufacturing is a highly competitive industry that constantly develops new software, algorithms and commercial applications. Therefore, rivals continually seek to overtake each other. In order to safeguard the corporate resources and to avoid interruption of software development activities, information security is necessary. To translate raw vulnerabilities into risks, a risk calculation matrix was created. The following points were used to base the methodology:

- Categorizing weaknesses
- Pairing of vectors for risks
- Evaluating the likelihood of event and potential effects

4.2 Impact Scale

Different areas are identified in order to perform qualitative risk analysis, where possible

threats produce some degree of impact with respect to the company's operations. It also assesses the impact and likelihood of each, providing a baseline that will set an action plan to minimize these risks as they occur.

Table 4: Description of Operational Effect

Impact Area	Weak	Moderate	Strong
Delivering Service	Small influence on a business unit's results and/or priorities.	Moderate effect on the delivery of services through one or more business units due to extended loss of service.	Significant compromise between the company's business interests and targets.

Table 5: Reputation Impact Definition

Impact Area	Weak	Moderate	Strong
Integrity	Reliability is slightly affected; in order to recover, little to no effort or cost is required.	Reliability is slightly affected; in order to recover, little to no effort or cost is required.	A credibility is irrevocably impaired or harmed.
Customer Loss	Decrease in users of less than 30 percent lead to decreased of interest.	30 to 80 % consumer reduction due to lack of trust.	Due to lack of confidence, customers decreased by more than 80%.

Table 6: Financial Impact Definition

Impact Area	Weak	Moderate	Strong
	Increase in yearly running costs by less than 25%.	Increase in annual operating costs by 25 to 100 %.	Annual running costs are growing by more than 100% .
Costs of Service	An annual sales loss of less than 25%.	25 to 40 % loss of annual sales.	Higher than 40% annual loss of sales.

Table 7: Legal Impact Definition

Impact Area	Weak	Moderate	Strong
Sanctions	Fines amounting to less than $2,000.00 was assessed.	Penalties are assessed between US$2,000.00 and US$40,000.00.	Penalties greater than 40,000.00 US dollars are levied.
The Disagreement	The corporation is charged with non-frivolous lawsuits or fines of less than US$5,000.00.	Between US$5,000.00 and US$50,000.00 are non-frivolous cases or litigation brought against the company.	Non-frivolous cases are brought against the company or lawsuits greater than US$50,000.00.

4.3 Assessing Chances (Probability)

In order to calculate the probability and consequences of risks and to understand their consequences for the project goals, an analytical evaluation is necessary for the performance and objective assessment. Discussions, sensitivity analysis, probability distribution, logistic regression, and measurements are the key tools used. This segment addresses a qualitative scale that has been used to calculate the likelihood of the risks under consideration.

Table 8: Description of The Likelihood Limit

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Rating	Description	Meaning
5	Nearly Sure	Predicted to happen in 1 – 4 months.
4	Entirely possible to	Predicted to happen in 4 – 8 months.
3	Potential	Predicted to happen in 8 – 12 months.
2	Feasible but improbable	Predicted to happen in 1 – 4 years.
1	Nearly Rarely	Not Predicted to happen in 4 years.

Furthermore, confidential data that plays a critical role in the company's everyday operations was also accounted for. The corresponding items are classified into classification categories related to information asset's use and origin.

Table 9: Asset Group Definition

Asset	Location	Group	Priority
Data of Worker	Unrevealed	**Financial Management and Processes**	
Income Statements	Unrevealed		
Information about clients	Unrevealed		
Databases for Businesses	Unrevealed		
Backups	Unrevealed		
Databases of Buyers	Unrevealed	**Tools for Software Engineering**	H (9)
Software Design Document	Unrevealed		H (9)
Documenting Architectures	Unrevealed		H (9)
Apps & Libraries Compiled	Unrevealed		M (3)
Source Code	Unrevealed		H (9)
Password for Network Equipment	Unrevealed	**Governance of the framework**	M (3)
Authentication of Devices for Servers (Production)	Unrevealed		H (9)
Authentication of Devices for Servers (Development)	Unrevealed		M (3)

4.4 Module of Risk

To establish a risk-level quantitative assessment linked to potential risks and vulnerabilities, a risk matrix was created. This was followed by an overall risk rating matrix which, as shown in In accordance with the company's threats and likelihood of occurrence, Table 10 and Table 11 stated the weight of the threats.

Table 10: Risk scale matrix.

Impact	Vigorous	8	16	24	32	40
	Medium	3	6	9	12	15
	Frailed	1	2	3	4	5
		Nearly Rarely	Feasible but improbable	Feaible	Extremely Likeable	Nearly Assured
	Likelihood					

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 11: Max Ranking of Risks: [0 – 200 bottom], [201 – 400 Medium], [+401 top]

Threat		Probability		Impact		Risk Score
DOS	4	Definitely	6	Influence		32
Masquerading's Impersonating	2	Probable	4	Medium		6
Malevolent Script	2	Probable	3	Influence		10
Unintended Failures	3	Extremely	8	Medium		15
Insider Leaks	2	Probable	6	Influence		14
Intrusion	3	Highly	5	Influence		12
Spamming	3	Probable	8	Medium		12
Significant impairment to Peripheral	2	Unlikely	7	Influence		16
Internet apps error such as SQL injection, cross-site scripting	3	Unlikely	6	Influence		24
Internet Application error	3	Probable	5	Influence		24
User Machine Affected such as Virus attack	3	Probable	4	Medium		9
Developer/administrator breached system: e.g. virus infection	4	Probable	7	Influence		27
Test Servers that are unreliable	4	Probable	6	Medium		12
Passcodes figuring	3	Maybe	8	Influence		27
Vulnerabilities of database servers	4	Probable	8	Influence		36
Total Failure System	4	Uncertain	7	Influence		36
Abuse in data	3	Uncertain	7	Influence		27
Environment Catastrophe	4	Probable	5	Medium		12
Total Risk Score						387

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.5 Vulnerability Matrix

Techniques such as checklists and advanced software that assess vulnerabilities at the operating system and network level are used to detect weaknesses in the technology infrastructure. The resulting matrix was computed according to Goel & Chen's guidelines (2005) [17]. This approach correlates the organization's assets, weaknesses, risks, and controls and evaluates the value of various controls relating to the organization's assets. Let's assume, as described in the following formula, that there are q controls that can help reduce p threats and that control ***Z*** is influencing the ***T*** threat.

$$Z0 = \sum_{l=1}^{l=p} eol * Tl$$

Table 12:

Vulnerability Matrix 6 = Influence 4 = Medium 2 = Thin 0 = Not Related Implication/ Priority Levelling 7 = Key Supporter 5 = Crucial 3 = Crucial, not Key Supporter 1 = Not Crucial	Preference / Implication	Credibility (Believe)	Market Missed / Income	Data Reliability	Product relibiality	Communication	Application System	Infrastructure System	Total Score	Rank
Susceptibility		7	6	5	4	3	2	1		
Security Firewalls	7	6	4	6	6	4	6	6	266	1
Data Transfer	7	6	6	4	6	4	6	4	238	2
Databases	7	6	4	6	6	4	2	4	224	3
Applications (data management and analysis, e-business)	5	4	6	6	2	6	6	4	170	4
Internet Service Servers	5	6	2	2	6	4	2	6	180	5
Strength of Passwords	5	6	2	4	2	4	4	2	72	6
Nodes of Clients	3	2	4	4	2	4	2	6	72	7
Internet Based Services (DSL, VPN)	3	4	0	2	6	6	0	0	54	8

5. RESULT & DISCUSSION

The steps in the management process that are introduced in the face of the threat of cybercrime are 1) detection, i.e. the possibility of cybercrime being regularly detected against the triggering of cybercrimes. Identification of all factors must then be assessed and split into two categories, namely probability and probability of effects, 2) evaluation, which is the stage of risk assessment resulting from cybercrime that affects all aspects of life. The assessment is assessed using cybercrime-induced matrices and risk assessments. 3) The next step is to coordinate the risk response and intervention after performing recognition and risk assessment. 3) Danger. At this stage, information and data theft must be controlled individually or by institutions; 4) regulation, a monitoring and improvement stage that continues to determine the effectiveness of risk management. Early alert for security controllers to expect cybercrime has been included in the monitoring process [6]

The cybercrime eradication approach is by a violent criminal conduct program in the law such that the act falls into the cyberspace crime group. In addition to developing policies outside criminal law to help cybercrime prevention efforts, socializing against the potential of cybercrime, building cooperation with private parties and establishing an institutional network in the national and international sphere to deter cybercrime [9]

Some businesses also have objectives to fight cybercrime, including 1) performing cybercrime awareness training, 2) accessing data in compliance with the Authority, 3) introducing cyber information and security strategies, 4) restricting the network, 5) installing/creating malware detector, 6) replacing old system upgrade technology [2]

V. CONCLUSIONS

The risk reduction steps that need to be done by non-bank institutions are based on some literature that has been reviewed and discussed:

1) Detection of hazards that exist in the organization or business
2) Appraisal of the identified risks
3) Construct a matrix based on the results of the test.
4) Establish preventive measures against the results provided by the matrix, including:
   a) Provide socialization and cybercrime training.
   b) Limit requests for data in accordance with its competence.
   c) Limit network access.
   d) Installing/creating Detectors for malware
   e) Replace with newer systems the old system.
5) Establish databases for any risk reduction steps taken.
6) Monitor the execution of the compiled actions.
7) A routine analysis of the risks and of the steps already taken.

REFERENCES:

[1] Deliote, “Global risk management survey , 11th edition Reimagining risk management to mitigate looming,” 2011.
[2] PwC, “Cybercrime Survey 2018,” *Cybercrime Surv.*, 2019.
[3] Kaspersky, “Kaspersky ICS CERT | Kaspersky Industrial Control Systems Cyber Emergency Response Team,” 2020. .
[4] Polri, “Patroli Siber,” 2020. .
[5] T. Abdullah, “Lembaga Keuangan,” pp. 1–43, 2015.
[6] I. Rahmawati, “Analisis manajemen risiko ancaman kejahatan siber,” *J. pertahanan Bela Negara*, vol. Vol.7, no. No.2, pp. 51–66, 2017.
[7] N. Katende, “IMPLEMENTING RISK MITIGATION , MONITORING , AND MANAGEMENT IN IT,” no. July 2017, 2019.
[8] N. Katende, K. Ann, and K. David, “Implementing Risk Mitigation, Monitoring, and Management in It Projects,” *Comput. J.*, no. July 2017, pp. 1–8, 2017.
[9] D. Bunga, “Politik hukum pidana terhadap penanggulangan,” *J. Legis. Indones.*, vol. Vol.16, no. No. 1, pp. 1–15, 2019.
[10] Goel, S., Che, V. (2005). Information security risk analysis a matrix based approach. Retrieved from http://www.albany.edu/~GOEL/publications/goelchen2005.pdf

[11] Rossi, B. (2015). Critical steps for responding to cyber attacks . Retrieved from http://www.information-age.com/technology/security/123459644/6-critical-steps-responding-cyber-attack

[12] Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, 26(1), 2-12. doi: 10.1080/10580530802384639 9.

[13] Marcus, R., & John, B. (2000). Access Control Systems and Methodology Information Security Management Handbook, Four Volume Set: Auerbach Publications.

[14] Demidecka, K. (2015). Communicating a Cyber Attack - A Retrospective Look at the TalkTalk Incident. Retrieved from http://www.contextis.com/resources/blog/communicating-cyber-attack-retrospective-look-talktalk-incident/

]15] Forester Research. (2015). Protect Your Intellectual Property And Customer Data From Theft And Abuse. Retrieved from https://www.forrester.com/reports/

[16] Caralli, R. (2007). The OCTAVE Allegro Guidebook, v1.0. Carnegie Mellon University.

[17] Creasey, J., & Glover, I. (2013). Cyber security incident response guide. Retrieved from http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf

[18] NIST. (2012). Computer security incident handling guide. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf