Jurnal Teknik Komputer AMIK BSI
Volume 7, No.1, Januari 2021
P-ISSN 2442-2436, E-ISSN: 2550-0120
Akreditasi Ristekdikti, No: 36/E/KPT/2019 (Sinta 4)
DOI: 10.31294/jtk.v4i2

Maintaining The Continuity of The Company's Operation using the NIST Framework for SME

Eko Haryadi[1*], Dewi Yuliandari[2], Abdussomad[3], Diah Wijayanti[4], Mike Amelia[5], Syafrianto[6]

[1,2,3,4,5,] Sistem Informasi, Universitas Bina Sarana Informatika
[1]e-mail: eko.ehy@bsi.ac.id
[2]e-mail: dewi.dwy@bsi.ac.id
[3]e-mail: abdussomad.bdu@bsi.ac.id
[4]e-mail: diah.dhw@bsi.ac.id
[5]e-mail: mike.mke@bsi.ac.id

[6] Sistem Informasi, STMIK Nusa Mandiri
e-mail: syafrianto.yfr@nusamandiri.ac.id

Diterima	Direvisi	Disetujui
29-11-2020	20-12-2020	25-01-2021

Abstrak - Perusahaan kecil dan menengah yang mulai berkembang pesat harus mulai berpikir untuk melindungi semua aset sistem informasi untuk kelangsungan hidup di industri 4.0. Menjaga kelangsungan operasi perusahaan merupakan masalah. Serangan cyber tidak hanya menyerang perusahaan besar tetapi juga secara acak mengancam level perusahaan lain. Identifikasi ancaman dan serangan cyber merupakan masalah utama. Perusahaan tidak memahami dengan baik celah dalam risiko keamanan jaringan komputer. Banyak risiko yang akan dihadapi dari segi ekonomi, operasional, dan teknologi yang harus diperhitungkan. Tujuan dari penelitian ini adalah agar perusahaan memiliki kemampuan untuk memahami posisi keamanan teknologi informasi dan sistem informasi. Akibatnya, perusahaan masih perlu menyesuaikan objeknya dari risiko tinggi menjadi risiko rendah. Salah satu panduan Manajemen Risiko yang dapat digunakan untuk meningkatkan sistem teknologi informasi kritis adalah standar dari NIST. Penelitian ini menggunakan wawancara dengan karyawan perusahaan sehingga dapat memberikan solusi untuk memperbaiki sistem informasi agar dapat bertahan dalam persaingan bisnis
Kata Kunci: NIST, Cybersecurity, Jaringan komputer, Manajemen Risiko

Abstract *- Small and medium-sized companies that are starting to grow rapidly should start thinking of protecting all information system assets for survival in industry 4.0. Maintaining the continuity of the company's operations is a problem. Cyber-attacks are not only attacking large companies but also randomly threaten other companies' level. The identification of threats and cyber-attacks is a major problem. The company does not properly understand the gaps in computer network security risks. Many risks will be faced in terms of economic, operational, and technological aspects that must be taken into account. The purpose of this research is to make the company have the ability to understand the security position of information technology and information systems. As a result, the company still needs to adjust its object from the high risk to low risk. One of the Risk Management guides that can be used to improve critical information technology systems is the standard from NIST. This study using interviews with company employees so that it could provide a solution to improve information systems to survive in business competition*

Keywords: NIST, Cybersecurity.Computer network. Risk management.

INTRODUCTION

In the industry 4.0 era, many new companies began to emerge, both on a small and a medium scale. To remain in a stable and sustainable condition, every company must be able to adapt to the rapid development of information technology. While issues relating to cybersecurity have been on the security policy agenda for decades, cyberspace has recently moved to the top of national and international security agendas. (Friis & Reichborn-Kjennerud, 2016). Specifically, technological aspects of cyberspace such as computer technology, access to information and systems, greater connectivity between subsystems, and the combined effect of all of these aspects on the list of diverse fields that are developing expose the world to unprecedented risks. (Harel et al., 2017). Cyber-

attacks have raised hopes for the board of directors to mobilize greater risk and compliance oversight and for executives to develop and implement managerial strategies for the risk management process to combat cyberattacks business sustainability (Bozhikov, 2013). Based on the report in 2019, while malicious breaches are most common, inadvertent breaches from human error and system glitches are still the root cause for nearly half (49 percent) of the data breaches studied in the report. Human error as a root cause of a breach includes "inadvertent insiders" who may be compromised by phishing attacks or have their devices infected or lost or stolen. (IBM, 2019)

PT WLCI has computer network security issues such as the occurrence of important company data leaks, inadequate data backup, and recovery systems, lack of updated network infrastructure, and lack of supervision and good management from top-level related to information system issues. In December 2019 there had been an attack in the form of ransomware, As a result of the ransomware, personal data belonging to its current and former employees was encrypted by the attacker. A ransom payment was demanded in exchange for the decryption key. To solve the problem, it is necessary to use a framework that can provide the best solution for improving computer security systems. Some similar research has been done published using the same method and this publication will show some detailed control recommendation with real support using up to date technology for better improvement. The framework used is the NIST framework. The reason for choosing NIST framework is Superior and unbiased cybersecurity, Enable long-term cybersecurity and risk management, Ripple effects across supply chains and vendor lists, Bridge the gap between technical and business side stakeholders, Flexibility and adaptability of the Framework and Built for future regulation and compliance requirements. (Bresnahan, 2019).

RESEARCH METHOD

Risk is defined as the potential for an unwanted outcome. This potential is often measured and used to compare different future situations (Steer, 2010).

Threat is the natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operation, the environment and or property (Ishtiaq, 2019).There are three primary vulnerabilities or weaknesses in network security: Technology weaknesses, Configuration weaknesses, and Security policy weaknesses (Alabady, 2008). The National Institute of Standards and Technology (NIST) Cybersecurity Framework has established a framework that can be used to improve critical infrastructure in cybersecurity (NIST, 2014). Which discusses the improvement of information systems security and control systems industry. This study describes the adaptation and improvement of the methodology for aligning proposals for information security management that is appropriate for strategic objectives. Research conducted by (Nugraha, 2016), this study discusses the application of risk management in information systems using the SP 800-30 Framework. The purpose of this study is to analyze data and information security in implementing information systems. By analyzing risk management, the results are expected to reduce the risk of data and information theft that has the potential to be misused. Risk management is an activity that involves every aspect of the organization. NIST said that risk management can be applied at three levels in the organization, as well as risk assessment activities, namely Level 1 (organizational level), Level 2 (business process level), and Level 3 (information system level). This level of the hierarchy will show the perspective of risk from the strategic to the technical side (NIST, 2012). To protect corporate data from irresponsible parties both inside and outside the company, and also all infrastructure assets that support the company's operational sustainability, it is necessary to researcher to understand the current situation and what the company needs to have, so to achieve these objectives, a research methodology is needed to lead to the research objectives. In this study, researchers conducted direct observations on an object, and researchers also conducted interviews with some employees who understood our research theme, in addition to that researchers also conducted a library method including collecting reference data related to the research theme from various scientific journals and e-book. The NIST SP800-30 has nine steps to conduct the risk analysis are system characterization, threat identification, vulnerability identification, control analysis, trend analysis, impact analysis, risk determination, control recommendations, and documentation (NIST, 2012). Further, the research will use the NIST SP 800-30 as a method that will be used to solve the problems.

RESULT

The research was conducted at one of the companies engaged in the industrial pipeline, the research area used as an object is finance and production departments. Research is a focus on assessment in the area of the production system and finances. Inputs used include software, hardware, data, and people. To understand the implementation process by using the NIST SP 800-30 Framework (NIST, 2012), the researcher described the risk assessment methodology with all the input is mentioned in the Research Method section.

4.1. System Characterization.

The researcher focuses more on the information system resources and support systems owned by this company as a basis for risk assessment. For Hardware using Personal Computer, Small Backup storage, switches, router, and Uninterruptible power supply (UPS). The software they use to support their daily activities is Win 10, MS. Office application, Computer-aided Design, Accurate Finance software, and tax system. Data set in the storage system includes work data, tax data, and e-mail. Human involvement consists of a cross-department, i.e finance staff, human resources, and production management

4.2. Threat Identification

The process of examines IT vulnerabilities and determines their capacity to compromise the system. The researcher found several things that could make a threat to the security of the information system. The use of hardware systems on PC devices with non-standard specifications that allow delays in processing a report, The use of UPS that does not nd the requirements in the office system, so that if there is a power failure the user will not have time to do backup data and no calibration process or regular checking for battery UPS and Adequate server systems are not found with appropriate cooling devices, smoke detectors, and system-controlled room temperatures. Threats to the software system occurred as they do not have a centralized data backup system, where every user data will be stored automatically in the server, using anti-virus on each client PC, password management is not good that should be set on the server-side of the client. The Employee does not understand the importance of network security because the training or socialization awareness about network security is not conducted regularly

4.3. Vulnerability Identification

All outputs in an earlier process become an important part of this process. The threat source from hardware we can see some explanation, Improver personal computer or notebook hardware becomes the main problem during data processing, calculating and analyzing the report, especially for the employee who works in the finance department. Normally a company must use UPS that can survive supplying power for at least 30 minutes if it is less than that there will be a lot of risks that must be borne. The existence of firewalls is a very important component of maintaining a computer network security system, if not done then the enterprise data will be vulnerable and the data security system will be compromised. Standard server rooms must be met and meet all the requirements. The presence of smoke detectors and air conditioning systems are inevitable. Data Loss, inaccurate archives, loss of business is the impact of an unsuitable standard backup data system. Data stolen, User privacy is not maintained, data is protected by intruders, time delay, and loss of opportunities, are some examples of improper password management and Anti-virus for client and server are not well taken care of. Due to not understanding how important company data and SOPs are not properly managed it will result in arbitrary use of computer devices, vulnerable to hacker attacks, malware violation code of conduct, and abuse of power at the end

4.4. Control Analysis

The goal of this step is to analyze the controls that have been implemented or were planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability (NIST, 2012). Control analysis in risk assessment has not well documented, risk recognition only limited to knowledge and only understood by certain parties. There is no preparation for risk analysis, process, IT equipment submission, and survey results. A clearer and more specification division of labor are needed. Control analysis that can be used by all standards and procedures that govern all aspects of infrastructure systems and information systems, the use of company assets and control of management, and work responsibilities

4.5. Likelihood Determination.

Possible risks can be obtained from the control analysis. Determination of this possibility to determine the level of likelihood that will occur against the risks that have been identified. High Risk is the current system continues to operate, but corrective action must be taken immediately, the Medium risk is Corrective action is carried out according to the planned period. Low risk is Corrective action still needs to be done or the risk can still be tolerated or accepted (Susilo, 2017). Based on the analysis controls on the previous stage, the potential threats that can be exploited as a source of risk are limits on work responsibilities, system security, the authority of access rights, and operational procedures

4.6. Impact Analysis

The next major step in measuring the level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. The impact rating is divided into two categories

a. Medium Impact Rating. As for the risks included in this category are improver PC hardware specification which results in process data especially for calculating and analyzing reports will be slow, data processing is stuck

especially when doing multi-processing. No Standard UPS for Power backup which results in generally there will be data loss, lost time for recovery and lost business opportunities, and system-controlled room temperatures will affect unstable room temperature will result in the shorter hardware life span

b. High Impact Rating. As for the risk included in these categories are Firewall system does not exist will affect The possibility of user data will be easily hacked and the system will be disrupted security, Adequate server systems are not found with the appropriate cooling device will affect to the important and confidential IT assets will be easy identified, making it highly vulnerable to internal intruders and Smoke detectors will affect to the threat of an unexpected disaster cannot be anticipated earlier.

4.7. Risk Determination

This section is a risk determination that aims to assess the level of risk to the company system, refer to table 1, it can assess the level of risk that refers to the possibility of risks and risks that have been determined based on risk assessment standards with 3 level of risk, High (H), Medium (M) and Low (L).

Table 1. Risk Determination

Risk (N.A or non standard)	Threat Likeli hood	Table Impact	Risk Value	Risk Level
UPS	0.5	50	25	Medium
Firewall system	1	50	100	High
Adequate server	1	100	100	High
Smoke Detector	1	100	100	High
System-controlled room temp	0.5	100	25	Medium
Backup data	0.5	50	25	Medium
Password Management	0.5	50	25	Medium
Anti Virus Client and Server	0.5	50	25	Medium
Data Security	0.5	50	25	Medium
Standard Operating Procedure	0.1	50	5	Low

4.8. Control Recommendation

The author will give recommendations from three items that caused a high impact. The company is suggested to use a firewall such as Check Point Firewall Security Solution, each firewall rule allows or prohibits a certain defined communication. The use of multiple server rooms by adopting the concept of network links connecting two different switches in di different IT rooms. Connecting the host to a remote switch will require a minimum of two fiber ports per host. Highly sensitive re detectors can detect even the lowest smoke concentrations, which may be caused by a malfunction of an electric or electronic element. Do some immediate actions by replacing some computer using standard hardware. The UPS must be able to be a backup power source if there are electric problems. The temperature control system and system alerts are usually integrated with the UPS server system.

4.9. Result Documentation

Result Documentation is the final stage that the authors convey. Based on the explanation above, finally, the conclusion and final report are de ned in this section, as shown in table 2. Every step on Risk Assessment fulfilled by the required output. Management can see the risk determination is a high priority for improvement.

Table 2. NIST Risk Assessment Result (Summary)

Input	Assessment Activities	Output
H/W,S/W, System Data	System Characterization	PC,UPS,Router, Etc.
PC, UPS, Router.	Threat Identification	Slow respond on Processing,etc
Slow respond on Processing	Vulnerability Identification	Loss Of Business
Plan Of Control	Control Analysis	SOP, Procedure
SOP, Procedure	Likelihood Identification.	SOP, Job description
Hardware, UPS	Impact Analysis	Slow respond on Processing.
Hardware, UPS	Risk Determination	Result Of risk analysis: H,M.L
|	Control Documentation	Stated on sec. 4.8
|	Result Documentation	Documents

CONCLUSION.

As a conclusion of this research, the company still needs to improve its system to survive in the business area by updating the information technology system. On Risk Determination Section still found some area in High position, it means the improvement is still needed with priority and became full attention from management. This study only discusses the stages of risk analysis, and for subsequent study research risk mitigation and risk, evaluation can be developed.

REFERENCE

Alabady, S. A. J. (2008). Design and implementation of a network security model using static VLAN and AAA server. In *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA*. https://doi.org/10.1109/ICTTA.2008.4530276

Bresnahan, 2019 What Are the Bene ts of the NIST Cybersecurity Framework. From https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework

Bozhikov, A. (2013). Cyber Security Risk – An Important Business Continuity Planning Issue for Business Organisations. *3rd International Conference On The Application Of Information And Communication Technology And Statistics In Economics And Education*, (Dec), 1–5.

Framework for improving critical infrastructure cybersecurity: Version 1.0. (2014). *Cybersecurity: Executive Order 13636 and the Critical Infrastructure Framework*, 55–98.

Friis, K., & Ringsmose, J. (2016). *Conflict in cyber space: Theoretical, strategic and legal perspectives*. *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (pp. 1–204). Taylor and Francis Inc. https://doi.org/10.4324/9781315669878

Harel, Y., Gal, I. B., & Elovici, Y. (2017). Cyber security and the role of intelligent systems in addressing its challenges. *ACM Transactions on Intelligent Systems and Technology*, *8*(4). https://doi.org/10.1145/3057729

IBM: Cost of a Data Breach Report 2019. (2019). *Computer Fraud & Security*, *2019*(8), 4. https://doi.org/10.1016/s1361-3723(19)30081-8

Ishtiaq, M. (2019). Book Review Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.). Thousand Oaks, CA: Sage. *English Language Teaching*, *12*(5), 40. https://doi.org/10.5539/elt.v12n5p40

NIST, 2012 NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments NIST Spec. Publ. September p. 95.

Nugraha, U. (2016). Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist Sp 800-300. *Seminar Nasional Telekomunikasi Dan Informatika (SELISIK 2016)*, (Selisik), 121–126.

Steer R, 2010 DHS Risk Lexicon 2010 Edition September.

Susilo. (2017). Analisa Tingkat Resiko Tata Kelola Teknologi Informasi Perguruan Tinggi Menggunakan Model Framework National Institute of Standards & Technology (NIST) Special Publication 800-30 dan IT General Control Questionnaire (ITGCQ). *Journal Industrial Servicess*, *Vol. 3c No*(1), 240–248.