Journal of Computing and Applied Informatics (JoCAI) Vol. 6, No. 1, 2022 | 45 – 54

DATA SCIENCE
Journal of Computing and Applied Informatics

Applied Approach Impact Information Security for Government and Companies (A Review)

T.H.F Harumy[1], Dewi Sartika Br Ginting[2], FY Manik[3], Mahyudin[4]

[1,2,3,4] Faculty Of Computer Science and Information Technology, Universitas Sumatera Utara Indonesia]

Abstract. The government and industry currently use information and communication technology a lot. The government and companies in Indonesia have regulations on procedures for managing information and communication system security. Information security is critical because there are many threats to information security. Information security in this era of information and communication technology (ICT) is fundamental. Information Exchange Environment (IEE) vulnerabilities have increased as threats become more widespread and complex. Information security has become a fundamental issue for businesses, organizations, and governments. In this paper, a review of the impact of information security on the government and companies is described in terms of threats and types of information security. Some security system methods are analyzed, including—application security, cloud security, cryptography, security infrastructure, incident response, and vulnerability management. The results of this review analysis, it is known that threats have several solutions, each depending on the type of threat for both the Government and the companies. Furthermore, information security is considered very important, especially for data stored in government and companies.

Keyword: Information, Security, Aplication Security, Government, Companies, Industry.

Received 28 December 2021 | Revised 16 March 2022 | Accepted 16 March 2022

1 Introduction

The Government and industry are currently using information and communication technology a lot; the Government and companies in Indonesia have regulations on operational standards and management procedures for information and communication system security at the Government regarding implementing information system security. Information security is essential because there are many threats to information security, including malware infection methods and malware actions. Malware based on action methods includes viruses, worms, trojans, and bots. Meanwhile, action-based malware includes spyware, scareware, rootkits, and zombies. Further information threats are identity theft, device and information theft, sabotage, information extortion, social

*Corresponding author at: Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia

E-mail address: hennyharumy@usu.ac.id

Copyright © 2022 Published by Talenta Publisher
ISSN: 2580-6769 | e-ISSN: 2580-829X | DOI: https://doi.org/10.32734/jocai.v6.i1-7935
Journal Homepage: https://jocai.usu.ac.id

media attacks, and mobile malware attacks. This paper describes a review of the implementation of information security systems and the impact on the Government and companies using several information security systems (ISS).

Today information security systems (ISS) are very important. Information exchange environment (IEE) vulnerabilities have threats have increased so varied that this issue becomes critical to analyze, especially for governments, companies, and organizations[1][2]. During this period, the current Government has not maximally carried out an audit of information system security. Many studies on information security systems are a framework for information security audits and are able to provide comprehensive information security. Currently, the types of information security include cryptography, cloud security, security applications, and others. So, in this paper will explain the impact of information security for government and companies review both in terms of threats and types of information security.

2 Research Objective

The research objective in this paper is how to analyze threats and information security in a government which in this case uses several methods of system security and analyzes the advantages and disadvantages of system security methods [3][4]. This is done as a basis for improving information security in a government. There is a form of securing information because information on Government is critical and must be secured appropriately.

3 Research Contribution

The research contribution in this paper is to analyze threats to information security and as a basis for improving information security in a government and companies. This is a form of securing informationbecause information on government is very important and must be properly secured.

4 Novelty Research

The novelty obtained in this research is to find and review the best data security method for companiesand companies. Next, analyze the best information security system, especially for data contained in thegovernment and companies so that it can be a reference for the discovery of the next latest method.

5 Literature Review

The Information Security Risk Analysis Method (ISRAM) are new technologies in information security. Information security risk analysis process is very influential on this big change. The challenge of implementing this analytical tool has an enough risky, therefore it is hoped that further researchers will develop this method further. The application of this method to information

security is one form of maintaining information security. The success and development of a business that focuses on information is highly dependent on the availability of technology and accurate information security methods [5]. One of the infrastructure security information security audit systems is COBIT 5, which is information security, processing, and application infrastructure. One of the COBIT 5 output products is COBIT 5 for information security in a company.

Additionally, one of the information security auditing systems for infrastructure security auditing is COBIT 5, which is information security, processing, and application infrastructure. One of the output products of COBIT 5 is COBIT 5 for information security. For information security, well known for checking the security of Government, business systems, and information [2][6]. The security mechanisms allow one user of the system to influence another, rather than just excluding those who are not supposed to be users, posing many strategic and political challenges.

The difficulty of measuring information security risk is a different matter. The result of this information security failure mechanism, it can lead to other market disturbances and distortions. Digital rights management (DRM) in the online music and software market is a vivid example of this mechanism. Furthermore, an important issue regarding the information security of the banking industry is the falsification of information on banking share incentives [3]. In addition, the effectiveness of information security is used to provide a positive return on investment, namely, the amount of investment to the ratio of the amount received [4][7][8]. The results of data analysis show that promotion, reputation gain, as an irrelevant motive, and satisfaction with curiosity as an intrinsic motive have a positive effect on employee attitudes towards ISCS. However, satisfaction with self-esteem does not affect attitudes towards ISKS.

Another study explained that attitudes, behavioral analysis, subjective norms, and integrated security system (UTI) intentions affect integrated security system (UTI) behavior. Prevention theory (GDT), defense motivation theory (PMT) and skills adoption models (TAM). The result, presented in general terms about these factors significantly affect employee safety behavior. The combination of the results of a validated research model, presented about the factors that have been shown to significantly influence employee safety behavior [9]. Furthermore, there are many theories used, proved to have a significant effect [9-10]. It is known that good security management must be based on the same policies and standards, so that it will make a good contribution. On specific issues that are explicitly discussed the view of information security management is very technology-centered [8].

6 Analysis Methodology

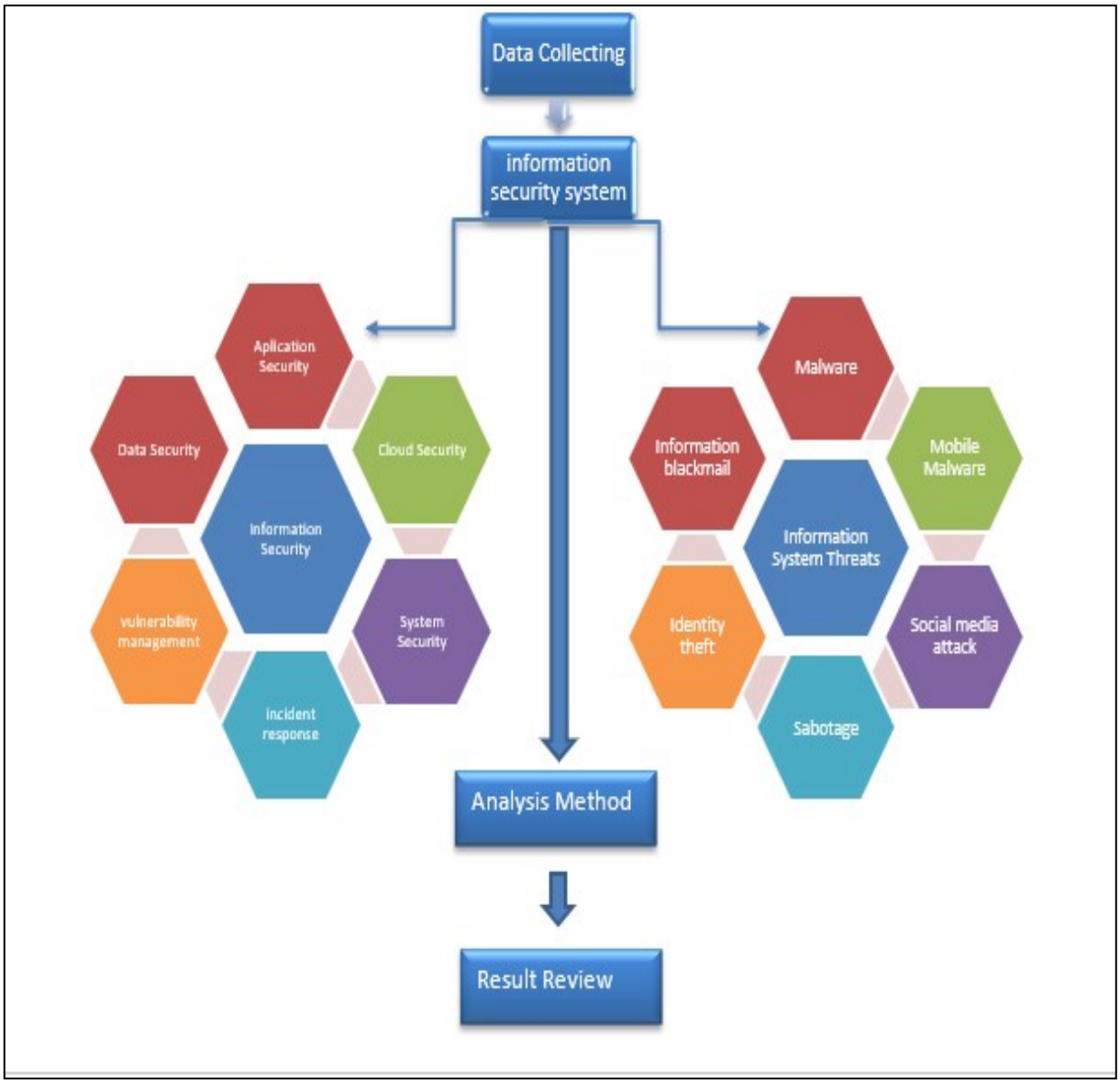

Figure 1 Analysis methodology information security

The Analysis methodology in this paper begins with collecting data regarding the information security system, including how to process information data security, system security, incident response, cloud security, Data security. Furthermore, this analysis also explains about securing data from various attacks such as sabotage, malware, blackmail information, social media attacks, identity theft, and others, where these threats often occur in companies and the Government. It is undeniable that this threat often happens because a lot of essential and confidential data is stored in companies, which triggers hackers and irresponsible people to try to retrieve that data. The next step that will be carried out in this analysis methodology is to analyze the methods offered or the solutions provided to overcome these threats through a literature review analysis that has previously been applied in various case studies in the companies and Government. Researching and analyzing the method used the next alternative in the form of an effort to produce the best

results. This research methodology draws from various kinds of literature and previous studies to analyze and review in-depth data security methods from threats that have been carried out previously and the workings of these methods.

The analysis aims to improve analysis in the field of information security, although sometimes research in this field has some difficulties. Security mechanisms and analysis failures are very likely to occur, both disruptions and other market distortions. The examples are the digital rights of songs in the music world, digital content in online media, counterfeiting incentives, and copyrights is some of the triggers for the development of research on information security [3]. These problems significantly affect the development of risk analysis in this field.

The results of the review produced in this paper are that there are several methods that can be applied for data security and solutions to overcome threats that occur in the companies or companies, such as for cloud data security, data security, information system security and applications. One of the data security applications such as RESIN. The application has a comprehensive security framework for application authentication, authorization and transport-level SSL based security. The application can protect against various vulnerabilities in Python and PHP applications. The RESIN prototype incurs 33% CPU overhead.

Further application security with secure access layer provides. In addition, for cloud data security, several solutions could be used namely, an information risk management framework, and cloud providers can apply this framework to organizations to mitigate risks. The system can be concluded that data and system security can be done by various available methods.

7 Result Review

Table 1 Solution Information Security System and Methods

Government/Companies		Solution	Advantages	Disadvantage	Impact Security to Government/Companies
Threat	**Information Security System**	**Reference Approach**			
Malware	Application Security	Application Security with Data Flow Assertions.[11]. A security system application that has an interface in the form of secure Access layers.[12]	Using RESIN, Web application programmers can prevent a range of problems from SQL injection and cross-site scripting to inadvertent password disclosureand missing accesscontrol checks. The requires few changes to the existing application code, and an assertion can reuse existing code and data structures [11].	A prototype of RESIN incurs a 33% CPU overhead running the HotCRP conference management application.	Recommended
Mobile Malware	Cloud Security	This application can understand the crucial areas in Cloud Computing. Retrievable threats and vulnerabilities. This application is also a service model for cloud computing. Organizations that work cloud- based can implement this application in the form of information	Cloud computing provides an efficient, scalable, and cost-effective way for today's organizations to deliver business or consumer IT services over the Internet. A variety of different cloud computing	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest [13].	Recommended

		security risk mitigation [13]	models are available, providing both solid support for core business functions and the flexibility to deliver new services [13].		
Social Media Attack	Information Security	Crowdsourcing Cybersecurity: This application performs information security detection using social media applications [14–17]	A new query expansion strategy based on convolution kernels and dependency parses helps model semantic structure and aids in identifying key event characteristics.	The class of attacks that the system is geared to as well as at modeling sequential dependencies (from occurrence to reporting) of cyber-attacks.	Recommended
Sabotage	System Security	Mitigation of information security threats with FMEA approach and Fuzzy Theory [18-20]	The consistency of improved FMEA proved to be more consistent than traditional FMEA	The limitation of this study was memory issues because both action research cycles were carried out by the same team and with similar case studies.	Recommended
Identify Theft	Incident Response	Information Security risk factors. [5][21][22]	This procedure evaluates risk levels more accurately by coping with the interdependencies among security control families and determines the information systems safeguards required for better security	The limitation is the inner and outer dependences within a cluster and among different clusters can be handled by the ANP method to overcome the limitation in linear hierarchic structures.	Recommended

Information blackmail	Vulnerability Response	Analysis of the Relationship between Blackmail and Criminal Threats [23]. Analysis of Forced Contract Solutions for information security threats	Threats are uncontrived warnings.	The limitation to a modification which is 'fair and equitable' requires an objectively demonstrable reason for seeking a modification.	Recommended
Information System Threats	Data Security	Analysis of Attack Solutions, Threats with CCTV and Video surveillance security systems [24-25]	A solution to detect such attacks could be tainting of video frames	A new type of optical covert channel that exploits the limitations of human visual perception in order to unobtrusively leakdata through a standard computer LCD display.	Recommended

8 Conclusion

There are many information security methods that can be used to maintain information security. The methods that can be used include the Failure mode and effects analysis (FMEA) method and fuzzy theory, the RESIN method, the open-source security assertion markup language (SAML) method and the secure access layer. In this analysis it can be concluded that these methods are considered accurate in securing data and systems.

REFERENCES

[1] D. Ciptaningrum, E. Nugroho, D. Adhipta, and J. Grafika, "AUDIT KEAMANAN SISTEM INFORMASI PADA KANTOR PEMERINTAH KOTA YOGYAKARTA MENGGUNAKANCOBIT 5," vol. 2015, no. Sentika, 2015.

[2] I. J. Aritonang, E. D. Ud Ayanti, and N. Iksan, "Audit Keamanan Sistem Informasi Menggunakan Framework COBIT 5 (APO13)," *ITEJ (Information Technol. Eng. Journals*, vol.03, no. 02, pp. 2548–2157, 2018.

[3] H. Zafar and J. G. Clark, "Current state of information security research in IS," *Commun. Assoc.Inf. Syst.*, vol. 24, no. 1, pp. 557–596, 2009.

[4] M. Dečman and M. Vintar, "A possible solution for digital preservation of e-government: A centralised repository within a cloud computing framework," *Aslib Proc. New Inf. Perspect.*, vol.65, no. 4, pp. 406–424, 2013.

[5] B. Karabacak and I. Sogukpinar, "ISRAM: Information security risk analysis method," *Comput.Secur.*, vol. 24, no. 2, pp. 147–159, 2005.

[6] heru pratama, "Audit Keamanan Sistem Informasi Pada Kantor Samsat Di Kota Krui Menggunakan Cobit 5," vol. 2015, no. Sentika, 2018.

[7] J. M. Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizationalinformation security measures," *Inf. Manag. Comput. Secur.*, vol. 16, no. 4, pp. 377–397, 2008.

[8] International Journal of Information Management, "Institutional Repository The information security policy unpacked : A critical study of the content of university policies This item was submitted to Loughborough ' s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made availa," *https://dspace.lboro.ac.uk/)*, vol. 29 (6), pp. 449–457, 2009.

[9] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016.

[10] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance modelin organizations," *Comput. Secur.*, vol. 56, pp. 70–82, 2016.

[11] A. Yip, X. Wang, N. Zeldovich, and M. F. Kaashoek, "Improving application security with dataflow assertions," *SOSP'09 - Proc. 22nd ACM SIGOPS Symp. Oper. Syst. Princ.*, pp. 291–304, 2009.

[12] J. W. J. W. Yoder and J. Barcalow, "Architectural patterns for enabling application security," *Proc. PLoP 1997*, vol. 51, p. 31, 1998.

[13] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management frameworkfor the cloud computing environments," *Proc. - 10th IEEE Int. Conf. Comput. Inf. Technol. CIT-2010, 7th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2010, ScalCom-2010*, no. 2007, pp. 1328–1334, 2010.

[14] R. Goolsby, "On Cybersecurity, Crowdsourcing and Social Cyber-Attack," *Policy Memo Ser.*, vol. 1, pp. 1–8, 2012.

[15] R. P. Khandpur, T. Ji, S. Jan, G. Wang, C. T. Lu, and N. Ramakrishnan, "Crowdsourcing cybersecurity: Cyber attack detection using social media," *Int. Conf. Inf. Knowl. Manag. Proc.*, vol. Part F1318, pp. 1049–1057, 2017.

[16] E. Fink, M. Sharifi, and J. G. Carbonell, "Application of Machine Learning and Crowdsourcingto Detection of Cybersecurity Threats," *Contract*, no. 2009, pp. 1–12, 2011.
[17] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 914–925, 2018.
[18] M. M. Silva, A. P. H. De Gusmão, T. Poleto, L. C. E. Silva, and A. P. C. S. Costa, "A multidimensional approach to information security risk management using FMEA and fuzzy theory," *Int. J. Inf. Manage.*, vol. 34, no. 6, pp. 733–740, 2014.
[19] A. P. Subriadi and N. F. Najwa, "The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment," *Heliyon*, vol. 6, no. 1, p. e03161, 2020.
[20] N. Rahmatin, I. Santoso, C. Indriani, S. Rahayu, and S. Widyaningtyas, "Integration of the fuzzy failure mode and effect analysis (Fuzzy FMEA) and the Analytical Network Process (ANP) in marketing risk analysis and mitigation," *Int. J. Technol.*, vol. 9, no. 4, pp. 809–818, 2018.
[21] G. Goth, "Identity theft solutions disagree on problem," *IEEE Distrib. Syst. Online*, vol. 6, no. 8, p. 2, 2007.
[22] M.- Chang Lee, "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 1, pp. 29–45, 2014.
[23] A. B. Cox, R. A. Epstein, and E. A. Posner, "The university of Chicago law review," *Univ. Chicago Law Rev.*, vol. 80, no. 1, pp. 1–6, 2013.
[24] A. Costin, "Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," *Trust. 2016 - Proc. Int. Work. Trust. Embed. Devices, co-located with CCS 2016*, pp. 45–54, 2016.
[25] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.