www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Data and Information Security Management: Preparing Data in the Cyber Era in Indonesia

Rosyada Amiirul Hajj[1], Abdul Muta'ali[2], Benny Jozua Mamoto[3]
[1,2,3]*School of Strategic and Global Studies, Universitas Indonesia*

Abstract

One of the findings that has the greatest influence in the information society is the discovery of the internet. The Indonesian government has issued a policy related to the information security management system through Minister of Communication and Information Regulation No. 4 of 2016 which regulates the Information Security Management System. One of the negative impacts that arise in cyber-space is the occurrence of cyber crime. The rise of cyber crime requires attention and seriousness in developing cyber-security for a country including Indonesia. The theory used is using the theory of cyber crime and also physical management theory. The methodology of this research uses qualitative methods. So the results of the research are recommendations made from several written sources. So that it can be a reference for future research.

Keywords
data security; cyber era; Indonesia

I. Introduction

Currently the world is in the information age which is an advanced stage of the prehistoric era, the agrarian era, and the industrial era. One of the findings that has had the greatest impact on the information society is the invention of the internet. The Indonesian government has issued a policy related to the information security management system through the Minister of Communication and Informatics Regulation No. 4 of 2016 which regulates the Information Security Management System for electronic system operators consisting of state administration institutions, corporations, independent institutions and other legal entities engaged in the realm of public services based on the principle of risk. This regulation also stipulates that the operator of the electronic system that implements the strategic electronic system must immediately be certified to SNI ISO/IEC 27001. Likewise, the operator that implements the high level electronic system must also immediately implement the standard of SNI ISO/IEC 27001. Implementation of SNI ISO/IEC 27001: 20013, BSN has conducted a comparative study related to Information Security Management System in one of the government institutions that have been certified, namely LPSE West Java Province. BSN has also conducted a Workshop on Understanding Permenkominfo No. 4 of 2016 concerning "Information Security Management System" in internal BSN. However, as time goes by, the challenges found in the effort towards implementing SNI ISO/IEC 27001:2013 are increasing, including the competence of personnel resources owned by BSN are still limited. (http://www.bsn.go.id/main/berita/detail/8331/keamanan-informasi-dalam-era digital#.XMEuM-gzbIU/Diakses pada tanggal 27 Maret 2022.

One of the negative impacts that arise in cyber-space is the occurrence of cyber crime. The rise of cyber crime requires attention and seriousness in developing cyber-security for a country, including Indonesia. Subsequent developments practitioners call the media in telematics the term multimedia. Meanwhile, along with the use of computer

DOI: https://doi.org/10.33258/birci.v5i3.5924

system networks that use telecommunications system infrastructure, the user community then seems to find a new world called cyber space. The prefix cyber, is a prefix used for almost anything that involves communication via computers. Cyberspace is a virtual place where communication takes place. The term cyber-space was introduced by science-fiction novelist William Gibson in his book Neuromancer. At that time, in 1984 he saw that there was a kind of integration between computers and humans.4 Based on data from the Ministry of Communication and Information (Kemkominfo) internet users in Indonesia to date have reached 82 million people. With this achievement, Indonesia is ranked 8th in the world. (http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G4o5R_tfs, Diakses pada tanggal 27 Maret 2022.

Management systems to maintain data security must be very concerned, therefore the author wants to examine security management in the cyber era which everything is related to information technology. Not only the tools that must be sophisticated, but also must be supported by qualified human resources. So that the function of the technology can be used optimally to maintain important data systems that can later create a sense of security, for the government, agencies or the community in general. The role of the management system must be considered.

II. Review of Literature

Physical Management Theory

a) Management According to the definition of management, among others:
   1. Management is a series of processes that include planning, organizing, implementing, monitoring, evaluating, and controlling activities in order to empower all organizational or company resources, both human resources (human resource capital), capital (financial capital), material (land, natural) resources or raw materials), as well as technology optimally to achieve organizational goals. (Al Magassary, Ardi, 2013).
   2. Management consists of: HR structure, policies and SOPs and all kinds of resources.
   3. Good management requires a balance of stages of planning, implementation, direction and supervision step by step, by creating zero defects (zero error points), from one stage to the next. (Sabariah, Ethics, Strategic Management, 2016).

b) Management Information System (MIS) Management Information System is a planning system part of the internal control of a business which includes the use of humans, documents, technology and procedures by management accounting to solve business problems, such as product costs, services or business strategies (Hartoyo, Tri, Hasis, 2015).

c) Accounting Information System (AIS) Accounting Information System is an organizational component that collects, classifies, processes, analyzes and communicates financial information and relevant decision making for parties outside the company and external parties (Priyambodo, Esa, 2014).

d) Audit Competence Auditor competence is one of the determinants of the quality of the audit to be carried out, because when the auditor carries out his duties, competence is needed to carry out appropriate audit judgment in completing audit work which influences the final conclusion (opinion), (Ariati, 2014).

e) Audit technique is the method used to obtain audit evidence, including: confirmation, vouching, inspection, cash taking, stock taking and others. Where to do this work, the auditor must first study the SOP from the Client related to the accounting system and management system.

f) Query Understanding Query is the ability to display data from the database for further processing which is usually taken from the tables in the database. Another definition of query is a question (question) or request (order) certain information from a database that is written in a certain format. (http://hariannetral.com/2014/10/pengertian-query-dan-sql.html).

g) Online (Online/Virtual communication) The definition of communication in a network/online is a way of communicating conveyed and received information (messages), using technology. Online communication refers to reading, writing and communicating using a network, (Warschauer, M. 2001 pp. 207-212). (http://jagat-gadget.wordpress.com, 2016) h. Standard Classification of Indonesian Business Fields The Central Statistics Agency (BPS) publishes the standard classification of Indonesian business fields (KBLI), for the classification of increasingly diverse economic activities.

III. Research Method

In this study, the method used is qualitative with a case study approach. This research will focus on the level that can affect physical security in the era of information technology. So the data collection techniques in this study were documentation, audio-visual and interviews. The instruments used by researchers in this case were the main instruments and supporting instruments. The main instrument is the human himself, while the supporting instruments are library research, documentation and interviews. The main instrument in this research is the researcher himself. Researchers as instruments can understand and assess various forms of interaction in the field. According to Moleong (2011) the position of the researcher in qualitative research is that he is at the same time a planner, implementer, data collection, analysis, data interpreter, in the end he becomes a reporter for the results of his research.

The methodology used in this writing is through the study of texts and news documentation as well as articles that have been collected and read by the author, so the author makes an analysis and description. All articles and news that have been read are studied repeatedly so that a conclusion can be obtained which can be summarized back into an article which is a combination of the core explanations of the collection of articles.

Data collection methods are carried out through document collection, both written documents and electronic documents originating from articles, theses, proceedings, blogs and so on. The collected data are then compared and selected to be displayed in this paper. To validate the research data, a triangulation technique was used, namely a qualitative research technique as a reference to test whether the findings or research results reflect the existing situation and are supported by existing evidence. Triangulation in principle is a technique for checking the validity of data that utilizes something other than the data for checking purposes or as a comparison against the data (Astrini, 2017: 3).

IV. Discussion

4.1. Cyber-security and National Defense

Cyber-security is a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organizations and users' assets. Organizations and user assets in cyber-security include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of information transmitted and/or stored in cyberspace.

Cyber-security is an effort to ensure the achievement and maintenance of the security properties of organizations and users' assets against Global cyber-security is built on five areas of work: Global cyber-security is built on five areas of work: Legal Assurance (cybercrime law); technical and procedural actions (end users and business (direct approach and service providers and software companies); organizational structure (organizational structure is highly developed, avoiding overlaps); capacity building and User education (public campaigns and open communication of the latest cybercrime threats); International cooperation (including mutual cooperation in efforts to overcome cyber threats) (cybercrime law); technical and procedural actions (end users and business (direct approach and service providers and software companies); organizational structure (organizational structure) highly developed, avoiding overlaps); capacity building and user education (public campaigns and open communication from the threat of cybercrime.

Meanwhile, according to ISO 27001 and the NIST Cybersecurity Framework, there are five key components in the cyber risk management framework, which are as follows.

1. Protect valuable data

Organizations should identify which information is the most valuable and includes confidential company data, including where it is stored and who has the right to access it.

2. Monitor for cyber risk

Monitoring this risk is not only by being reactive to the occurrence of leaks, but also being proactive to other possibilities that sometimes develop faster than internal systems. The approach that can be taken is to develop an intelligence system that can immediately provide a risk signal before it actually occurs.

3. Understand your cyber perimeter

The nature of the network, especially the internet, which is so extensive requires companies to know the extent of security that needs to be maintained. Not only in the office building area, but also in areas where stakeholders have access to the company's internal network. Of course, an adequate IT system and employee discipline are the pillars supporting the success of cyber risk management.

4. Improve cyber intelligence

Referring to point 2, companies do need to develop an intelligence system related to cyber risk. Its function is to address the gap between the systems owned by the company, be it the financial system, human resources, and others. With cyber intelligence, companies can also analyze in more depth about other possibilities that can be detrimental. Research and developments around cyber intelligence are also relevant to be continuously enriched.

5. Report and Take action.

It takes a solid team to build effective cyber security, namely all parties who have the knowledge, expertise, and strong influence who can ensure the cyber risk management control system runs in an optimal corridor. So that the management can immediately make quick and appropriate decisions on accurate reports.

The five key components in the cyber risk management framework above can be a reference for companies in maintaining the resilience of organizational resources. Apart from being a form of defense, cyber risk management can actually be an offensive move.

Imagine, if our company has the resilience and readiness to any risk, especially cyber risk, the organization's actions will be effective and more efficient. This will also smooth out our company's steps in mastering the "game" of Besides, this could be a selling point to our clients. The company's risk management advantages will be a competitive advantage, so that clients or prospective clients have more confidence in products and services. (https://ppm-manajemen.ac.id/id_ID/blog/artikel-manajemen18/post/ancaman-cyber-risk-1317/Diakses pada tanggal 10 April 2022.

Global cyber-security has five areas of work: Global cyber-security is built on five areas of work: Legal Assurance (cyber-crime law); technical and procedural actions (end users and business (direct approach and service providers and software companies); organizational structure (organizational structure is highly developed, avoiding overlaps); capacity building and User education (public campaigns and open communication of cyber-crime threats latest); International Cooperation (including mutual cooperation in efforts to overcome cyber threats) (cyber-crime law); technical and procedural actions (end users and business (direct approach and service providers and software companies); organizational structure (organizational structure is highly developed, avoiding overlaps); capacity building and user education (public campaigns and open communication from the threat of cyber-crime.

Another challenge going forward in the development of cyber-security policies is the multidimensional nature of cyber threats making handling them not only the responsibility of the TNI and/or Polri. Ministry of Defense and Ministry of Communication and Information. According to Sjafrie Sjamsoeddin, cyber threats are included in asymmetric threats whose handling requires a comprehensive approach. Due to its multidimensional nature, making cyber-security is not and is not the business of only one ministry, but also the business of various other ministries. Therefore, a cyber-security or cyber-defense policy is needed which in its implementation requires a coordinating body. (Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTI), 2011).

The regulation and arrangement of a strong national cyber-security institution is one of the prerequisites for the realization of a reliable cyber-security. Therefore, the formation of institutional arrangements and arrangements that handle cyber-security nationally must be integrated as described in the following chart:

From the organizational chart and institutional management of cyber-security nationally, it can be seen that cyber-security management must be strongly integrated and involve various related institutions, namely intelligence, law enforcement, defense and security, both the Ministry of Defense and the TNI as well as the government as a regulator which in terms of This is represented by Kominfo and ISSIRTI as well as the National Crypto Agency.

Related to the organization of cyber-security handling. One of the interesting strategies that should be observed in dealing with cyber wars is the serious efforts of the United States government in developing The National Cyber Security Division (NCSD) or a special division tasked with handling cyber security nationally, supported by the private sector and the public who have the task of building and maintain an effective national cyber security system or cyberspace, create and implement risk management programs for the cyber world to protect telecommunications and cyber infrastructure from critical situations known as the National Cyber space Response System. The establishment of a special cyber unit command by the Ministry of Defense led by General Keith Alexander in

2009 is a strategic step that needs to be implemented immediately in an effort to take the defense framework more seriously and maintain sovereignty in the cyber field.

This condition is caused by seriousness in addressing cyber-security requires very large incentives, because not only because the scope of handling cyber-security is complex, but also serious cyber-security handling requires the development of supporting infrastructure that requires no small amount of financing and requires resources. balanced with the complexity of the supporting infrastructure to be built. The next step in cyber-security is technically improvements to computing-connected devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of information sent and/or stored in the cyber world.

The development of cyber security is integrated, information technology is built based on a system designed to support work, management where cyber-security is built. In addition Second, the development of information systems. Third, external resources information systems. Fourth, management of information resources.

Various concepts and steps related to improving the organization and handling of institutions that deal with cyber-security are carried out in order to ensure the achievement and maintenance of the security nature of the organization and user assets both at institutional and national levels against relevant security risks in the cyber environment, (hardware) development of information technology facilities and infrastructure, content management (content management), telecommunication and networking, internet development and online trading or via the internet.

Given the rapid development of technology, the management of cyber security resources must be placed as a business management process. This is necessary because cyber-security handling is not something that is cheap and has developed very rapidly. Infrastructure capacity development by placing it as a business management process can reduce potential losses or costs due to technological developments. Likewise with the capacity development of human resources engaged in cyber-security. By managing cyber-security HR with business management, it is hoped that it will be able to accelerate the fulfillment of the needs of human resources who master the field of cyber-security.

One surprising fact came from internet monitoring company Akamai which revealed that internet crime in Indonesia has doubled. This figure puts Indonesia in the first position as a potential target for hackers, replacing China. Of the 175 countries investigated, Indonesia contributed 38 percent of the total target of hacking traffic on the internet. This figure increases along with the increase in internet speed in Indonesia. According to David Belson of Akamai Research, internet speed has no relationship with the huge potential for internet crime that threatens Indonesia. The hacking action is due to the weak internet and computer security system in Indonesia. http://m.news.viva.co.id/news/read/507480-saat-hacker-more-menakukan-teroris-terrorist, accessed on Thursday, July 5, 2022 at 11.55 WIB.

This condition is caused by seriousness in addressing cyber-security requires very large incentives, because not only because the scope of handling cyber-security is complex, but also serious cyber-security handling requires the development of supporting infrastructure that requires no small amount of financing and requires resources. balanced with the complexity of the supporting infrastructure to be built.The next step in cyber-security is technically improvements to computing-connected devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of information sent and/or stored in the cyber world.

V. Conclusion

The legal framework for cyber-security in Indonesia is currently built, among others, based on the Information and Electronic Transaction Law no. 11 of 2008, Government Regulation on the Implementation of Electronic Systems and Transactions no. 82 of 2012 as well as ministerial circulars and ministerial regulations. Nationally, there are a number of problems related to the development of strong cyber-security, including the weak understanding of state administrators on security related to the cyber world which requires restrictions on the use of services whose servers are located abroad and the use of secured systems is required; there is no adequate legality for handling attacks in the cyber world.

Information security management in this cyber era must be carried out by means of well-established management systems and procedures, and inevitably the role of technology is very important. Currently, cybercrimes have occurred, both in Indonesia and abroad. So there needs to be a really serious management. This is of course only one of many strategies. This research also still needs improvements and developments to improve for the advancement of research in related fields.

References

Ariati, "Pengaruh Kompetensi Auditor Terhadap kualitas audit denganKecerdasan spiritual sebagai Variabel Moderating" Melaluihttps://eprints.undip.ac.id/43417/1/06_ARIATI.pdf, 2014.

Creswell, John W. (2002). Research Design Qualitative and Quantitatif Approaches (Pendekatan Kualitatif dan Kuantitatif). Jakarta : Pustaka Pelajar.

Hartoyo, Tri, Hazis, "Pengertian dan Manfaat Sistem Informasi Manajemen (SIM)" Melalui: https://hazistrihartoyo.wordpress.Com/2015/10/15/penertian-dan-Manfaat-sistem-informasimanajemen-sim/.

Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta, http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indone sia+Capai+82+Juta/0/berita_satker#.U9G4o5R_tfs/ Diakses pada tanggal 27 Maret 2022.

https://ppm-manajemen.ac.id/id_ID/blog/artikel-manajemen-18/post/ancaman-cyber-risk-1317/. Diakses pada tanggal 10 April 2022.

http://www.bsn.go.id/main/berita/detail/8331/keamanan-informasi-dalam-era-digital#.XMEuM-gzbIU/ Diakses pada tanggal 27 Maret 2022

http://m.news.viva.co.id/news/read/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris, diakses Kamis, 5 Juli 2022 pukul 11.55 WIB.

Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI) di Universitas Pertahanan di tahun 2011.