Journal of Multimedia Information System VOL. 7, NO. 3, September 2020 (pp. 215-220): ISSN 2383-7632(Online)
http://doi.org/10.33851/JMIS.2020.7.3.215

Framework for assessing responsiveness to personal data breaches based on Capture-the-Flag

Sangik Oh[1], Byung-Gyu Kim[2], Namje Park[1*]

Abstract

Many state agencies and companies collect personal data for the purpose of providing public services and marketing activities and use it for the benefit and results of the organization. In order to prevent the spread of COVID-19 recently, personal data is being collected to understand the movements of individuals. However, due to the lack of technical and administrative measures and internal controls on collected personal information, errors and leakage of personal data have become a major social issue, and the government is aware of the importance of personal data and is promoting the protection of personal information. However, theory-based training and document-based intrusion prevention training are not effective in improving the capabilities of the privacy officer. This study analyzes the processing steps and types of accidents of personal data managed by the organization and describes measures against personal data leakage and misuse in advance. In particular, using Capture the Flag (CTF) scenarios, an evaluation platform design is proposed to respond to personal data breaches. This design was proposed as a troubleshooting method to apply ISMS-P and ISO29151 indicators to reflect the factors and solutions to personal data operational defects and to make objective measurements.

Key Words: Personal data, System of Infringement Response, ISO29151, ISMS-P, *Capture the Flag*

I. INTRODUCTION

We live in a society where anytime, anywhere can be connected with the touch of a finger. People are connected, people are connected, things are connected. Artificial intelligence and big data analytics technologies are combined with IoT to bring incredible innovation and change. This factor of change is particularly possible thanks to the data. In recent years, the paradigm of the global economy has shifted to the data economy. The data economy is a system that creates new added value based on data assets. Data is a source resource that enables innovation in all areas, including big data, artificial intelligence, autonomous vehicles, smart factories, and smart healthcare. Among data, personal data is a key asset in the data-driven economy. Korea recently revised the Privacy Act in January 2020 to ensure the use and protection of personal data in order to secure the initiative in the data-driven economy [1]. These changes in the environment will require data subjects to find new balances in advancing the data economy without losing control over their personal data and to seek win-win strategies for both data subjects, data controllers and data users.

To do this, data subjects, data controllers, and data users all need a way to securely manage their personal information. However, the higher the utilization of personal information, the higher the risk of personal data infringement. State agencies and private companies use personal data to increase the use of personal data to deal with complaints or to pursue revenue through marketing. However, the risk of personal data infringement is increasing due to lack of awareness or mistakes of personal data handlers. According to the Korea Internet Agency, about 159,255 personal data infringement reports were received in 2019, and even after entering in recent years, personal data leakage and abuse cases have continued to increase [2]. Due to such accidents related to personal information, at the corporate level, we are experiencing cost expenditures due to legal disputes and the deterioration of corporate credit, and personal data is used indiscriminately at the individual level as well. Accordingly, the number of cases of damage such as invasion of privacy and phishing is increasing. In order to reduce the damage caused by such careless handling of personal information, the government is continuously strengthening public relations for changing awareness of personal data protection. Is committed to the security protection of personal data managed by public

Manuscript received September 09, 2020; Revised September 15, 2020; Accepted September 22, 2020. (ID No. JMIS-20M-09-025)
Corresponding Author (*): Namje Park, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, Korea, +82-64-754-4914, namjepark@jejunu.ac.kr
[1]Dept. of Convergence Information Security, Graduate School, Jeju National University, Jeju, Republic of Korea, raitsu58@jejunu.ac.kr
[2]Dept. of IT Engineering, Sookmyung Women's University, Seoul, Republic of Korea, bg.kim@sm.ac.kr

institutions. Institutions and companies have long recognized the importance of protecting personal data and, in order to manage it continuously, have introduced a certification of various personal data management systems such as ISMS-P (Personal Information and Information Security Management System) [3] and ISO27002 [4] to build a risk management system. It was However, even if a systematic management system of personal data protection is established at the organizational level, some members of the organization neglect the management of personal information, lack of consciousness, intentional leakage of personal information, etc. When an accident occurs, it becomes a big problem. The theory-based education and paper-based personal data breach response training do not greatly help raise awareness among members of the organization. In this paper, we design and propose a framework for assessing responsiveness to personal data breaches based on Capture-the-Flag. Capture the Flag (CTF) is a game that challenges problems composed of complex scenarios and is a useful way to solve many problems of engineering or fusion [5]. The Problem Method scenario is designed using the various types of privacy breaches that have occurred over the past five years, as well as indicators of ISMS-P and ISO29151 [6]. The framework for evaluating personal information infringement response based on Capture-the-Flag is an educational design plan aimed at helping anyone to easily detect signs of personal information infringement and increase the ability to respond quickly to accidents. In this research, we analyze the processing pattern of personal data managed by the organization, detect signs of abnormality, and can easily handle personal data leakage and abuse in advance, personal data leakage response training platform I will try to present you about the design proposal. In order to design such a framework for assessing responsiveness to personal data breaches based on Capture-the-Flag, we first identify the risks that may occur in connection with personal data leakage and identify the root causes that can cause the risk. We will try to define the important risk factors, and how to create important risk indicators that can be managed by quantifying the important risk factors. In particular, by giving an example of the main risk indicators related to the leakage of personal data and presenting them so that they can solve problems for each processing step and processing difficulty, the technical management of the organization for personal data protection It presents about the method that can implement the protective measures as a concrete system.

II. THEORETICAL BACKGROUND

2.1. Classification of Personal data

Personal data defined in the Personal data Protection Act refers to information that can identify an individual by using information that can be recognized by a living person, such as name, social security number, and video, or by using additional information that can be easily combined. The classification of personal data was classified into four stages, as shown in Table 1, by evaluating whether the person was identified and the risk of infringement [7].

Table 1. The classification of personal data.

Rating	Level of Personal Identification	Level of Infringement risk	List of Personal Data
1	High	High	Resident registration number, Alien registration number, Passport number, Driver's license number, Credit card number, Bio information (face, iris, fingerprint, vein, etc.) [8] , Consultation details, Location information, IP information, Personal video information, System (homepage) usage details, etc.
2	General	High	Name, Address, Phone number, Mobile phone number, Email address, etc.
3	Low	High	Race information, Religion information, Military service, Social group activities, Health information, etc.
4	Low	Low	Pseudonymized Data, General information (no personal information)

2.2. ISO/IEC29151 & ISMS-P

ISO/IEC29151 [9] defines control objectives, controls and control guidelines to meet the requirements identified by the risk and impact assessment associated with the protection of personally identifiable information, based on ISO/IEC 27002. The system applies to both public and private companies, government agencies and non-profit organizations that process personal information. Personal Information and Information Security Management System (ISMS-P) [10] is a system suitable for Korea based on the international standard ISO27001 and ISO29151. This

system is a system that the Korea Internet & Security Agency investigates and certifies that the organization's personal information protection and information management system is properly established and operated.

Table 2. Check list of ISMS-P & ISO29151.

Type	Check Category	ISMS-P	ISO29151
Collection of Personal Data	Restrictions on the Collection of Personal Data	O	O
	Agree to collect personal data	O	O
	Restrictions on processing resident registration numbers	O	O
	Limited processing of unique identification data and sensitive data	O	O
	Protection Measures for Indirect Collection	O	O
	Installation and operation of CCTV	O	-
	Action if used for marketing purposes	O	O
Protecting the retention and utilization of personal data	Managing the status of personal data	O	O
	Quality Assurance of Personal Data	O	O
	Restricting personal information display and protective measures when using it	O	O
	User terminal access protection	O	O
Protective measures against personal data destruction	third party provision of personal information	O	O
	Notice of the subject of information according to the consignment of duties	O	O
	Transfer of personal information according to work, etc.	O	O
	the transfer of personal information abroad	O	O
Protective measures against personal data destruction	destruction of personal information	O	O
	Measures to be taken when holding after retention	O	O
	User management of suspension of use	O	O
Protection of the rights of information subjects	Disclosure of Privacy Policy Disclosure	O	O
	guarantee of the rights of information subjects	O	O
	Usage Details Notice	O	O

2.3. Process for responding to infringement of personal data

In the event of a personal data breach, respond step by step as shown in Figure 1 [11].

Fig. 1. Process for responding to infringement of personal data.

2.4. Analysis of Personal Data Infringement Cases

The major infringement incidents of personal data from 2018 to 2020 are shown in Table 3. Most of the cases were found to have been caused by poor management and lack of awareness of personal information handlers.

2.5. Limitations of Related Research

So far, various curricula and simulations have been conducted to prevent the leakage and outflow of personal data from state agencies and a number of corporate-level applications. However, as the education system adopted a one-sided education system centered on legal compliance and theory, it lacked awareness of personal information handling and the personal information handler was always at risk of infringement. Simulated response tests based on virtual scenarios are limited to the participation of only some of the agencies and personnel who have personal information, and many of the personal information handlers do not understand the procedures for personal information infringement and thus cannot handle accidents quickly. To

overcome this, this study proposes the design of framework for assessing responsiveness to personal data breaches based on Capture-the-Flag.

Table 3. Infringement of Personal data (2018-2020).

Year	Case	Content
2018	Google Plus: 52.5 million major privacy breaches [12]	Two software vulnerabilities in Google Plus have resulted in 52.5 million major privacy breaches
2018	Marriott Hotel: Approximately 500 million customer data exposures [12]	The Marriott Hotel had an accident in November 2018 in which about 500 million customer data were exposed.
2018	Facebook: Software bugs [12]	Software bugs have occurred, exposing 70 million users' information
2020	A number of local authorities in Korea: Information leak of infected persons with the COVID-19 [13]	Disclosure and leakage of route information of COVID-19 infected persons due to lack of awareness and error by the person in charge.
2020	Local government in jeju: Failure to comply with restrictions on processing unique identification information [14]	70,000 people's personal information is exposed because the person in charge of personal data does not enforce unique identification processing restrictions

III. DATASET ANALYSIS AND PLATFORM DESIGN PROPOSAL

3.1. Design of framework based on Capture-the-Flag

A response assessment framework for assessing responsiveness to personal data breaches based on Capture-the-Flag is proposed as shown in Figure 2. The proposed framework was divided into stages 1 to 3 by difficulty. Level 1 is a sub-level question that measures basic concepts such as the definition of personal data and general legislation. Level 2 is designed as a virtual environment in which management methods and technical, administrative and physical security measures for systems collecting personal data can be practiced to help them understand the process of personal data processing at an intermediate level. Level 3 focuses on developing the ability to quickly respond to various personal information breaches at the top level. At this stage, it is designed as a problem-solving method to learn how to take action at a high level for fault results measured by standard indicators such as ISMS-P, ISO27001, ISO29151.

All the problems given to each level were solved so that they could move on to the next level, and if they did not pass, they had to study online education courses and guides to give feedback. Ranking is given based on processing completion time. Through all stages, the overall score and ranking could be checked, and the evaluation results could be checked and printed by item.

3.2. Measurement Item Classification and Metrics by Level

The problem types of the personal information infringement response assessment platform for problem solving methods are as shown in Table 4, and the composition is divided by difficulty level. Based on the casebook published by the Personal Information Protection Commission (2012-2018) [15] and the casebook for personal information protection evaluation between 2013 and 2017 [16], data by case were collected and analyzed. Defect cases based on the results of the ISMS-P [17] certification review by local governments were classified as cases and designed as a solution to the problem [18]. The scoring criteria for each question were given one point, and the measurement methods were multiple choice and practical.

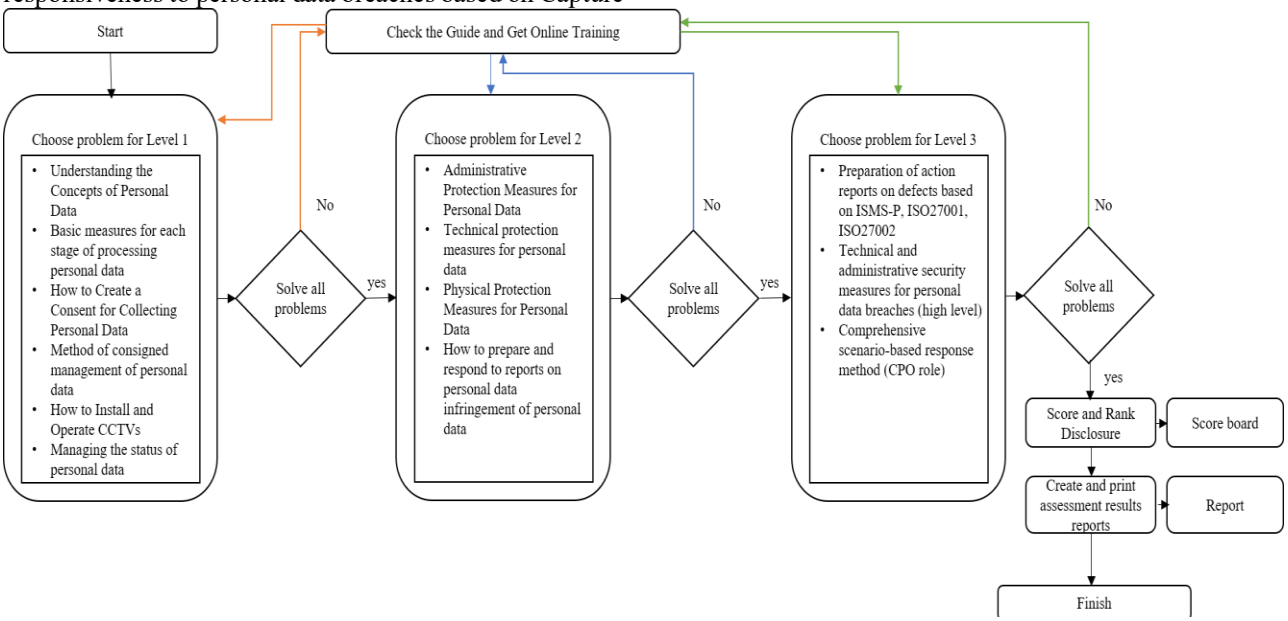

Fig.2. Design of framework for assessing responsiveness to personal data breaches based on Capture-the-Flag.

Table 4. Measurement item classification and metrics by level.

Level	Measurement Item	Number of cases	Ideal score	Measurement method
1	Understanding the Concepts of Personal Data	5	5	Multiple-choice
	Basic measures for each stage of processing personal data	15	15	
	How to Create a Consent for Collecting Personal Data	10	10	
	Method of consigned management of personal data	10	10	
	How to Install and Operate CCTVs	20	20	
	Managing the status of personal data	5	5	
2	Administrative Protection Measures for Personal Data	20	20	Multiple choice or practice
	Technical protection measures for personal data	25	25	
	Physical Protection Measures for Personal Data	10	10	
	How to prepare and respond to reports on personal data infringement of personal data	15	15	
3	Preparation of action reports on defects based on ISMS-P, etc.	25	25	Multiple choice or practice
	Technical and administrative security measures for personal data breaches (high level)	25	25	
	Comprehensive scenario-based response method	20	20	

IV. CONCLUSION

We have conducted various curricula and mock training to prevent the leakage and outflow of personal data. As the education system adopted a one-sided education system centered on legal compliance and theory, there was a lack of awareness of the handling of personal information, and the personal information handler was always at risk of infringement. Simulated response training is also conducted based on virtual scenarios, with only part of the agencies and personnel holding personal information participating. As a result, many personal information handlers are unable to handle accidents quickly because they do not understand the procedures for personal information infringement.

In this study, we proposed the design of CTF game-based personal information leakage response education platform that can analyze the processing patterns of personal information managed by the organization, detect anomalies, and easily handle leakage and abuse of personal information in advance. The platform focused on understanding the possible risks associated with personal data breaches, identifying the root causes of risk induction and strengthening the ability to resolve them on its own. In particular, it is expected that organizations and managers in charge of personal data protection will help by guiding and presenting major risk indicators related to personal data leakage through a web-based platform to solve problems by processing stage and level of difficulty. In future research, we would like to establish a proposed training and training platform and conduct empirical research on institutional personnel.

Acknowledgement

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A04083374).

REFERENCES

[1] S. Kim. “Meanings and Tasks of the Three Revised Bills which Ease Regulations on the Use of Personal Information,” *Journal of Information and Security*, vol. 20, no. 2, pp. 59-68, 2020.

[2] Personal Information Protection Commission. “Annual Report on Personal Information.” *Personal Information Protection Commission*, pp. 2-30, 2020.

[3] S. Oh, W. Jung, and N. Park. “A Study on the Improvement and Application of Information Protection Management System Model for the Application of State and Public Institutions,” *Journal of Academic Announcement of the Korean Information Science Association*, vol. 19, no. 6, pp. 1162-1164, 2019.

[4] Georg Disterer. “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *Journal of Information Security*, vol. 13, no. 4, pp. 92-100, 2013.

[5] H. Huang. et al. “A differential game approach to planning in adversarial scenarios: A case study on capture-the-flag,” *2011 IEEE International Conference on Robotics and Automation Robotics and Automation (ICRA)*, 2011 IEEE International Conference on, pp. 1451-1456, 2011.

[6] Kung A. et al. “A Privacy Engineering Framework for the Internet of Things,” *Law, Governance and Technology Series*, vol. 17, no. 36, pp. 163-202, 2017.

[7] C. Park. et al. (full authors list) “Improvement of Personal Information Protection Level in the Military Using the Measurement of Disclosure Risk,” *Journal*

of Security Engineering, vol. 12, no. 6, pp. 581-596, 2015.

[8] L. Leng. “Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain,” *International Journal of Physical Sciences*, vol. 5, no. 17, pp.2543-2554, 2010.

[9] International Organization for Standardization. “ISO/IEC 29151:2017.” https://www.iso.org/standard/62726.html (Sep. 7, 2020)

[10] Korea Internet & Security Agency. “Personal Information & Information Security Management System.” https://isms.kisa.or.kr/main/ispims/intro/ (Sep. 7, 2020)

[11] Seogwipo city, “Guidelines for Information Protection and Personal Information Management,” *Seogwipo city*, vol. 1, pp. 5-242, 2020.

[12] Boan News. “Large-scale information leakage cases that caused havoc in 2018. https://www.boannews.com/media/view.asp?idx=75796 (Sep. 7, 2020).

[13] DongA.com. Ilbo, “Anyone can see personal information recorded for quarantine purposes,” https://www.donga.com/news/article/all/20200904/102787012/1 (Sep. 7, 2020).

[14] Halla-Ilbo. “I'm sorry to the citizens for exposing their personal information on tax returns,” http://www.ihalla.com/read.php3?aid=1598407971690676048 (Sep. 7, 2020).

[15] Personal Information Protection Commission. "Casebook of rulings on matters concerning personal information protection of local governments." https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS079&mCode=D070020000&nttId=6159 (Sep. 7, 2020).

[16] Ministry of Public Administration and Security. “Personal Information Inspection and Administrative Action Casebook (2013-2017),” *Ministry of Public Administration and Security*, pp. 48-344, 2018.

[17] S. Oh, N. Park. "The Improvement of Information Protection Service Cost Model in Public Institution," *Journal of the Korean Society of Information Technology*, vol. 17, no. 7, pp. 123-131, 2019.

[18] S. Oh, N. Park. “Performance Analysis and Improvement for the Cost Model of Information Protection Service,” *Domestic Master's Degree Paper, Graduate School, Jeju National University, jeju*, pp. 27-41, 2020.

Authors

Sangik Oh is a doctoral student in the Department of Convergence Information Security at Jeju National University. Since 2009, he has been working for the information protection team in Seogwipo City. His research interests include personal data protection, information security policies in the public sector, cybersecurity and ISMS-P.

Byung-Gyu Kim has received his BS degree from Pusan National University, Korea, in 1996 and an MS degree from Korea Advanced Institute of Science and Technology (KAIST) in 1998. In 2004, he received a PhD degree in the Department of Electrical Engineering and Computer Science from Korea Advanced Institute of Science and Technology (KAIST). In March 2004, he joined in the real-time multimedia research team at the Electronics and Telecommunications Research Institute (ETRI), Korea where he was a senior researcher. In ETRI, he developed so many real-time video signal processing algorithms and patents and received the Best Paper Award in 2007. From February 2009 to February 2016, he was associate professor in the Division of Computer Science and Engineering at SunMoon University, Korea. In March 2016, he joined the Department of Information Technology (IT) Engineering at Sookmyung Women’s University, Korea where he is currently a full professor.

He is serving as an associate editor of Circuits, Systems and Signal Processing (Springer), The Journal of Supercomputing (Springer) and The Journal of Real-Time Image Processing (Springer). From March 2018, he is serving as the Editor-in-Chief of The Journal of Multimedia Information System and associate editor of IEEE Access Journal. From 2019, he was appointed as the associate editor and topic editor of Heliyon-Computer Science (Elsevier), Journal of Image Science and Technology (IS &T), Electronics (MDPI), Applied Sciences (MDPI), and Sensors (MDPI), respectively.

Namje Park received the BSc degree in information industry from Dongguk University, Korea in 2000, and received his M.E., and Ph.D. degrees in Information Engineering from Sungkyunkwan University in 2003, and 2008 respectively.

He is a Professor of Department of Computer Education in Teachers College at Jeju National University since 2010. He has been serving as a Research Scientist of Arizona State University since 2010. Prior to joining the researcher at ASU, he had worked as a post-doc at University of California, Los Angeles for 1 year. And he had an appointment as the senior engineer of the information security research division of the Electronics and Telecommunication Research Institute for 6 years.