TELKOMNIKA, Vol.17, No.2, April 2019, pp.753~762
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i2.10165

Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang

Astari Retnowardhani*[1], Raziv Herman Diputra[2],Yaya Sudarya Triana[3]
[1,2]Information Systems Management Department, Bina Nusantara University, Jakarta, Indonesia
[3]Faculty of Computer Science, Universitas Mercu Buana, Indonesia
*Corresponding author, e-mail: aretnowardhani@binus.edu[1], raziv.diputra@binus.ac.id[2], yaya.sudarya@mercubuana.ac.id[3].

Abstract

Nowadays information system has become popular used for help effectiveness and efficiency operation on a company. Bring Your Own Device (BYOD) system is a growing trend in corporate environment, where employees could access the system from anywhere. BYOD system is system information development using some technology like a Virtual Private Networks (VPN) or using some application to make the client on outside network office can access to inside networks with remote system. The remote system has strength to help employees working anywhere and anytime, that could make some issue for a security thing. The security issue that can be happen is unauthorized access and lost some important of company information. XYZ company as a manufacturing company in Tangerang, Indonesia has been used BYOD system in their company. They want to improve the security of the system with do risk analysis, with the aim to protect the internal data. The risk analysis use Cybersecurity Framework NIST will assist organizations to understand the risk of BYOD system. The analysist results obtained by the use of cybersecurity analysis on BYOD system in XYZ company are found some improvement need to develop in terms of security system recommended. According to the stages of respond with the analysis using Cybersecurity NIST framework and ISO/IEC 27002:2013.

Keywords: *BYOD, cybersecurity, efficiency, security*

1. Introduction

Technology and information systems today has become one of the things needed in everyday life. According to a survey conducted by the Association of Internet Network Providers Indonesia (APJII) revealed that more than half of Indonesia's population has now been connected to the internet. The survey, conducted throughout 2016, found that 132.7 million Indonesians were connected to the internet. As for the total population of Indonesia itself as much as 256.2 million people. It is indicates a 51.8 percent increase compared to the number of internet users in 2014 and according to a survey conducted APJII in 2014 there are only 88 million Internet users [1].

If we are looking from the development of internet usage in Indonesia can be taken conclusion which means the development of smartphone sales in Indonesia as the marketing research institute E-marketer smartphone users Indonesia is also growing rapidly. Research institute digital marketing E-marketer estimates that in 2018 the number of active users of smartphones in Indonesia more than 100 million people. With that amount, Indonesia will be the country with the fourth largest smartphone active users in the world after China, India, and America [2]. Indonesia is "the sleeping Asian digital technology giant". Indonesia's population of 250 million is a big market.

Related to the development of technology and internet usage will certainly be an added value for a company. Based on a survey conducted syntonic.com to the company in 2016 as many as 87% of companies believe that giving access to mobile business applications of companies from each smartphone employee, the company's estimate of employees can increase productivity work 6.7 hours per week [3]. Viewed from the side of the company of course this becomes a value more with the existence of a system that can make the workers do not need to come to the office to access the company system. This trend is called "Bring Your Own Devices" where BYOD is a growing trend and can provide benefits such as from a flexible

Received June 2, 2018; Revised October 24, 2018; Accepted November 20, 2018

side of work, increasing productivity and efficiency of employees [4]. BYOD is where a company allows employees to use their personal devices for access into corporate networks [5, 6]. By using a remote system the employees only need to have a mobile device and internet, then use the remote system to be able to access the office system from everywhere [7]. But it turns out that in addition to providing benefits from the implementation of BYOD systems in a company, BYOD also need to be considered for its use related to the security of information and data available on the company. Based on the explanation by [4], where there is a risk to the implementation of the BYOD system is the existence of loopholes for loss of data from the side of important information company or the possibility of data taken by unauthorized parties. XYZ company as a manufacturing company in Tangerang, Indonesia has been used BYOD system in their company. XYZ company has used Virtual Private Network (VPN) to monitor the use of system. They want to improve the security of the system with risk analysis, with the aim to protect the internal data.

Cybersecurity framework National Institute of Standards and Technology (NIST) is an easy-to-apply framework because it's easier to discuss technical or non-technical. By using the NIST stakeholder cybersecurity framework, partners and suppliers will be easier to discuss to achieve the intended goal [8]. Based on the survey conducted by tenable, 84% of organizations in various countries have implemented several types of security framework, one of them is NIST cybersecurity framework [9]. NIST's Cybersecurity framework is one of the framework options for assessing information systems security, analyzing risks that will occur in information systems and can build effective strategies to tighten the security of the current system. Gartner has an expectation that the upgrading of the implementation of the NIST cybersecurity framework will reach 50% by 2020 [10].

Based on the survey, it is estimated there are 74% of companies that have or want to apply to allow employees to use their personal devices to work [11]. This means showing that the implementation of the BYOD system to work has started to become a trend and survey results by the Indonesia cloud forum show that only 44.2% of employees prefer to work in the office, the rest of them say they feel more comfortable working outside the office with the largest percentage at home (39.5%) or in places such as cafe/mall (16.3%) [12, 13] . The advantage of using the system with BYOD method from the side of the company is very clear by just using the system BYOD this company can improve the productivity of work of existing employees. While from the employees themselves get the benefit of the employees will be more mobile and flexible to work anytime and anywhere [4].

The challenge when it comes to implementing the BYOD system is whether the data accessed by employees using their personal device is secure or whether it is in accordance with authentication that should be allowed to access the server or information. But it cannot be denied that from this BYOD system there are some shortcomings of security aspect related to information or company asset. This aspect is worth noting for the implementation of this BYOD system is a matter of security and confidentiality [4, 14].

The application of BYOD system also needs to be considered in terms of data security company, based on study by security firm CPP UK found that over 50% of used mobile devices still contained large amounts of data from previous mobile devices owners and the fact is 86% survey data found that they must remove all personal data first before selling or recycling the mobile devices [5].

This paper will be presented the risk of information system security with the cybersecurity NIST framework, which is related to how the framework can perform risk analysis on the existing information system. The expectation of this analysis is to reduce the risk of data security in XYZ company. We use a case study in XYZ company as a manufacturing company in Tangerang, Indonesia which is has been used BYOD system in their company.

2. Research Method

The research methodology used in this study consists of 3 stages. First, doing analysis of existing information systems, focused on the security risks in the use of BYOD. Secondly, made a recommendation design system based on the results of the analysis in the first stage. The design made based on ISO 27002: 2013. The last stage is a recommendation system based on Gardner Quadran. Figure 1 presented the research methodology in this research. This paper disscussed stage 1 and 2.

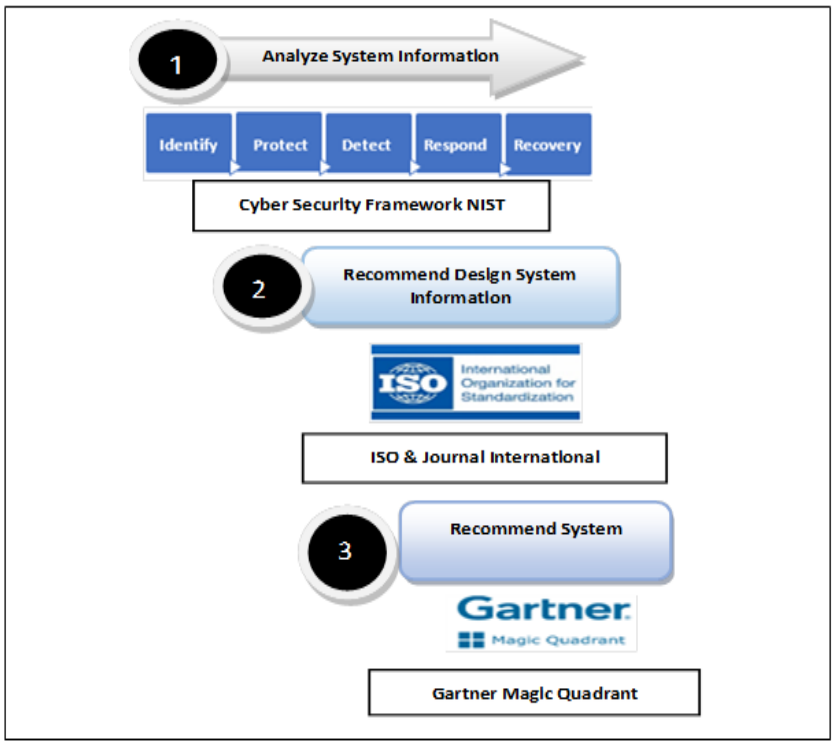

Figure 1. Research methodoly of this reseach

The way to make this BYOD trend working well is to improve security on information to make sure that the information is not leaking to the people there is not authorized to access or have that information [15]. In first stage the analysis of the system is done by use Cybersecurity NIST framework. Cybersecurity NIST framework has 3 components, they are core framework, profile framework, and implementation tier framework. This research focused on core framework. This framework is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sector [16]. The core framework comprises 4 elements: Functions, Categories, Subcategories, and Informative References. Function element organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover, depicted on Figure 2.

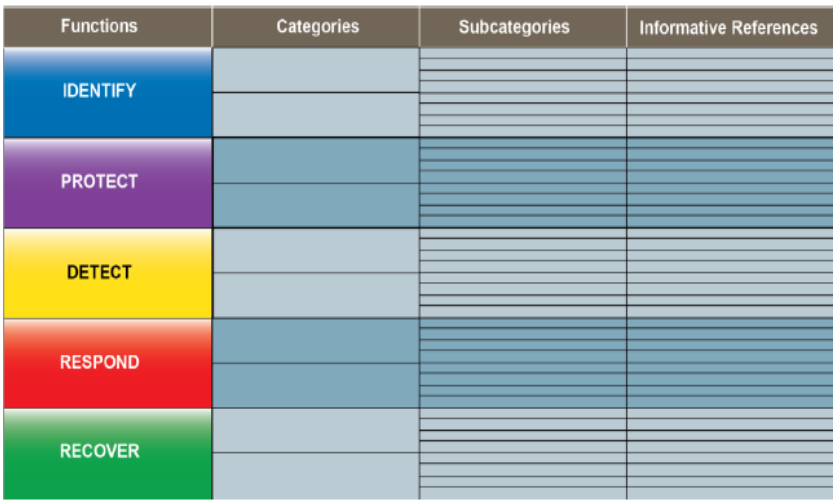

Figure 2. NIST core framework

This study use ISO/IEC 27002:2013 Information Technology at stage 2 [17]. The reason of the use this ISO because ISO/IEC 27002:2013 also introduces how to achieve technical security architecture that is of good quality, risk aspects, design and control related to network scenarios and network technology areas. This is accordance with the purpose of the study. ISO/IEC 27002:2013 has 14 security control clauses as follows: Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and environmental security, Operation security, Communication security, System acquisition,development, and maintenance, Supplier relationship, Information security incident management, Information security aspects of business continuity management, Compliance. Gartner Magic Quadrant also use in this research in stage 3. It is provide a graphic competitive position of four types of technology categories in a rapidly growing market: leader, visionary, niche player and challenger. As a side note gartner can provide a deeper insight into the recommended conformity of products and services of information systems based on specific or customized use case [18]. However, this paper focussing on stage 1 and 2.

3. Results and Analysis

XYZ company as a manufacturing company in Tangerang engaged in the production and sale of paint products. XYZ company has implemented information system for database using oracle and network security system. In head office already has network firewall as internet gateway. They uses a virtual private network (VPN) method where the IT department can remotely monitor the system from anywhere, as well as the sales and manager levels. VPN is one way to safely remotely [19]. XYZ company using the existing VPN on windows system so that employees who have access to VPN can access the existing system at office by using laptop provided by office or personal laptop. This is the focus in this study related to the existence of the system BYOD by giving permission to perform remote access system by using the VPN method of course there is an excess or risk that will occur when applying the system BYOD [20-22].

With this remote system implementation make the job more efficient because there is a reduction in working time due to having to go to the office first if you want to access data available on XYZ system. Information security has become a critical issue. Various steps have been taken to improve and develop the level of security [23, 24]. The reason of remote system implementation is because the need for control when the system needed during a sudden condition, while the person in charge is not available at the office but they need to access the system to do their work. Then, with this remote system implementation they can access the system to retrieve or input data and also seen from the needs of the sales team or some other end-user to check the database system, or inventory of paint production.

For the infrastructure itself is supported by the implementation of wireless network and authorization system for wireless network access, where only employees who can access the system when using wireless network while for guests are only allowed to access the internet when using the wireless network available at the office. In terms of wireless access is set can only be used by employees only based of SSID and password for wireless connectivity access at headquarters. The company uses a system of centralization where each system is at the head office, so for the Tangerang branch requires a connection to the headquarters in advance if you want to access the existing system. For the gateway side there is already a firewall that serves as the internet gateway headquarters, but for each branch and every segmentation zone on the system still no firewall. On the server side for the current condition is still using the manual backup server and data or information available in the PC or laptop office.

With the implementation of a remote system certainly can help and facilitate employees in performing their duties while working, but in the application of this remote system also there are risks associated with the security of corporate data. Figure 3 has shown the network topology of the system. In analysis and recommend stages is done based on interview and observation method to get the data. The interviews conducted to IT supervisor and IT manager, plan manager, IT senior, and production engineering manager. The Identify Function from NIST Core framework are listed in Table 1. The Identify Function Results listed in Table 2. The results have shown several subcategory need to check again and need to do action to solve the problem.

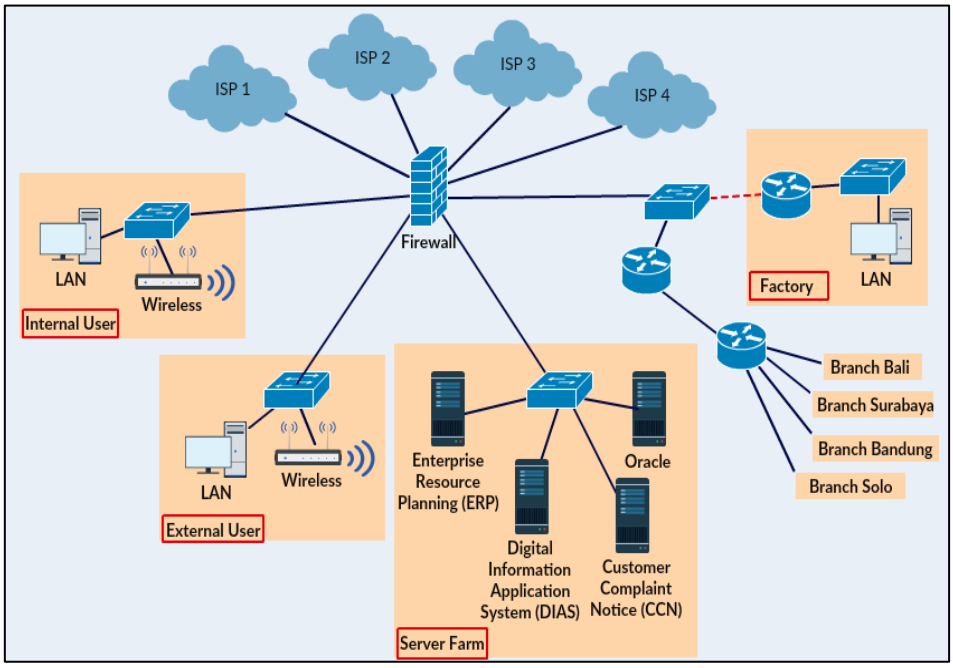

Figure 3. Network topology at XYZ Company

Table 1. Identify Function

Category	ID	Subcategory	Informative References
Asset Management	ID.1	Responsibility for assets	ISO/IEC 27002:2013 Section 8
	ID.2	Information classification	
	ID.3	Media handling	
Business Environment	ID.4	Internal organization	ISO/IEC 27002:2013 Section 6
	ID.5	Mobile devices and teleworking	
Governance	ID.6	Rules of Employment	ISO/IEC 27002:2013 Section 7
	ID.7	Backup	
Risk Assessment	ID.8	Operational procedures and responsibilities	ISO/IEC 27002:2013 Section 12
	ID.9	Protection from malware	
	ID.10	Logging and monitoring	
	ID.11	Control of operational software	
	ID.12	Information systems audit considerations	

In implementation of Protect Function XYZ company has implemented security gateway like firewall as internet access gateway can help in general to handle attacks and also maintain XYZ internal network, rules are made to handle viruses implemented in network gateway for inbound or outbound traffic as well as sandboxing method on firewall in order to know zero day malware where the virus that has a new signature and certainly cannot be maintained only with intrusion prevention system (IPS) that exist in the firewall because it still uses a signature based to guard against threats.

From the authentication side there is also a special user to do remote with VPN technology to maintain the security of communication between networks. From the side of the router also has done access control list so that only certain IP from the WAN side that can access to the existing system in the head office. In XYZ company also has been doing protection for endpoint devices by using antivirus to keep from direct threats directly attack from the endpoint devices.

Awareness of users related to information updates or updates that are trend so as to reduce the risk of threats from the side of the user's habits related to existing threats, as described in the discussion by [25] about "*policy based framework BYOD for preserving confidentiality in BYOD environments*" which explained that the data protection needs done as separation of confidential data of company with personal data. Table 3 has listed a Protect

Function Subcategory based on ISO/IEC 27002:2013. Table 4 is a summary of the steps in protecting NIST's cyber security framework in XYZ company:

Table 2. Result of Identify Function

ID	Subcategory	Result	Status
ID 1	Responsibility for assets	XYZ company has identified and registered all devices or devices in accordance with their ownership	Ok
ID 2	Information classification	XYZ company has categorized every critical server until it is not critical server	Ok
ID 3	Media handling	XYZ COMPANY has implemented control of USB	Need to check
ID 4	Internal organization	XYZ company has provided division of parts for IT as the responsibility of the system	Ok
ID 5	Mobile devices and teleworking	XYZ company has installed antivirus for every PC or laptop office, but XYZ COMPANY cannot manage centrally for mobile devices	Need to do an action
ID 6	Rules of Employment	XYZ company has applied access to every employee profile for accessing system	Ok
ID 7	Backup	XYZ company has implemented a backup system using storage craft for server but for system log still not exist	Need to do an action
ID 8	Operational procedures and responsibilities	XYZ company still uses manual processing for documentation, PT did not have a system that can automatically documented all process	Need to do an action
ID 9	Protection from malware	XYZ company only apply antivirus on the gateway side and endpoint device	Need to do an action
ID 10	Logging and monitoring	XYZ company will implement system logging using loganalyze	Ok
ID 11	Control of operational software	XYZ company has implemented controls for each system manually through the IT division	Need to do an action
ID 12	Information systems audit considerations	XYZ company has not conducted an audit system	Need to do an action

Table 3. Protect Function

Category	ID	Subcategory	Informative References
Access Control	PT.1	Business requirements of access control	ISO/IEC 27002:2013 Section 9
	PT.2	User access management	
	PT.3	User responsibilities	
	PT.4	System and application access control	
Awareness and Training	PT.5	Information security in supplier relationships	ISO/IEC 27002:2013 Section 15
	PT.6	Supplier service delivery management	
Data Security and Information Protection	PT.7	Network security management	ISO/IEC 27002:2013 Section 13
	PT.8	Information transfer	
Maintenance and Protective Technology	PT.9	Security requirements of information systems	ISO/IEC 27002:2013 Section 14
	PT.10	Security in development and support processes	

The BYOD system running on XYZ company can improve the efficiency level of work. However, this system needs to be developed the security side. The system due to access using VPN connection without enough protection such as encryption data from the system, then the data can be moved safely as recommended ISO/IEC 27002: 2013 related cryptography.

Based on ISO/IEC 27002: 2013 section 9.4 related password management required account management system. It is about user authentication to assist in standardization, such as password that must have more than 6 characters with numbers, alphabet and special characters. In addition, it is expected that this account management system can also prevent unnecessary login. In addition, account management can also set the schedule for the change

of password periodically. Table 5 has listed a Detect Function Subcategory based on ISO/IEC 27002:2013. Table 6 is an results of Detect Function in XYZ company. The results have shown all status of subcategory are need to do an action from company.

Table 4. Result of Protect Function

ID	Subcategory	Result	Status
PT.1	Business requirements of access control	XYZ company has implemented a company regulation policy in firewall and router	Ok
PT.2	User access management	XYZ company has applied user access profile	Ok
PT.3	User responsibilities	XYZ company has done periodic knowledge sharing on end user of remote system user	Ok
PT.4	System and application access control	XYZ company has implemented control based on access list, for password management still need to do with manually control	Need to do an action
PT.5	Information security in supplier relationships	XYZ company only implements open communication with branch office	Ok
PT.6	Supplier service delivery management	XYZ company only implements open communication with branch office	Ok
PT.7	Network security management	XYZ company has divided every segment network including wireless, server and branch office	Ok
PT.8	Information transfer	XYZ company only implements open communication with branch office	Ok
PT.9	Security requirements of information systems	XYZ company has applied profile and access using username and password	Ok
PT.10	Security in development and support processes	XYZ COMPANY is still implementing manually testing for development system	Need to do an action

Table 5. Detect Function

Category	ID	Subcategory	Informative References
Anomalies and Event Continuous Monitoring Detection Process	DT.1	Management of information security incidents and improvements	ISO/IEC 27002:2013 Section 16

Based on ISO/IEC 27002: 2013, access control is one of the important things in doing security practitioners to make the running system more secure. The solution required for XYZ company is an integrated solution and can provide event related information that occurs on XYZ company system. In ISO/IEC 27002: 2013, information technology is related to network security management guidance in terms of monitoring, logging and as well as detection of existing systems, as well as security information and event management solutions which can provide information related to devices and traffic that are experiencing or have the possibility of system down, then the backup system must be prepared at the time the incident did occur.

Based on ISO/IEC 27002: 2013 in section 18 need an audit system and also testing on each segmentasinya to know the conditions that have been implemented whether it is in accordance with standard or compliance of existing information systems in XYZ company. Implementation of the BYOD system in XYZ company also needs to be documented on every security event that occurs, it is required in accordance with ISO/IEC 27002:2013 section 16 standards related to information security incident management in order to respond to a cybersecurity event that occurs and can perform analysis to perform system recovery if needed.

Table 6. Result of Detect Function

ID	Subcategory	Result	Status
DT.1	Management of information security incidents and improvements	XYZ company needs to do awareness to users related to office device that can be lost (with confidential data company)	Detection ID.5, Need to do an action
DT.2		XYZ company needs to do awareness and monitoring to users change password periodically with the high complexity of password	Detection PT.4, Need to do an action
DT.3		XYZ company needs to keep and analyze every log of the existing system	Detection ID.7, Need to do an action
DT.4	Management of information security incidents and improvements	XYZ company needs to do awareness about regularity of sharing password to another, XYZ company need to enhance with two-factor authentication	Detection PT.9, Need to do an action
DT.5		XYZ company needs to do a periodic system testing	Detection ID.12, Need to do an action
DT.6		XYZ company still documented all process manually after changes configuration	Detection ID.8, Need to do an action

The IT department needs to do awareness to the management regarding the information system at XYZ company and the possible risks that will occur if the system is still running without any improvement from the current system. This should be applied as a continuation of XYZ company business as recommended in ISO/IEC 27002: 2013 section 17. Also be re-generated new standard with new system security implementation in accordance with ISO/IEC 27002: 2013 standard in section 5.

In addition, based on interviews related to log-analyzer implementation, it is necessary to realize the standard ISO/IEC 27002: 2013 section 12.4 that is related to system user activity and administrator/operator, exceptions, correction and event log should be recorded and protected. Table 7 has listed a Respond Function Subcategory based on ISO/IEC 27002:2013. Table 8 is an implementation summary of Respond Function in XYZ company:

Table 7. Respond Function

Category	ID	Subcategory	Informative References
Response Planning	RP.1	Response Planning	ISO/IEC 27002:2013 Section 14,18
Communications	RP.2	Communications	ISO/IEC 27002:2013 Section 10, 11,17

Based on ISO/IEC 27002: 2013 section 17 related information security continuity that explains about how to plan, implement and check the system running for the interests and continuation of XYZ company business. Where necessary awareness of possible risks such as company formulation or data related price or company sales that can occur when the use of the remote system is not used with care. This can happen due to loss of laptop or smartphone used to run the remote system because of course the device stores data taken from the oracle system in the central office, and the absence of a system that provides a password or encryption of the file. At this stage in accordance with the standard ISO/IEC 27002: 2013 section 5 where the management must re-determine the policy of each system running and of course related to information or company data needs to be reviewed. If we want to continue implementation the system BYOD then there should be an adjustment of existing security systems in XYZ company. This is done for the continuation of XYZ company business, for the current system is expected to be adjusted and a more strict policy such as the written documentation related to the rules of the company to be awareness on every user who uses BYOD remote system. Table 9 has listed a Recovery Function Subcategory based on ISO/IEC 27002:2013. Table 10 is a Results of Recovery Function analysis and recommended action in XYZ company:

Table 8. Result of Respond Function

ID	Subcategory	Result	Action
RP.1	Response Planning	XYZ COMPANY needs to implement a two-factor authentication system	Response for DT.4
		XYZ COMPANY needs to implement a password management system	Response for DT.2
		XYZ COMPANY needs to upgrade more advanced endpoint security	Response for ID.9, ID.11 & DT.1
		XYZ COMPANY needs to perform testing and checking by 3rd party on the system to match the compliance	Response for PT.10 & DT.5
		XYZ COMPANY needs to implement log analyzer system	Response for ID.10 & DT.3
		XYZ COMPANY needs to implement security information and event management	Response for DT.6
RP.2	Communications	Need for communicate to the management related the respond planning	Need to do an action

Table 9. Recovery Function

Category	ID	Subcategory	Informative References
Recovery Planning	RC.1	Recovery Planning	ISO/IEC 27002:2013 Section 5
Improvement	*RC. 2*	Improvement	
Communication	*RC. 3*	Communication	

Table 10. Results of Recovery Function

ID	Subcategory	Result	Action
RC.1	Recovery Planning	Need to do documentation related to the rules about awareness users of system BYOD	Need to do an action
RC.2	Improvement	Need to improve the security system based on respond planning	Need do an action
RC.3	Communications	Need to do awareness related to cybersecurity for user who using BYOD system	need to do an action

4. Conclusion

Based on data gained from interview and observation we make an analysis about BYOD system security risk. The results obtained by the use of cybersecurity analysis on BYOD system in XYZ Company there are some points need improvement to develop in terms of security system recommended. Based on the stages of respond with the analysis using Cybersecurity NIST framework and ISO/IEC 27002:2013 then the results and actions were obtained. In Identify Function obtained 10 results.

In Protect Function also obtained 10 results. In Detect Function obtained 6 results, one of the results as like a company needs to do awareness and monitoring to users change password periodically with the high complexity of password. In Respond Function results have 7 results, such as need to upgrade and implement the security planning of the BYOD system. In Recovery Function generate 3 results, such as a XYZ company is urgent to make a rules documentation. Then, the use of Cybersecurity NIST framework is useful to determine the weaknesses of the BYOD system security in XYZ company.

References

[1] Cnn Indonesia, *www.cnnindonesia.com*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20150326134506-185-42064/2014-pengguna-internet-indonesia-capai-881-juta/

[2] Emarketer,*www.emarketer.com*. Retrieved from Emarketer: www.emarketer.com/Chart/Smartphone-Activities-of-Smartphone-*User*s-Indonesia-by-Age-July-2016-of-respondents/194074

[3] Syntonic. Employee Report: BYOD Usage in the Enterprise. *Retrieved from Syntonic: https://syntonic.com/byodresearch/.* 2016.
[4] Garba A B, Armarego J, Murray D. Bring Your Own Device Organisational Information Security and Privacy. *ARPN. Journal of Engineering and Applied Sciences*. 2015; 10(3):1279-1287.
[5] Wang Y, Wei J, Vangury K. *Bring Your Own Device Security Issues and Challenges*. IEEE 11th Consumer Communications and Networking Conference (CCNC). 2014.
[6] Bailette P, Barlette Y, Leclercq-Vandelannoitte A. Bring Your Own Device in Organizations: Extending The Reversed IT Adoption Logic To Security Paredoxes for CEOs and end users. *International Journal of Information Management.* 2018; 43: 76-84
[7] Wanda P, Jie Huang J. Efficient Data Security for Mobile Instant Messenger. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2018; 16(3): 1426-1434.
[8] Garlipp M. Benefits of The NIST Cybersecurity Framework. Retrieved from Govloop: www.govloop.com/benefits-of-the-nist-cybersecurity-framework. 2015.
[9] Tenable. Adoption Cybersecurity framework NIST. Retrieved from Tenable: https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise. 2016.
[10] Infosecurity. Simplify NIST Cybersecurity Framework Adoption. Retrieved from Info Security: https://www.infosecurity-magazine.com/opinions/simplify-nist-cybersecurity/. 2017.
[11] Zdnet, *Research: 74 percent using or adopting BYOD*, 2015, Retrieved from Zdnet: http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/
[12] Biznetgiocloud, 2017, Retrieved from Biznetgiocloud: http://www.biznetgiocloud.com/byod-tren-perusahaan-di-masa-depan/
[13] Dhingra M. Legal Issues in Secure Implementation of Bring Your Own Device. *Procedia Computer Science, International Conference on Information Security & Privacy, India.* 2016; 78:179-184
[14] Disterer G, Kleiner C. BYOD Bring Your Own Device. *Procedia Technology, International Conference on Health and Social Care Information Systems and Technologies.* 2013; 9: 43-53
[15] Matteson Scott. 10 Ways BYOD will evolve in 2016. Retrieved from Techrepublic: http://www.techrepublic.com/blog/10-things/10-ways-byod-will-evolve-in-2016/
[16] NIST. Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology,* 2014, Retrieved from cyberframework@nist.gov
[17] Zhang S, Fever HL .An Examination of the Practicability of COBIT. *Journal of Economics, Business and Management*. 2013; 1(4): 391-395.
[18] Techtarget. Gartner Magic Quadrant . 2013, Retrieved from Techtarget: http://whatis.techtarget.com/definition/Gartner-Magic-Quadrants
[19] Ahlawat S, Anand A. An Introduction to Computer Networking. *International Journal of Computer Science and Information Technology Research*, 2014: 373-377.
[20] Ghosh A, Gajar PK, Rai S. Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies. *Journal of Global Research in Computer Science.* 2013; 4(4).
[21] Network Intelligence. Mobile Device Management-Deployment, Risk Mitigation & Solutions. 2018. Retrieved from https://www.niiconsulting.com/solutions/mobile-device-management.html
[22] Hilal, H, Nangim, A. *Network Security Analysis SCADA System Automation on Industrial Process*. International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP). 2017: 1-6.
[23] Nurhaida I, Ramayanti D, Riesaputra. Digital Signature & Encryption Implementation for Increasing Authentication, Integrity, Security and Data Non-Repudiation. *International Research Journal of Computer Science (IRJCS)*. 2017; 11(4): 4-14.
[24] Jillepali AA, Conte de Leon D, Steiner S, Alves-Foss J. Analysis of Web Browser Security Configuration Options. *KSII Transactions on Internet and Information Systems.* 2018; 12(12): 6139-6160.
[25] Vorakulpipat C, Sirapaisan S, Rattanalerdnusorn E, Savangsuk V. A Policy-Based Framework for Preserving Confidentiality inBYOD Environments: A Review of Information Security Perspectives. *Security and Communication Networks.* 2017