EVALUATION OF CYBER SECURITY IN THE BANKING SECTOR OF BANK BTN SURABAYA BRANCH

Rudiatno[1], Aldea Mita Cheryta[2]
Universitas Wijaya Putra[1,2]
Email korespondensi: rudiatno@uwp.ac.id

Abstract

This study discusses the evaluation of cyber security policies in the banking sector at Bank BTN Surabaya using qualitative methods and data collection techniques indepth interviews and focus group discussions. The focus of this study is policy evaluation and prevention of cybercrime in banking. The location of this study was conducted at Bank BTN Prioritas Surabaya Branch, the selection of the location of this study was due to bank BTN being one of the banks that implemented preventive measures in preventing cybercrime. The problem that will be described in this article is First, How is the impact of cyber security on Bank BTN Surabaya Branch? Second, What is the government's policy strategy on cyber security? Third, How to prevent cyber-crime at Bank BTN Surabaya Branch? The conclusion of this study is that Bank BTN Surabaya shows good preventive steps by forming a special organizational structure to deal with legality issues and the implementation of cybercrime prevention applications. Bank BTN conducts policy evaluations every two weeks as a form of evaluation of target achievement and monthly evaluations carried out by their superiors directly. Furthermore, every six months Bank BTN Surabaya brings in an external audit to be able to supervise and monitor.

Keywords: *Bank; Cyber Security; Evaluation*

1. INTRODUCTION

Policy evaluation is one of the most important efforts in public policy making. The application of evaluation produces a real improvement and can be the main reference in the improvement of a policy, apart from this evaluation is also the main standard in the final stage of formulating a policy. The study (Calderaro & Craig, 2020) concludes one analysis that policymakers should continue their efforts to increase knowledge in countries that have not yet fully implemented connectivity.

Evaluation is always accompanied by empirical monitoring, so that the effectiveness of an evaluation can function better. However, often an evaluation is used as a normative requirement to implement a policy that exists in society. The consequence of such a policymaker is to risk the condition of the integrity of the people in developing their social activities. Moreover, if the direction of a policy is not on target, it will actually become a contradiction in society, finally the level of public trust. Today public trust is measured based on quantitative surveys to calculate whether each individual feels helped by the policy.

Policy evaluation will be continuously applied to policies that are still new in nature as well as new issues that exist in the community. One of these issues is cyber security, which is a major benchmark in the success of transformation policies. It is possible that a policy can have a bad impact, because the direction and objectives of the policy targets cannot be adjusted to the empirical conditions of society. Cyber security is very important to reconsider so that there is a high level of trust which has implications for accelerating investment turnover.

Research (Stevens et al., 2019) proposes that in a crucial area there must be intelligence and security cooperation that urgently needs to be improved, cyber security challenges are the most common cyber-crime that will have special implications in the case of Brexit in Europe. The case of Brexit in Europe is a world lesson about the importance of evaluating cyber security to exist amid the onslaught of cyber-crime actors. The main point of Brexit in Europe is the weak cyber security at that time to deal with sudden attacks on the banking sector.

The banking sector is the most vulnerable sector to cyberattacks, considering that so many transactions occur in the banking sector. The extremes of a weak banking sector for example can have implications for parming, spoofing, keyloggers, phishing, sniffing and carding. Some of these problems are the main points of how the government's policy in implementing and interpreting so as to maintain the stability of the banking sector. Banking auditors of the digital age require special skills to be able to analyze better and precisely. At least (Rosati et al., 2020) reminds that cyber security incidents are focused on established proxy checks for the quality of banking audits. The implication is that the auditor is required to be able to understand certain proxies so that he can better audit modern banking.

Recent research initiated auditors who responded to cyber security incidents by charging their clients higher surcharges (Lawrence et al., 2018; Li et al., 2020; Rosati et al., 2019). Even a cyber security breach can result in the possibility of a re-audit of financial statements at the time of the breach (Lawrence et al., 2018). Auditors should update their skills and ability to audit financial reports so that additional insights with respect to the implications of cyber security on the quality of financial reporting (Rosati et al., 2020). Although there are some loopholes in internal control that increase audit risk, it does not determine the decline in audit quality.

The main focus of this research is the banking sector at Bank BTN Surabaya Branch. This focus is important to provide literature on cyber security policy evaluation. The hope in the future is that this research contributes significantly to the development of science as well as addressing empirical problems faced by society. Some of the cyber attacks on banks in Indonesia will be presented through Table 1 as follows:

Table 1. Indonesia's Cyber Crime Trends

No	Number of Online Scams	Illegal Action	Year
1	1.430	153	2017
2	1.781	263	2018
3	1.617	248	2019
4	1.319	303	2020
5	508	167	2021

Source: (Idntimes, 2021)

Based on Table 1, it can be explained that cyber-crime in Indonesia is massive and the trend tends to increase except in 2020 and 2021 which are indicated by the Covid-19 pandemic. Meanwhile, in 2017 and 2018 there was an increase of more than 50% in cyber-crime cases. This indicates that regulation of cyber-crime policies and the participation of users to reduce cyber-crime is urgently needed.

Cyber-crimes that occur around the world have an explosive impact on each country's annual financial statements. Some more detailed types of cyber-crime will be described in Table 2 as follows:

Table 2. Types of Cyber Crime

No	Types of Crimes	Information
1	Phishing Crimes	*Cyber-crime to commit fraud by tricking victims*
2	Carding Crimes	Crimes committed by transacting using someone else's credit card
3	Ransomware Attacks	*Malware or malicious software that can not only infect computers, but also hold user data hostage*
4	Online Scams	Fraud mode under the guise of a selfie of id card or other personal identity
5	SIM *Swap*	Mode of taking over someone's mobile number to hack
6	Site and Email Hacking	Crime by hacking a site or email to change its appearance
7	The Crime of Skimming	The crime of stealing debit or credit card data to withdraw funds in the account
8	OTP Fraud	Crime of misuse of one-time codes to access or complete transactions
9	Data Falsification	Crime by falsifying important data or documents over the internet
10	Illegal Content	The crime of entering data or information is untrue, unethical, unlawful or disrupts public order
11	*Cyber Terorism*	Rations that interfere with or make damage to computer networks
12	*Cyber Espionage*	The crime of using the internet network to spy on others
13	Plagiarizing Other People's Sites	The crime of violating IPR on others on the internet

Source: (Republika, 2021)

Table 2 shows the various kinds of cyber-crimes that occur in Indonesia, not closing the possibility that in the following year there will be other types of crimes. This implies that the potential of cyber security must continue to be improved, so as to prevent different cyber-crimes. This research actively seeks to evaluate cyber-crime policy policies in the banking sector.

Based on Law Number 19 of 2016 Article 31 paragraph 2 explains that "Everyone intentionally and without rights or against the law intercepts the transmission of Electronic Information and/or Electronic Documents that are not public from, to and in a computer and/or certain Electronic Systems belonging to others, whether they do not cause any changes or changes, omission of, and/or termination of electronic information and/or electronic documents being transmitted". The legality of this legislation implies that cyber security has been given a legal basis, but often in the application of policies it becomes multi-interpretive so that the direction and purpose of the policy becomes floating.

The big themes in this study are policy evaluation, cyber security, and banking. This study discusses paradigmatic debates to provide appropriate policy alternatives to the cyber security policy of the banking sector. The locus of this research is at Bank BTN Surabaya Branch. Furthermore, this research seeks to contribute to policy evaluation so that later policy updates can be more precise and directed.

The state of the art research refers to the policy of referring to the cyber policy of the United States which has two important reasons namely: First, the United States became the trendsetter of the evolution of cyber space; Second, lessons from the U.S. case can be applied informing, and policy decisions in other countries (Lilli, 2020). Furthermore, this research will seek to analyze the perspective of policy in the United States on banking to be applied at Bank BTN Surabaya Branch. The rationalism of the policy is also one of the focuses of the research carried out. Rationalism is important to get maximum suitability and implementation when applied at Bank BTN Surabaya Branch. Further to explain the state of the art this research will be explained in the next chapter using Vosviewer.

The urgency of this study is to analyze cyber security policies at Bank BTN Surabaya Branch based on the researcher's initial analysis that often cyber security policies become multi-interpretation. Furthermore, this study seeks to provide a strategy about efforts to narrow the space for cyber-crime which is an implication of cyber security. The initial problem will be analyzed using qualitative tools on policy evaluation.

The problem that will be described in this article is First, How is the impact of cyber security on Bank BTN Surabaya Branch? Second, What is the government's policy strategy on cyber security? Third, How to prevent cyber-crime at Bank BTN Surabaya Branch?

Literatur Review

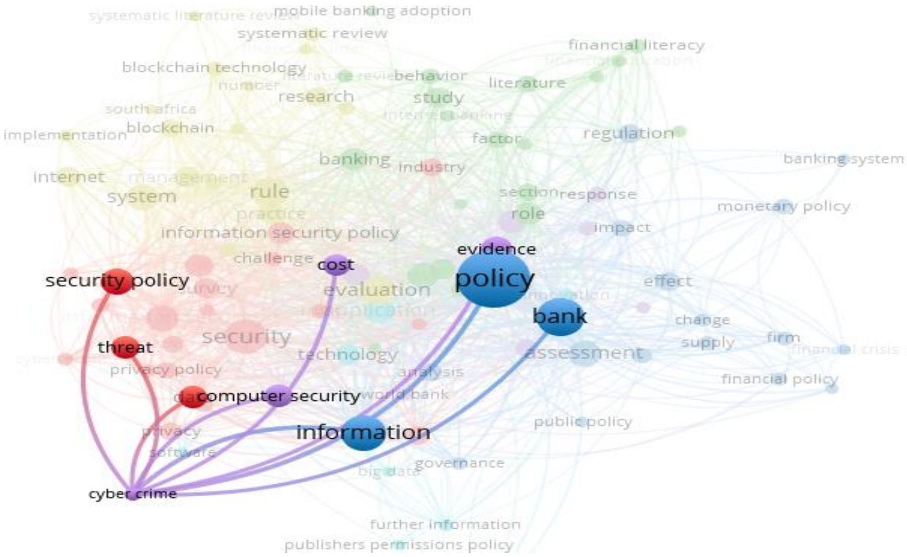
Theoretically, the researcher will explain some of the previous research that has been carried out and collect some international article literature that is relevant to the research to be carried out. Some of them are research (Rosati et al., 2020): This research supports the initial hypothesis written by the researcher and found that banking auditors did not reduce the quality of their audits despite the issue of cyber security. This research is the main basis that auditors in the United States have good competence, and later this research will further analyze how the femonene is if applied in Indonesia. The difference between this research and the research that will be carried out is that this research method uses qualitative to explain the phenomenon of cyber security while the research cited explains through empirical data about audits in the United States. This research will also explore cyber-crime prevention policies in Indonesia.

Research (Elijah, 2018): This study discusses the French problem of the government taking over policies on cyber-security and slightly opposes the view that government intervention lies in the economic sphere. Cyber security is considered very important to the French government, so the country takes over the role even though there is a stigma that government intervention goes too far. The difference between this research and the research that will be carried out is that policy evaluation in Indonesia will be possible if the government goes deeper into legality restrictions so that cyber security can be more controlled and cause continuous stability. Furthermore, this research will contribute to the literature of evaluating appropriate policies in the field of cyber security in Indonesia.

Research (Huang & Li, 2018): This study reviews weak oversight and also the focus of funding on cyber security in Taiwan. This research is an initial allegation to analyze the extent of the Indonesian government's intervention in the cyber security surveillance of the banking sector in Indonesia, considering that banks in Indonesia are prone to cyber-crime. The similarity of this study is to observe that whether there is a research agreement with the policies implemented by the government. At least this conjecture is important and interesting to observe as well as analyze as one of the references to cyber security policies in the Indonesian banking sector.

The next presentation is the result of vosviewer data processing which will explain the location of the state of the art of this study based on the Scopus database and google scholar which is the reference of many researchers. Based on the results of the Vosviewer analysis, the following results were obtained:

Figure 1. Vosviewer Data Processing Results



Source: Vosviewer, data processed by the Author (2022)

Based on the results of the analysis of the google scholar and Scopus databases used in the Harzing's Publish or Perish application, data was obtained that research using the themes of policy evaluation, cyber security, and banking indexed by Scopus did not exist. The three themes are novelty based on Vosviewer data showing the novelty of the research in Scopus literature if published in the international artikle. The smaller the sphere shown in Figure 1, the less the research is indexed by Google Scholar and Scopus. Based on the picture, we can see that the theme of cyber security and banking has nine articles on Scopus. The significance of this study is the contribution of the discussion on policy evalausion.

Policy Evaluation Theory

According to (Situmorang, 2016) policy evaluation is needed to prevent policy failures while in accordance with predetermined directions and objectives. Policy evaluation is not only carried out at the end, but enters the process of the stages of a policy. Evaluation at least consists of: specification, measurement, recommendations and analysis. Some types of policy evaluation consist of: 1) Evaluation is a functional activity that is seen as the same activity as policy making;

2) Evaluation has a focus on performance so as to choose honesty and efficiency in its implementation; 3) Policy evaluation seeks to provide answers to the question of policy conformity with the initial sales objectives while mapping the benefits achieved and the beneficiaries of the policy.

The purpose of carrying out the evaluation is to provide literature and views on policy objectives, including policy externalities. There are three elements used for the implementation of the evaluation, namely: 1) Describing the policy output that is the result of policy implementation; 2) Evaluation deals with the improvement of social problems; 3) Evaluation relates to policy consequences in the form of government actions and reactions.

Policy evaluation often experiences obstacles at its stage of the process, some of these obstacles include: 1) Uncertainty of policy objectives; 2) Casuality; 3) Dissemination of policy impacts, where the impact is part of a group outside the main target group; 4) Unopened access to relevant data and information in the implementation of evaluas; 5) Resistance of officials, so that the evaluator must be able to express objectivity in obtaining knowledge; 6) evaluation can reduce externalities so that it doesn't get many extensions or get waivers.

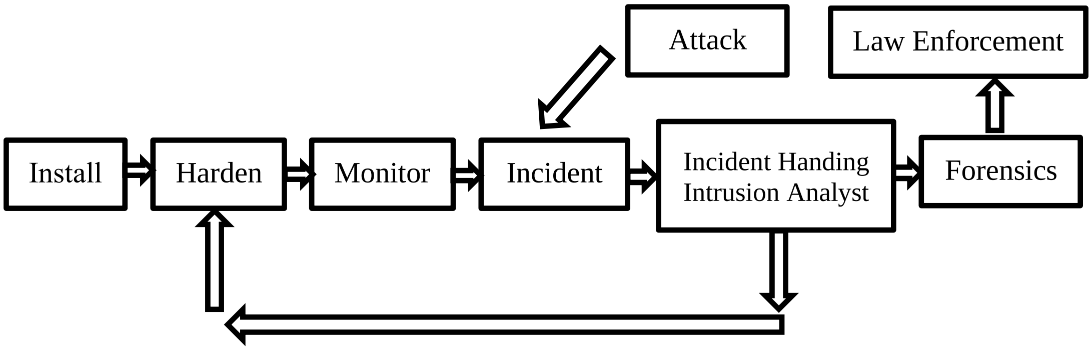
Furthermore (Situmorang, 2016) explained that there are several causes for policies not to have a real impact in accordance with the original objectives, namely caused by: 1) Insufficient resources; 2) Improper evaluation methods; 3) The complexity of public issues while policy focuses on a single problem; 4) The way the community responds to policies is also very important in the policy evaluation process; 5) The contradiction of one policy with another; 6) High cost; 7) It is not possible to solve all public problems; 8) Concerned with the nature of the problem to be resolved based on the actions of the policyholder.

Cyber Security Theory

Cyber security is a set of tools, security policies, protection against security, actions, training, assurance and technology that are used as protectors in the environment in cyber environments and user asset organizations. This organization is integrated with the connection of computing, infrastructure, applications, communication systems, and the totality of information transmitted in a cyber environment (Ardiyanti, 2016).

Cyber-security is one of the efforts to ensure the achievement and maintenance of the security nature of the organization and user assets against security risks that may occur. The general purpose of cyber-security is the integrity in it that allows efforts to address the occurrence of serious cyber threats. Globally, cyber-security is applied based on five areas of work, namely: 1) Legal Certainty (legality of cyber-crime); 2) Technical and procedural action; 3) Organizational Structure; 4) Capacity building and user education; 5) International cooperation. Furthermore, the scope of cyber-security will be explained in Figure 2 as follows:

Figure 2. Scope of Cyber Security Policy



Source: (Ardiyanti, 2016)

The theoretical data in Figure 2 explains that the scope of cyber-security starts from the installation or security carried out in the hardware used in the operation of the internet, monitors, which provide opportunities for cyber-crime. Cyber-security complex mechanisms protect and minimize confidentiality, availability, and integrity. Cyber-security is an effort to protect information from cyber-attacks, some of the main elements in cyber-security are: 1) The security policy document is a standard document of reference for carrying out all information security; 2) Information infrastructure is the continuity of operations using hardware and software; 3) Primere defense, which is a component of information infrastructure defense such as firewalls; 4) Network monitoring system, namely monitoring the feasibility of utilities and information infrastructure performance; 5) System information and evant management play a role in monitoring network events used in security incidents; 6) Network security assessment acts as a controlling mechanism and provides measurement of information security levels; 7) Human resources and security awareness related to resources. Another variable that needs to be taken into account is the continuity of physical security related to physical element systems such as data center buildings, disaster recovery systems, and transmission media.

2. METODE PENELITIAN

This research is to use qualitative methods that use interviews, documentation, and observation in analyzing femomena problems. Furthermore, this study analyzes primary data and secondary data to be applied using the theory used in this study. The data will be analyzed in more depth so as to form a scientific-natural conclusion that can be accepted by various groups, especially in this case the banking sector at Bank BTN Surabaya Branch as the object of this study.

Descriptive research analyzes interviews, survey results, field research, content analysis, mass media, and historical comparative research. This study used a snowball sampling informant determination technique that allowed researchers to obtain additional informants when interviews were conducted. Furthermore, the initial informants of this study were:

Table 3. Research Informants

No	Informant's Name	Work
1	Setia Budi	Teller Service Bank BTN Cabang Surabaya
2	Dedo Pratika	Customer Sevice Bank BTN Cabang Surabaya
3	Nanti Sulis	Teller Service Bank BTN Cabang Surabaya
4	Eric Saputra	Marketing Bank Sinarmas

Source: Author's Dioalah Data (2022)

The focus of this study is the evaluation of cyber-security policies in the banking sector at Bank BTN Surabaya Branch. This issue is very important to be researched based on the state of the art that has been explained upfront. This is also the novelty of the research combined with the theories used in this study. This research took the research location at Bank BTN Surabaya Branch located on Jl. Pemuda No. 50 Embong Kaliasin, Genteng District, Surabaya City. This research was conducted at one of the banks in the city of Surabaya for more details and specifics about the discussion of cyber security. Data analysis techniques use data triangulation based on the results of indepth interviews, documentation, and observations.

3. RESULT AND DISCUSSION

Interpretation of Policy Evaluation Theory

Based on the theoretical tools of policy evaluation, it is often difficult to create policies that are acceptable to all parties. Of course, this cannot be a relief for all parties, because a policy is formed based on problems that occur in society. Cyber security policy gets the largest share in the creation of a digital economy, because the security system is the main foundation in the creation of a digital application. Often cyber security policies in the banking sector have loopholes that can be exploited by irresponsible individuals to commit cybercrimes. This article seeks to further analyze based on the theoretical tools of policy evaluation.

Policy evaluation theory initiates obstacles that occur at its stages including: 1) Uncertainty of policy objectives, uncertainty of policy objectives is one of the important points in the sustainability of a policy. Regardless of the dynamics of the problem that occurs, that the objectives of the policy must lead to one of the parties to which the policy will be implemented. The overlapping of policies is also some of the things that public policymakers must take into account; 2) Improper evaluation method, the second indicator of success is the evaluation method used. Complex evaluation should involve internal audits and external audits, so as to create an output that can evaluate in detail the policies to be produced. External audit is needed as a form of evaluation that is not tied to the interests that exist internally, and of course this will result in a more mature and directed evaluation; 3) The spread of policy impacts, which is an indicator that assumes the effects caused by the implementation of the policy. This impact must be carefully and carefully calculated to the external conditions of policy implementation. Often the application of policies does not consider with certainty how the multiplier effect is caused when implementing the policy; 4) The lack of open access to relevant data and information in the implementation of the evaluation is the next indicator in the non-achievement of policy targets. Incomplete data information causes some public policies to be very ambiguous, and of course this will actually cause polemics in society; 5) Resistance of relevant officials, this has implications for bureaucratic reform. An organization must be able to adapt its system to the latest developments in society so as to create an organizational atmosphere that is friendly and has conformity with public needs. Some authorities who are reluctant to transform will be a burden in themselves in the implementation of policy evaluation; 6) Evaluation can reduce the impact of externalities, at the evaluation stage it is in dire need of external and internal evaluation. The internal evaluation will show some of the impact of the evaluation on the internal organization, while the external evaluation will take into account the impact of externalities outside the organization.

Furthermore, this article will discuss how cyber security policies do not have a real impact according to (Situmorang, 2016) in accordance with the original objectives caused by several things, namely: 1) Insufficient resources, this day a source includes cybersecurity capabilities in closing the loopholes that allow cybercrime to occur. Of course, preventive measures must always be implemented so that a policy can have a continuous impact; 2) Improper evaluation method, the bank must be careful in implementing the evaluation so that there is no blankness of evaluation or an ignorance of the problems that occur in their organization. In addition, in the application of evaluation, it must gain the right momentum in order to be accepted by the majority of members of the organization and this is important in an evaluation; 5) Policy contradictions, another issue that needs to be considered by the banking sector is the overlapping of policies resulting in multiple interpretations understood by members of the organization. This policy overlap does not only occur in the organizational environment sometimes also occurs outside the organization, the synchronization of external legality policies with internal legality is one of the next crucial things so that it is necessary to form a legal division that specifically handles the synchronization of the legality of the legislation; 6) High cost, a mature evaluation certainly requires a lot of costs. This budget should always be set aside from the results of the resulting production, so that at any time it can be possible to carry out an evaluation. The number of members of the organization determines the amount of cost needed, the higher the cost required for each evaluation carried out; 7) It is not possible to solve all problems, the next technical problem in policy making is the partiality of the policy towards certain parties. Of course a public policy cannot fairly benefit all parties, because indeed it must choose partisanship based on the views of libertarianism or utilitarianism. This partisanship is at odds between the freedom of each individual and the freedom based on the majority of society; 8) Conflict resolution mechanisms of policyholders, potential subsequent policy failures are caused by improper conflict resolution mechanisms. This is because a leader needs determination to be able to accommodate the problems that occur in their organization. This ability to accommodate is the main foundation in overcoming internal conflicts that occur.

Research (Sari et al., 2019) shows the results that the concentration in the development of an organization lies in Human Resources and the special training provided. This is done to facilitate policy development and increase the production potential of the organization's management. The support is shown by research (Puspitasari & Kartika, 2019) that an evaluation of the organizational field takes into account the concept of Human Resources, especially in providing performance compensation and assessment directly by superiors. This assessment becomes important as a first step in evaluating the organization, almost every sector line of the organization takes into account how the evaluation is carried out by the direct leader. Further research (Syovina et al., 2020) the quantity of qualified evaluations causes high trust in the community, this is proven by the existence of a family business image promotion that stably maintains the quality and quantity of goods so that they can be trusted even though they are not directly owned by the first owner.

The results of the indepth interview conducted at Bank BTN showed that policy evaluations are carried out almost every month by direct supervisors as well as evaluations carried out by external parties. The results of the data reduction carried out by Dedo as the priority teller of Bank BTN Surabaya showed the following results:

"At Bank BTN, it is periodically assessed by superiors directly almost every month, in fact, we have a policy evaluation every two weeks. The main goal is of course to achieve the target criteria set by the company and personally improve the quality and capability of the individual". (Interview conducted on June 4, 2022 at Bank BTN Surabaya)

Based on the interviews that have been carried out, it shows that the evaluation is carried out almost every two weeks and once a month for evaluations carried out by the immediate supervisor. Meanwhile, for the evaluation of cyber security policies, Bank BTN coordinates with IT as a cyber security service provider to take preventive steps in anticipation of preventing the rampant cybercrime that occurs. This is supported by an interview conducted with Pak Budi as General Manager of Bank BTN as follows:

"Regarding cyber security, we coordinate with IT experts as well as with the police, so that we can find out the latest modes carried out by irresponsible individuals. We continue to learn how this mode can be prevented, because of course it will cause a massive loss if the bank is still slack in implementing banking security. And of course this reduces people's trust to save at Bank BTN, therefore I am very concerned for the prevention and handling of this cyber security". (Interview conducted on June 4, 2022 at Bank BTN Surabaya)

The coordination carried out by Bank BTN with the police and IT parties serves as a prevention and a preventive measure in anticipating cybercrime. The security factor is one of the important points in digital sustainability, apart from this, of course, as a form of banking services to be able to provide a sense of comfort and security when customers transact.

Interpretation of Teory Cyber Security

The implementation of cyber security policies assumes at least five areas of work, namely: 1) Legal Certainty, in this case bank BTN formed a special team to handle legality and actively coordinate with other banks and with the police on how preventive measures should be taken as a form of cybercrime prevention; 2) Technical and procedural actions, technical implementation is carried out by experts in their fields, namely the field of Information Technology which was formed by Bank BTN as the frontline in tackling cybercrime. Generally, coordination is carried out by the OJK as a state institution authorized to re-check suspicious transactions; 3)

Organizational structure, this has been actively carried out by Bank BTN through the formation of a special IT Team that is structured in the organization so that it can hierarchically propose directly to the leadership what steps should be taken; 4) Capacity building, in this case Bank BTN is less complex in providing literacy to customers about how to improve the security of online transactions, including how to prevent cybercrime, is not explained in detail by the Bank. This is a special note for Bank BTN to improve the quality of banking services on capacity building indicators; 5) International cooperation, regarding international cooperation, Bank BTN does not actively cooperate directly but in implementing that the police must have coordinated directly with international institutions such as the FBI to prevent cybercrime from spreading.

Based on research (Putra, 2020) shows that consumer confidence will be high when a review of an organization is well realized. This implies to Bank BTN that the image and services of Bank BTN will be a benchmark for customers to be able to transact at the Bank. Of course, maintaining this image is not easy considering that the forms of cybercrime modes are increasingly varied and massive, but this is not the main reason for not providing the best service for customers. Research (Yadewani et al., 2020) reminds the importance of digital platforms as a company's brand image. Promotional support and good website design will certainly increase customer trust regardless of the cyber issue that is not only experienced by Bank BTN but by all banks in Indonesia. With a good brand image, the issue of cybercrime fades so that it can increase customer trust.

Government Policy Strategy Related to Cyber Security

We can understand that cyber security is one of the most crucial things in the digital economy. Even in all sectors, it is explained that the level of security is the main point in its sustainability. The government in this case does not massively allocate and adapt to the development of the times, especially the development of cyber security. This study found that the estuary of a less than optimal cyber security policy strategy is about budget allocation for the development of security systems. Based on the theoretical tools that have been reviewed in the previous sub-chapter, it is found that the government's way of allocating cyber security development budgets is still not optimal. This has implications for the strength of the government's cyber security system.

On the other hand, we find that government budget allocations will be difficult to implement because cyber systems are difficult to measure their achievement. Cyber security is measured by the number of cyber cases that occur, and that is just the main standard that can be applied. In contrast to the allocation of education budgets, for example, there is a standardization of the measure of educational achievement, namely the number of graduates or the number of students' learning to increase. It is also a challenge for the government to be able to adapt to the cyber security budget allocation.

Research (Budhi, 2016) analyzed that the weakness of the government lies in innovation strategy, consumer data security, Analysis (Karim, 2020) is that the government does not provide the widest possible space for the availability of the internet and network for its people. Of course, this is crucial for the acceleration of information in society, although we can understand that the acceleration of information can also lead to negative things. The main point is that the acceleration of information delivery through an internet connection has not been able to be facilitated by the government properly. The acceleration of this information can lead positively considering that various information can be accessed through the internet and social media.

This article suggests policy strategies related to cyber security as follows: 1) Open access to information and good network availability; 2) Cooperate with overseas cyber security; 3) Accommodate local programmers; 4) Increase budget allocations and focus on improving cyber security; 5) Strengthen all government institutions and prepare cybersecurity experts in every position of government agencies. Some of these strategies are aimed at at at least reducing the massive cybercrime occurring in Indonesia. Of course, there is great hope that the government can deal with and narrow the loopholes for hackers to be able to carry out their actions.

4. CONCLUSION

Cyber security in the banking sector is a massive issue experienced by almost all banks in Indonesia. Of course, this is a serious challenge and requires high efforts in efforts to prevent and limit the opportunities for cybercrime to occur. Bank BTN Surabaya shows good preventive steps by forming a special organizational structure to deal with legality issues and the implementation of cybercrime prevention applications. Bank BTN actively evaluates policies every two weeks as a form of evaluation of target achievement and monthly evaluations carried out by superiors directly. Furthermore, every six months Bank BTN Surabaya brings in an external audit to be able to supervise and monitor some things that are not in accordance with the legality of the law. This external audit can come from Bank Indonesia or the Financial Services Authority which is authorized to record and monitor banking financial transactions.

This research has limited locus of research in one place, it is very likely to be improved by comparing with other banks to be able to compare and show the advantages of each bank. It is hoped that the next researcher in using the research locus is more complex and not limited to the theme of cyber security. Furthermore, this article can be a logical reference on the implementation of cyber security policy evaluation in the banking sector.

DAFTAR PUSTAKA

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1).

Budhi, G. S. (2016). Analisis Sistem E-Commerce Pada Perusahan Jual-Beli Online Lazada Indonesia. *Elinvo (Electronics, Informatics, and Vocational Education)*, *1*(2), 78–83. https://doi.org/10.21831/elinvo.v1i2.10880

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Elia, D. D. (2018). *Industrial policy : the holy grail of French cybersecurity strategy ? Industrial policy : the holy grail of French cybersecurity strategy ?**. *8871*. https://doi.org/10.1080/23738871.2018.1553988

Huang, H., & Li, T. (2018). A centralised cybersecurity strategy for Taiwan A centralised cybersecurity strategy for Taiwan. *Journal of Cyber Policy*, *0*(0), 1–19. https://doi.org/10.1080/23738871.2018.1553987

Idntimes. (2021). *Serangan Siber Meningkat, Sektor Keuangan Paling Terancam*. https://www.idntimes.com/business/economy/helmi/hati-hati-sektor-keuangan-paling-terancam-nomor-2-kejahatan-siber/3

Karim, B. A. (2020). Pendidikan Perguruan Tinggi Era 4.0 Dalam Pandemi Covid-19 (Refleksi Sosiologis). *Education and Learning Journal*, *1*(2), 102. https://doi.org/10.33096/eljour.v1i2.54

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies? *Auditing: A Journal of Practice & Theory*, *37*(1), 139–165.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151–171.

Lilli, E. (2020). President Obama and US cyber security policy President Obama and US cyber security policy. *Journal of Cyber Policy*, *0*(0), 1–20. https://doi.org/10.1080/23738871.2020.1778759

Puspitasari, S., & Kartika, L. (2019). Evaluation of Job Analysys and Need for Trainingon Jakartapamong Praja Units. *Jurnal Apresiasi Ekonomi*, *7*(3), 219–231. https://doi.org/10.31846/jae.v7i3.237

Putra, E. (2020). Pengaruh Promosi Melalui Sosial Media Dan Review Produk Pada Marketplace Shopee Terhadap Keputusan Pembelian (Studi pada Mahasiswa STIE Pasaman). *Jurnal Apresiasi Ekonomi*, *8*(3), 467–474. https://doi.org/10.31846/jae.v8i3.298

Republika. (2021). *13 Jenis Kejahatan Siber | Republika Online*. https://www.republika.co.id/berita/r0sm8s6116000/13-jenis-kejahatan-siber

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, *54*(03), 1950013.

Rosati, P., Gogolin, F., Lynn, T., Gogolin, F., & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. *European Accounting Review*, *0*(0), 1–28. https://doi.org/10.1080/09638180.2020.1856162

Sari, V. N., Sari, M. W., Yulia, Y., & Wati, R. H. (2019). Marketing Strategy of Chicken Egg on Nrps Shop in Tanah Datar. *Jurnal Apresiasi Ekonomi*, *7*(1), 67–78. https://doi.org/10.31846/jae.v7i1.189

Situmorang, C. (2016). *Kebijakan Publik (Teori Analisis, Implementasi, dan Evaluasi Kerja)*. Social Security Development Institute (SSDI).

Stevens, T., Brien, K. O., Stevens, T., & Brien, K. O. (2019). *Brexit and Cyber Security*. *1847*. https://doi.org/10.1080/03071847.2019.1643256

Syovina, M., Sari, D. K., & Sari, D. K. (2020). Pengaruh Family Business Image Promotion Soraya Bedsheet Terhadap Social Media Engagement Dengan Brand Authenticity Dan Consumer-Company Identification Sebagai Variabel Mediasi (Survey on Facebook and Instagram Users). *Jurnal Apresiasi Ekonomi*, *8*(2), 221–234. https://doi.org/10.31846/jae.v8i2.285

Yadewani, D., Lukman Arief, M., & Indah Mursalini, W. (2020). Pengaruh Pemanfaatan Platform Sosial Media Pada Era Digital Terhadap Prestasi Mahasiswa Influence of Social Media Platform Utilization in Digital Disrupsy Era on Student Achievements. *Jurnal Apresiasi Ekonomi*, *8*(3), 521–527.