ICIC Express Letters
Volume **11**, Number **2**, February **2017**

ICIC International ©2017 ISSN 1881-803X
pp. **261–268**

A STUDY ON DEVELOPING FRAMEWORK FOR INFORMATION PRIVACY PROTECTION

Jinwoo Jung[1] and Jungduk Kim[2]

[1]Department of Security Convergence
Graduate School
[2]Department of Industrial Security
College of Business and Economics
Chung-Ang University
84, Heukseok-ro, Dongjak-gu, Seoul 156-756, Korea
{ zinuojung; jdkimcau }@gmail.com

Received August 2016; accepted November 2016

Abstract. *Although information privacy is one of the biggest issues in the enterprises, privacy incidents are relatively increasing because most companies concern privacy protection as a short term project not like an essential factor which needs to be considered consistently. IP3 (information privacy protection program) means that the program should be conducted continuously as a background program in enterprises. If the operation or design of privacy protection is inappropriately implemented in an enterprise, they must pay for the failure of information privacy protection because it is closely relative to customer and their trust toward the enterprise. Therefore, appropriate information privacy protection program is required to prevent enterprise from loss of trust. This study intends to analyze the topic of information privacy and proposes an information privacy program framework. The framework consists of 4 domains, 18 indicators and 59 metrics to cover the necessary components of the information privacy program. The proposed framework for information privacy protection program is pilot tested to identify the strength; it is measured by proposed indicators to realize a real condition and feasible object of information privacy protection program framework. The results are positive in terms of their materiality and feasibility by conducting focus group interviews with five privacy managers.*

Keywords: Information privacy, Information privacy protection program, Privacy protection model

1. **Introduction.** Nowadays, information privacy protection is regarded as a serious issue in public and private sectors [1]. The damage of cyber attack is increasing and becoming a serious issue for business because the result of information privacy leakage is equal to loss of trust from customers and business partners [10]. There are a number of cases about privacy leakage accidents. Even if they are well known international companies such as Sony, Blizzard entertainment and Apple, they already had an experience of the accidents. According to the Ponemon Institute's research (2014), the average cost for each stolen or lost record containing sensitive or confidential information is $145 (U.S). In case of Verizon's report it shows that 95% of the 174 million records contained personal information compromised worldwide in 2011, and the total cost is significant. These cases ostensibly address a relation between information privacy protection and its impact on business in terms of cost and reputation from customers; therefore, information privacy needs to be concerned as an essential factor in business [11]. Enterprises have their own method to manage information privacy relying on ISMS (Information Security Management System). Although the importance of information privacy is district, information

privacy protection is concerned one of parts of ISMS in general. In other words information privacy is running like a short term project. Privacy is not a subordinate concept of ISMS anymore in business; it should be one of the main concepts [9].

Most of researches on information privacy is still in early stage because they are focused on how to protect privacy independently; however, the approach of this paper is based on embedded information privacy protection in enterprise which is called IP3 (information privacy protection program) framework which is operating continuously like a background management program in enterprises for privacy protection.

In this study, a framework of IP3 is proposed by analysis of related documents, and after that, indicators and its metrics are developed from the framework. They are reviewed in terms of materiality and feasibility by using focus group method.

2. **Previous Study Analysis.** There are a number of documents for information privacy protection from ISO/IEC, NIST, Federal CIO Council and so on. In this section, these documents are analyzed to find pivot and distinct elements for privacy protection as a best practice. After that the necessary elements are combined with ISMS to build up the IP3 framework.

'Elements of a Federal Privacy Program' suggests a guideline to help federal organizations implement, continuous privacy awareness and management. It consists of leadership, privacy risk management and compliance documentation, information security, incident response, notice & redress for individuals, privacy training & awareness and accountability [2]. In case of Discovering Constructs and Dimensions for Information Privacy Metrics in Stockholm University, it mentions some of privacy frameworks which are AICPA/CICA (the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants) privacy framework and ISTPA (International Security Trust and Privacy Alliance). AICPA/CICA privacy framework introduced this privacy framework in November, 2003 and revised it in March, 2004. This framework contains ten privacy components: management, notice, choice and consent, collection, use and retention, access, disclosure, security, quality and monitoring and enforcement [8]. ISTPA released version 1.1 of its privacy framework in 2002. This privacy framework includes audit, certification, control, enforcement, interaction, negotiation, validation, access, agent and usage [16].

NIST 800-53 (Security Privacy Controls for Federal Information Systems and Organizations) is one of the most famous guidelines for security controls for organizations to establish secure information systems and effective risk management. This guideline also includes list of privacy controls: authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, security, transparency and use limitation [13]. ISO/IEC 29101 (privacy architecture framework) develops for ICT systems that processes personally identifiable information (PII). It also provides the list of controls for the framework which include high-level privacy controls for system that process PII, guideline for planning and establishing ICT system that needs to protect privacy by controlling the process, access and transfer of PII and privacy enhancing technology (PET) [12].

Above documents are fairly focused on an importance of privacy, as this study has mentioned privacy needs to be background program in business which means, privacy needs to run as the same level of ISMS. ISO/IEC 27001&27002 are the most general documents for ISMS; therefore, the analysis result of previous study combines with those international standards. For example, there is PIMS (Personal Information Management System) which should be appreciable management system in South Korea.

3. **Proposed Information Privacy Protection Program.** ISACA suggests a general business model consists of main elements (Organization Design and Strategy, People, Process and Technology) and dynamic interconnections (Governing, Culture, Architecture,

Enabling & Support, Emergence and Human Factor). Furthermore, Gartner's business model consists of security governance, security management and platform & IT operations. Proposed IP3 framework is based on these models and this framework is greatly divided into two main parts: oversight and implementation. Oversight layer includes G.R.C and implementation layer consists of People, Process, Technology which is well-known implementation model called P.P.T model.

In this section, the proposed IP3 framework and its indicators are developed. The indicators are used to measure the IP3 framework.

The proposed IP3 framework aims at systematic and continuous management of information privacy protection. This IP3 framework includes oversight layer (G.R.C) and implementation layer (people, process and technology) with 18 areas.

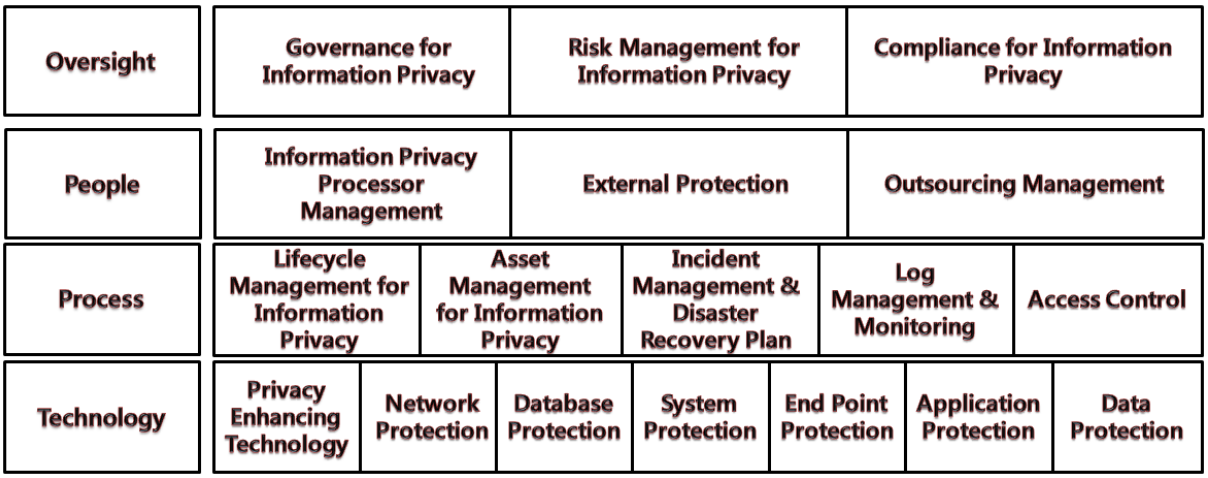

FIGURE 1. Framework of IP3

3.1. **Oversight layer.** As oversight layer is represented by G.R.C area, mostly the role and responsibility of executive management are emphasized in this layer [5]. Activities of information privacy protection need to be conducted by the result of risk assessment. If the selected countermeasure is not suitable, it will result in unnecessary budget wastage and ineffective information privacy protection. These activities which are identifying information assets, evaluating vulnerabilities and define risk about information privacy process/service play a key role of IP3. Especially, the analysis of information privacy flow chart is one of the most important methods to manage a process of information privacy and identify risk and then the risk should be continuously monitored and communicated with internal or external related parties [2]. Furthermore, the regulation of privacy compliance should be highlighted in information privacy protection [15]. Therefore, CEO would need to continuously check whether the activities of information privacy protection are followed by law or not, also objective and independent assurance need to be supported by internal or external audit.

3.2. **Implementation layer.** Typical implementation framework which applies with the PPT model includes People, Process and Technology to implement information privacy protection.

People area is divided into three parts: information privacy processor management, external protection and outsourcing management. Generally information is leaked by staff and therefore, information privacy processor management activity is one of the most important factors in IP3. For this reason, these are necessary: awareness for the employee who it may concern of information privacy, personnel audit, reward and punishment and clear responsibility of general user or administrator, to mitigate a leakage of information

privacy. External protection means how to manage visitors in business. The requirements of information privacy protection need to be noticed to 3rd party members and specified in the contract. If they do not follow the requirements or compliance, corrective measure is demanded to improve the situation. Furthermore, security written oath which includes requirements of information privacy protection with 3rd parties should be examined frequently especially, when there is any change of 3rd party members. The details of activities from 3rd party need to be examined and controlled consistently [4].

Process area means various management activities and it plays a core in IP3. This process includes lifecycle management for information privacy, asset management for information privacy, incident management & disaster recovery plan, log management & monitoring and access control. These processes can be controlled by technical tools but it needs to be conducted by the person in charge of information privacy. In other words, automated tools are used to assist it cannot substitute human input. The lifecycle management for information privacy means a management process for collection, sharing, storing, transmitting, use, and disposal of PII (Personal Identifiable Information) [13]. The system or service which deals with information privacy needs to be identified and the asset management list includes related employees and managers and so on; in addition, information privacy should be classified by confidentiality so it may include activities and control of categorizing and handling asset. One of the essential controls for information privacy protection is access control. Access control can be divided into physical access control and logical access control. Physical control includes admission to sensitive areas, facilities protection and so on. Logical control needs to categorize general user and system administrator to establish a different level of access control and authentication. Continuous monitoring is also one of the biggest issues. IDS (Intrusion Detection System) is required to mitigate the damage caused by information privacy incident because accidents or incidents cannot be prevented or controlled completely in IT environment. Furthermore, to prevent an information leakage, the number of employees in charge of information privacy need to be minimized and the PCs which contain significant amounts of information privacy need to be protected from phishing or tracking [4].

Technology area includes most of basic factors of IT: privacy enhancing technology (PET), network security, database security, system protection, end point protection, application protection, data protection. Privacy enhancing technology means technologies or tools to help a protection of the privacy of end-users. In short, it helps end-users to be more aware of privacy protection and sharing information or avoiding privacy risk and incidents [12]. In order words, an expected effect of PETs is to reduce information asymmetries, and thus negative externalities, by reducing the data flow from the individual user to the data controller [17]. The examples of PET are encryption tools, cookie-cutters, the platform for privacy preferences (P3P) and automatic anonymisation after a certain lapse of time. Network needs to be divided into internal and external network by privilege level to set a proper access control on network. If the access is from smart device to information privacy system, the countermeasures (e.g., authentication, approval, security setting on device, scope of allowance and monitoring) need to be established. A database which contains information privacy needs a strict access control and encryption. In addition, continuous auditing and monitoring about log file are necessary. System security means that only authenticated flash memory sticks are to be used which means that there should be a policy regarding the usage of flash memory. Moreover, frequent data backup of important information privacy is necessary as well testing a recovery system. Antivirus program must run on a server to prevent any risk from virus or malicious code. PCs or devices which contain information privacy should set up a virus vaccine or security solution to have secure setting (e.g., restriction of unauthorized software installation and prevention of keyboard hacking). Program for log monitoring and operation history

needs to be executed as a base on a system. Also spam filtering for Email or SNS is necessary to prevent a phishing, smishing and pharming. Application security means that program users need to be authenticated and it should be documentation. In addition, the main program which has an access to information privacy needs to apply for an enhanced authentication (e.g., OTP, Public-Key-Certificate). Encryption is required to response security incident; especially secure encryption algorithm is necessary for data which includes unique identification number and password. Web-hard, P2P and shared network drive should be restricted and monitored to prevent an information privacy leakage. Table 1 shows 18 indicators are developed to measure a maturity of IP3.

4. **Review of Research Result.** This study has developed the IP3 framework for enterprise and the propriety of proposed IP3 framework is required to verify. Accordingly, survey and in-depth interview with focus group has conducted. Propriety of proposed IP3 framework is verified by the focus group interview. The focus group consists of information privacy protection managers from five different organizations. Proposed 18 indicators have measured with its 59 metrics, also three-point Likert scale is used to measure its materiality and feasibility of each indicator. The result of focus group interview is on Table 2.

As a result of focus group interview, all of areas can be adopted. The area of G.R.C is relatively low in this result, it shows that experts realize the materiality of G.R.C; however, the feasibility is lower (2.4), which means that organizations recognize the importance of G.R.C; however, it is hard to apply to presenting business environment because the concept of G.R.C is difficult to understand. Therefore, stakeholder involvement for effective decision making and risk based approach to control various conflicts in terms of business are suggested by this focus group interview. People area shows that most of accidental privacy spills occur by an information privacy processor, that is why there is wide variation between materiality (2.8) and feasibility (2.4); on the other hand, outsourcing management and external protection are considered as a necessary factor in business in respect of both materiality and feasibility (2.6). It is ironic that even personal information leakage caused by the 3rd party members occurs recently, the materiality of controlling internal employees is higher than the 3rd party members; because that means comparing to the 3rd party members, internal employees are widely informed about organizational vulnerability. Comparing to control about internal employees, meanwhile, the 3rd party members are easy to be controlled by strict technical security mechanism and contract.

The feasibility of Lifecycle Management for Information Privacy and Incident Management & Disaster Recovery Plan is relatively lower than others in Process area. The focus group interviewer says it may mean that these processes are strictly controlled by policy and law but each enterprise has different organization culture or process, these elements make a difficulty of feasibility. The materiality of all factors in Technology area is highly recommended (2.8); however, feasibility of end point protection is significantly low (2.4) which means that although there is solution program for security, the fundamental caused by security accident is user who controls the end-point that is why the feasibility of end point protection in terms of Technology area is lower. Finally, average of materiality and feasibility is relatively high, 2.73/3, 2.58/3 in each. 5 organizations which are involved in investigation highly recognize an importance of areas, but in terms of feasibility it recognizes the difficulties because of realistic conditions.

TABLE 1. Contents of framework for information privacy protection program IP3

Domain	Indicator	Metric
G.R.C	Governance for Information Privacy	Development Plan & Strategy
		Decision-making Framework
		Management of Investment and Budget
		Implementation & Supervision of Information Privacy Program
		Performance Measurement
	Risk Management for Information Privacy	Impact Assessment and Risk Analysis
		Risk Assessment and Mitigation
		Risk Monitoring and Reporting
	Assurance of Compliance for Information Privacy	Review & Development of Policy
		Reporting a Present Condition of Law
		Handling External Audit
People	Information Privacy Processor Management	Awareness & Education
		Training Employees
		Reward and Disciplinary Action
	External Protection	Access Control for Visitors
		Device in & out Management
		Access History Management
	Outsourcing Management	SLA Management
		Outsourcing Employee Management
		Information Leakage Protection
Process	Lifecycle Management for Information Privacy	Collection
		Use
		Storage and Maintenance
		Sharing and Disposal
	Asset Management for Information Privacy	Management of Asset List
		Categorizing Asset
		Handling Asset
	Incident Management & Disaster Recovery Plan	Countermeasure Plan
		Instant Response & Following-up Management
		Disaster Recovery Plan
	Log Management & Monitoring	Log Management
		Monitoring and Reporting
	Access Control	General User Access Control
		Operation Manager Access Control
		Physical Access Control
Technology	Privacy Enhancing Technology	Cookie Management
		Data Anonymisation
		Data Encryption
	Network Protection	Network Access Control
		Firewall or Intrusion Detection System
		Wireless Protection
		Network Vulnerability Analysis
	Database Protection	Database Encryption
		Database Monitoring Activities
	System Protection	Storage Protection
		Backup and Recovery
		Secure OS
		Virus Vaccine for Windows Server
		OS Protection Enhancement
	End Point Protection	Anti Virus Program
		Secure Setting on PC
		Spam Filtering
	Application Protection	Authentication
		Transmission Encryption
		Web Protection
	Data Protection	Secure Data Sharing
		Document Encryption and Monitoring
Sum	18	59

Table 2. The result of focus group interview

Domain	Area	Materiality	Feasibility
G.R.C	Information Privacy Governance	2.6	2.4
	Risk Management of Information Privacy	2.8	2.4
	Assurance of Compliance for Information Privacy	2.6	2.4
People	Information Privacy Processor Management	2.8	2.4
	External Protection	2.6	2.6
	Outsourcing Management	2.6	2.6
Process	Lifecycle Management for Information Privacy	2.8	2.4
	Asset Management for Information Privacy	2.8	2.6
	Incident Management & Disaster Recovery Plan	2.6	2.4
	Log Management & Monitoring	2.6	2.8
	Access Control	2.8	2.8
Technology	Privacy Enhancing Technology	2.8	2.4
	Network Protection	2.8	2.8
	Database Protection	2.8	2.8
	System Protection	2.8	2.8
	End Point Protection	2.8	2.4
	Application Protection	2.8	2.8
	Data Protection	2.8	2.8

5. **Conclusion.** This study has attempted to establish the framework of IP3 for sustainable improvement of IP3 level in enterprises. Criteria and attributes are developed by various views (privacy, information security, business) to develop IP3 framework which has high applicability. In addition, indicators and its metrics are developed to measure indicators.

One of limitations of this study is that IP3 framework is difficult to generalize because the IP3 framework is verified by the focus group which is made up with only five experts; in other words, the empirical validation is slightly inadequate. As a result, more systematic and quantitative research is required to be utilized for future study. On the other hand, as this study mentioned, there has been minimal research regarding privacy protection program, so this study should lay the foundation for future work on privacy protection program in enterprises additionally, and the developed indicators and metrics can be used for future study.

Acknowledgments. This research was supported by the Chung-Ang University Research Scholarship Grants in 2015.

REFERENCES

[1] A. Sangar, Data privacy protection: A serious business for companies, *International Law News*, vol.41, no.4, https://www.thelawyer-network.com/documents/whitepapers/pdf/Qa2_Bk837.pdf, 2012.

[2] C. Barrett, C. Brannigan, P. Carcirieri et al., *Best Practices: Elements of a Federal Privacy Program v1.0*, Federal CIO Council Privacy Committee, 2010.

[3] ISO/IEC 27001:2013, *Information Technology-Security Techniques-Information Security Management Systems-Requirements*, 2013.

[4] ISO/IEC 27002:2013, *Information Technology-Security Techniques-Code of Practice of Information Security Controls*, 2013.

[5] ISO/IEC 27014:2013, *Information Technology-Security Techniques-Governance of Information Security*, 2013.

[6] ISO/IEC 29100:2011, *Information Technology-Security Techniques-Privacy Framework*, 2011.

[7] ISO/IEC 29101:2013, *Information Technology-Security Techniques-Privacy Architecture Framework*, 2013.

[8] K. Askelson, Reasonable security practices: The AICPA/CICA privacy framework, *The CPA Journal*, DOI=https://www. questia.com/magazine/1P3-878023961/reasonable-security-practices-the-aicpa-cica-privacy, 2015.
[9] J. D. Kim, *A Study on the Measurement of the Information Privacy Program Maturity Model*, Chung-Aung University, 2014.
[10] L. Rainie, J. Anderson and J. Connolly, Cyber attacks likely to increase, *Internet Project Report for the 25th Anniversary of the World Wide Web*, Pew Research Center, 2014.
[11] M. J. Culnan and P. K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation, *Organization Science*, vol.10, no.1, pp.104-115, DOI=http://bear.warrington.ufl.edu/weitz/mar7786/Articles/procedural%20fairness%20and%20 privacy.pdf, 1999.
[12] N. Ripmann, *User Interface Design for Privacy Enhancing Technology*, Master Thesis, Norwegian University of Norwegian, 2012.
[13] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2013.
[14] Ponemon Institute, *The Role of Governance, Risk Management & Compliance in Organizations*, DOI=http://www.emc.com/collateral/about/news/ponemon-report-egrc.pdf, 2011.
[15] PWC, *Key Considerations in Financial Services Global Privacy Compliance*, DOI=http://www.pwc.com/en_US/us/banking-capital-markets/publications/assets/global_privacy_compliance.pdf, 2007.
[16] R. Dayarathna, *Discovering Constructs and Dimensions for Information Privacy Metrics*, Ph.D. Thesis, University of Stockholm, 2013.
[17] S. Berthold, *Inter-temporal Privacy Metrics*, Ph.D. Thesis, University of Karlstad, 2014.
[18] J. Tadewald, GRC integration: A conceptual foundation model for success (governance risk and compliance), *Management Accounting Quarterly*, vol.15, no.3, pp.10-18, 2014.