# Study on Scenario-based Personnel Risk Analysis

Inhyun Cho, Jaehee Lee, and Kyungho Lee*
Korea University, Seoul, Republic of Korea
{ihcho13, foodlook, kevinlee}@korea.ac.kr

**Abstract**

In South Korea, personnel security has become an important issue due to a series of data leakage incidents in financial companies. As a follow-up action, the government devised countermeasures against future data leakage including the supervisory regulations, and the obligatory certification of information security management system (ISMS). However, these measures inherently lack special attention to managing personnel security risk. Thus, we propose a scenario-based risk measurement methodology that focuses on personnel security. Based on the scenarios extracted from past incident cases from 2006 to 2014 in South Korea and the world, and the survey result of IT banking employees, we measure the data leakage risk of personnel members per combined risk scenario. We argue that the scenario-based personnel risk analysis can facilitate understanding data leakage risk from the perspective of risk scenario and also drawing up specific controls for risky employees.

**Keywords**: Scenario-based Risk Analysis, Personnel Security, Data Leakage

## 1 Introduction

Since 2006, a series of data leakage incidents have occurred in South Korean financial companies. In particular, a total of 142,769,800 data have leaked since 2011[1]. Considering the South Korean population of 51,302,044 as of Oct, 2014 [2], the number demonstrates how serious the data leakage problem is. The leakage incidents highlight the importance of the personnel security issue because internal and outsourced employees were main threat agents [1].

The South Korean authorities regarded this personnel issue as of utmost urgency so as to introduce a series of regulations. In October 2012, the Financial Supervisory Service revised a regulation that stipulates financial companies are required to secure more than 5 percent of personnel for IT jobs, and more than 5 percent of IT personnel for information security. The revision also set a requirement for financial companies to secure more than 7 percent of their budget for information security [3]. In addition, in February 2012 the authorities announced the obligatory certification of information security management system (ISMS). Based on the Information Communications Network Act, Article 47 and 49, the obligation is imposed on ICT service operators whose revenue exceeded 10 billion Korean won (USD 9,480,470 as of Oct 31, 2014) in the previous year and whose daily customers were more than 1 million for 3 months right before the end of the last year [4].

However, it seems that the governmental countermeasures will not be effective in handling the personnel security problem. Firstly, the FSS's actions do not touch upon the risk of individual employees. Secondly, the ISMS-based risk analysis considers personnel factor as only one of objects of consideration. Therefore, we will study personnel security by reinterpreting the scenario-based risk analysis methodology. Based on the scenarios extracted from past incident cases from 2006 to 2014 in South Korea and worldwide, and on the survey result of 44 IT banking employees, we will measure data leakage risk of individual employees per combined risk scenario. We argue that the scenario-based personnel risk

*Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE)*, Vol. 1, Article No. 12 (January 15, 2015)

*Corresponding author: Graduate School of Information Security, Korea University, Seoul, Republic of Korea, Tel: +82-2-3290-4885, Web: https://sites.google.com/site/kurmlab/

analysis can contribute to understanding data leakage risk from the perspective of risk scenario and also drawing up specific controls for risky employees.

## 2 Traditional ISMS Risk Analysis

Traditional risk analysis is the process of examining assets, related threats and vulnerabilities to the threats (Figure 1). The risk analysis comprises the identification and analysis of assets, threats and vulnerabilities[5]. This process has been widely used in the information security management system certification, or a basis of the risk management system established by enterprises. This methodology is useful in measuring values or significance of assets, and evaluating relationship between threats and vulnerabilities of the assets quantitatively or qualitatively[6].
However, the traditional ISMS risk analysis has a limitation of focusing on risks relating to technological threats and vulnerabilities because ISMS mainly deals with IT system assets. Also, it covers the managerial security area broadly so as not to clarify risk factors which are entangled in the business process of enterprises. In addition, those overlooked factors like personnel factor contributed to the recent security incidents where a great deal of sensitive data leaked[6]. In this vein, there needs to be a new methodology for highlighting personnel security in terms of risk analysis.

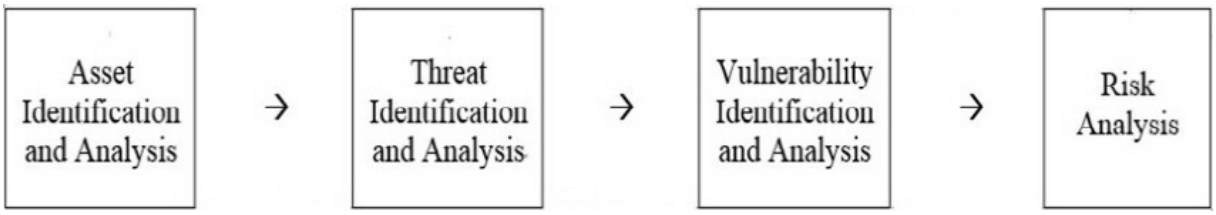


Figure 1: The traditional risk analysis process

## 3 Scenario-based Risk Analysis Methodology

Scenarios are effective in understanding risks and opportunities[7]. First, scenarios expand one's thinking in that they allow people to develop a range of likely outcomes and to demonstrate how the outcomes are and why they happen. Second, scenarios uncover inevitable or near-inevitable futures. Developing scenarios helps people to search for unexpected outcomes, which provides deep insight. Last but not least, scenarios protect people against 'groupthink' because they permit them to think beyond the organizational hierarchy and consider contrary perspectives. Although scenarios are not a cure-it-all, they are useful tools. In this sense, scenarios can make risk analysis more specific and tangible[8].

### 3.1 Scenario Analysis Flow and Risk Factors

Figure 2 illustrates that IT risk scenarios can be drawn from two different approaches[9]. A top-down approach begins from the overall business objectives and seeks to find the most relevant risk scenarios that influence the business objectives. A bottom-up approach draws up a list of scenarios and uses the list to define more detailed and tailored scenarios. On top of the two approaches, considering and applying risk factors contribute to refined and specific IT risk scenarios because the risk factors affect risk scenarios in terms of impact and frequency. Risk factors are composed of two main categories; environmental

factors and capabilities, each of which is divided into 1) internal and external environmental factors; and 2) IT risk management capabilities, IT capabilities, and IT-related business capabilities. Figure 3 describes risk factors in more detail[9].

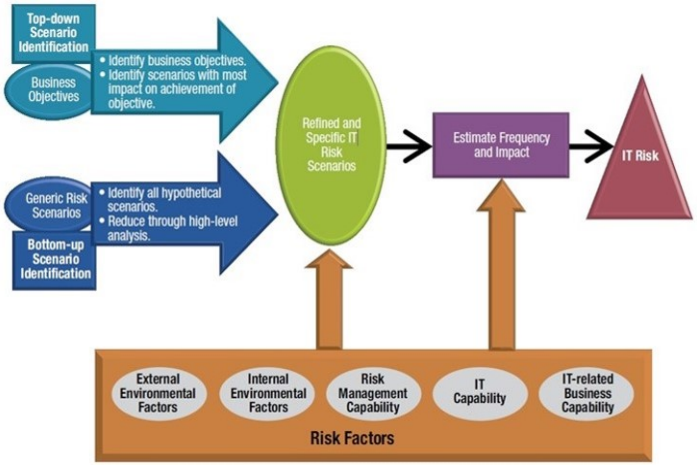


Figure 2: IT Risk Scenario Development

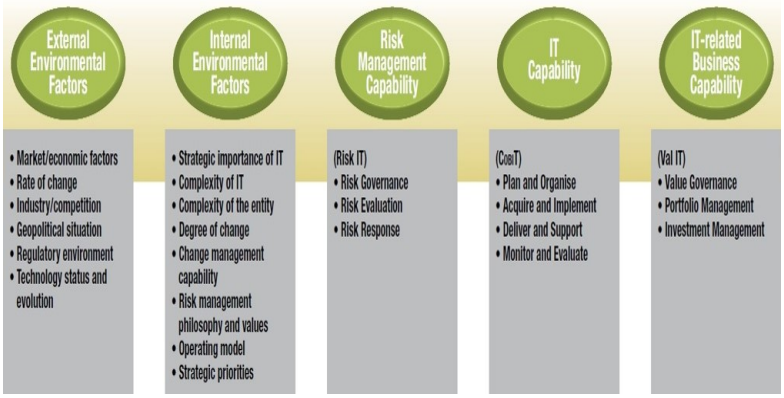


Figure 3: Risk Factors in Detail

## 3.2 Risk Scenario Components

In order to make risk scenarios complete and useful for risk analysis, they should contain components as shown in figure 4 [9]. Actors are agents who give rise to threats. They can be internal (e.g. internal staff, contractors) or external (e.g. outsiders, competitors, regulators, the market). Threat types means the nature of events. Depending on the nature, threat types have categories such as malicious, accidental or error, failure, natural, and external requirement. An event refers to a type of occurrence such as disclosure or modification of information, interruption of a system or a project, theft, destruction, ineffective design of a system or a process, ineffective execution of a process, etc. An asset or a resource is any valuable object that can be affected by events and causes business impact, or anything that helps achieve business objectives. Time refers to duration, timing of occurrence of an event, and timing to detect an event.


Figure 4: Risk Scenario Components

# 4 Scenario-based Personnel Risk Analysis in the Context of Data Leakage

## 4.1 Incident Case Analysis and Risk Scenario Components

The scenario-based risk analysis focusing on personnel security comes from reinterpreting the ISACA's scenario-based methodology. Thus, instead of starting by taking top-bottom and bottom-up approaches, we analyzed past incidents to establish a ground for scenario-based risk analysis. The past incidents are major data leakage cases that have occurred between 2006 and 2014 (Table 1). Through these cases, we identified risk scenario components of data leakage. In the context of data leakage, actors are hackers , internal and outsourced employees. Targeted data are sensitive data like business, customer, and financial data.

| Date | Title | Targeted Data | Actor | Method |
|---|---|---|---|---|
| Feb, 2008 | Korean E-commerce company's data leakage | Customer data | Hacker | APT attack |
| Sep, 2008 | Korean Oil refinery company data leakage | Customer data | Internal Employee | DVD |
| Nov, 2009 | Night Dragon (World) | Business data | Hacker | SQL injection |
| Jan, 2010 | Operation Aurora (USA) | Business data | Hacker | APT attack |
| Sep, 2011 | Samsung Card customer data leakage (Korea)[1] | Customer data | Internal employee | SQL injection |
| July, 2012 | Korean Telecommunication company data leakage[2] | Customer data | Retiree, hacker | Using hacking tool |
| Dec, 2013 | Standard Chartered Korea & Citibank Korea | Financial data | Internal employee | Printing, USB |
| Jan, 2014 | 3 Korean Card companies' data leakage | Customer data | Outsourced employee | USB |

Table 1: Major Data Leakage Cases

From the cases, we also found that the leakage incidents had been caused by those with malicious intention to disclose, or steal sensitive data during office hours or non-office hours (Figure 5).

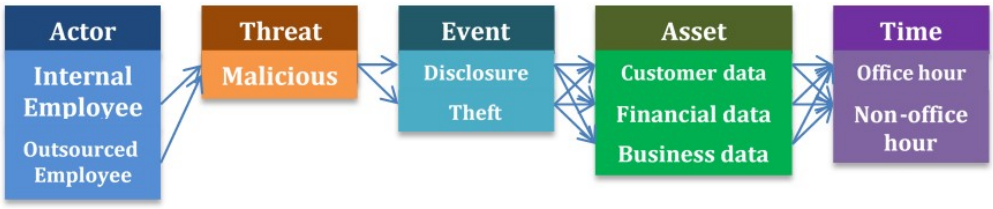


Figure 5: Personnel Risk Scenario Components in the Context of Data Leakage

Through closer examination of the cases above, we identified data leakage stages and detailed actions for each stage. We divided the data leakage stages into query stage, query result processing stage, and leakage stage. For each stage, we identified actions such as attempt to connect for query, query execution, file saving, leakage, and then analyzed each action in more detail (Table 2). We applied the output to generating data leakage risk scenarios.

[1]In the Samsung Card case, the infiltrator was an internal employee without authority to make an inquiry of customer data so that he used SQL injection of inserting asterisk(*) into customer name section in order to search all the customer data in the DB.

[2]In the Korean Telecommunications case, a retiree who was well aware of vulnerabilities of the customer sales management system colluded with a hacker and a telemarketer. The retiree shared the vulnerabilities with the hacker so that he could exploit the system by using customized RUN.BAT and Nfetcher. And the telemarketer took advantage of leaked data so as to make unfair profits.

| Stage | Detailed Action | | |
|---|---|---|---|
| Query/ Collection Stage | Attempt to connect for query | Connection time | Normal(Office hours) / Abnormal(Non-office hours) |
| | | Synchronous connection | Existence of users to connect simultaneously |
| | | Unauthorized connection | Connection attempt by users with unregistered IP |
| | | Administrator account connection | DB Root ID connection to sensitive data storage (DB) |
| | Query execution | Connection frequency / volume | 1. queries are made more than monthly average<br>2. queries are made for massive data, not individually |
| Query Result Processing Stage | File saving | Normal access | Request for deactivating digital rights management |
| | | Abnormal access | Attempt to forcibly deactivate digital rights management process |
| Leakage Stage | Leakage | Printing | Printing out sensitive data |
| | | External storage | Repeated file saving by users authorized to write in external storage media / Forced deletion of USB control solution or attempt to terminate control process |
| | | Internet | Transmission of sensitive data via email, messenger, SNS, etc. |

Table 2: Detailed Actions of Data Leakage

### 4.2 Risk Factors

Risk factors in the existing scenario-based analysis cannot apply directly to the context of data leakage because the existing scenario-based analysis centers upon IT system assets, as is the case with the traditional ISMS risk analysis. Still, the scenario-based personnel risk analysis sticks to the definition of risk factors, or what affects risk scenarios in terms of impact and frequency. Putting personnel factor at the center of analysis, we identify risk factors of data leakage as the impact of data accessed by employees, related risk components that materialize threats against the data, and likelihood of occurrence of threats.

In terms of information security goals, data leakage is mainly about disrupting confidentiality of data, rather than integrity or availability[3], and consequent impact on finance or business functioning is worthy of consideration. Detailed actions, or threats mentioned in Table 2 and the degree of the threats should be risk factors because they contain details that give rise to data leakage and have their own threat degree and likelihood of occurrence.

### 4.3 Risk Scenario Generation Process

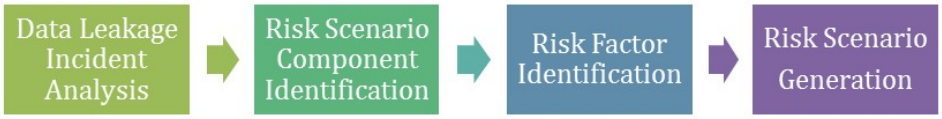


Figure 6: Risk Scenario Generation Process

Thus far, we have covered the first three steps of the risk scenario generation process (Figure 6). The next step is to generate data leakage scenarios based on the output of the previous procedures. As a result, we generated the following 23 threat scenarios (Table 3).

| Number | Scenario |
|---|---|
| 1 | Attempted access to DB by non DB administrator like developers, subcontractors, internal employees (success or failure) |
| 2 | Attempted access to DB by DB administrator account during non-office hours (success or failure) |
| 3 | Multiple DB queries that exceed the amount of normal queries |
| 4 | For an employee who only have inquiry authority to arbitrarily save sensitive data in PC (with abnormal access) |
| 5 | Inquiry of sensitive data by the same account connected from different IP addresses |
| 6 | Inquiry of sensitive data by an account unregistered in DB table |
| 7 | Saving sensitive data as files in the internal storage of DB (with normal access) |

[3]One may point out that other than confidentiality, integrity and availability (CIA), other goals such as non-repudiation, authentication should be considered in determining risk factors. However, fundamentally this paper focuses on the concept of information security, which aims to prevent attacks from taking place and protect information in terms of CIA, not information assurance, which seeks to ensure that even if an information system comes under attacks, certain degree of confidentiality, integrity, availability, authentication, or non-repudiation are secured [10]

| Number | Scenario |
|---|---|
| 8 | Booting in safe mode an inquiring sensitive data |
| 9 | Deleting security programs without permission and connecting to DB |
| 10 | A)System administrator PC infected by malicious code B) Connection by external system, or external attacks (when an attack agent is without access authority) |
| 11 | A) Connection by external system, or external attacks B) System administrator PC infected by malicious code (when an attack agent is without access authority) |
| 12 | Login attempt by an application user(developers, outsourced staff, internal employee) from an IP address different from previous access sources (success or failure) |
| 13 | Attempted access to applications by a user during non-office hours (holidays, overtime) (success or failure) |
| 14 | Multiple DB queries that exceed the amount of normal queries |
| 15 | For application user to save sensitive data through application (with normal access) |
| 16 | Connection to applications and inquiry of sensitive data by an account from different IP addresses |
| 17 | Deleting security programs without permission and connecting to application |
| 18 | Copying the data to storage media(USB, R-HDD, DVD) or via e-mail, messenger, SNS, etc. |
| 19 | Printing out sensitive data |
| 20 | Saving in PC or shared folders sensitive data unnecessary for tasks |
| 21 | Decrypting encrypted sensitive data (with normal access) |
| 22 | Sending an e-mail containing sensitive data |
| 23 | Accessing object of attack through remote access or during work |

Table 3: Data Leakage Scenarios

The scenarios above can be categorized according to the data leakage stages (Table 4).

| Stage | Query/Collection Stage | Query Result Processing Stage | Leakage Stage |
|---|---|---|---|
| Scenario Number | 1,2,3,5,6,8,9,10,11, 12,13,14,16,17,23 | 4,7,15,20,21 | 18,19,22 |

Table 4: Data Leakage Scenarios Categorized according to the Data Leakage Stages

### 4.4 Risk Analysis

Based on the result of the risk scenario generation process, a survey was conducted for 53 IT banking employees at K Bank in Seoul, South Korea. Among them, 44 returned questionnaires. A half of them were internal employees, and the other half were outsourced employees. The survey dealt with the

kind of data which employees handle for IT banking tasks, and the likelihood of data leakage scenarios each employee may have to do with. Then, another survey was done for the 44 respondents in order to determine the impact of data in terms of security (confidentiality), finance, and business functioning and the threat degree of risk scenarios. Here, impact is how much damage or effect can be caused when a data leakage incident occurs (Table 5, 6, 7, and 8 [11]). And likelihood means the frequency of occurrence of scenario situations (Table 9).

| Level | | Description |
|---|---|---|
| Very High | 5 | Data leakage incurs serious damage to enterprise or has public influence |
| High | 4 | Data leakage involves sensitive data, the violation of rules or law |
| Medium | 3 | Data leakage involves the violation of rules or law |
| Low | 2 | Insignificant data leakage |
| Very Low | 1 | Publicized data |

Table 5: Criteria of Security (Confidentiality) Impact

| Level | | Description |
|---|---|---|
| Very High | 5 | Severe financial asset damage to enterprise |
| High | 4 | Considerable costs for substitution or recovery |
| Medium | 3 | Costs of substitution or recovery that can be covered by switching budget item |
| Low | 2 | Low financial burden on enterprise |
| Very Low | 1 | No financial damage incurred |

Table 6: Criteria of Financial Impact

| Level | | Description |
|---|---|---|
| Very High | 5 | Extremely severe influence on business, critical damage to most services or critical service disruption |
| High | 4 | Major influence on business, likely damage to some services or service disruption |
| Medium | 3 | Influence on business, delay of some significant services |
| Low | 2 | Minor influence on business |
| Very Low | 1 | No influence on business |

Table 7: Criteria of Business Functioning Impact

| Level | | Description |
|---|---|---|
| Very threatening | 5 | Severe incidents are induced and public ripple effect is high |
| Threatening | 4 | Security-sensitive data are leaked out, which is deemed illegal |
| Middle | 3 | Incidents are involved with breach of enterprise rules or state law |
| Low | 2 | Information is handled that is not that important to enterprises |
| None | 1 | Incidents are about publicized data or data that are not significant to enterprises in terms of security |

Table 8: Scenario Threat Degree Criteria

| Level | | Description |
|---|---|---|
| High | 3 | Always occurring |
| Middle | 2 | Sometimes occurring |
| Low | 1 | Hardly occurring |
| N/A | 0 | Not applicable |

Table 9: Scenario Likelihood Criteria

Then, the survey results were quantified based on the criteria above. And the formulas were generated for the impact of data i, the impact of data accessed by an employee and the personal data leakage risk in scenario N were devised as below.

Here, confidentiality is the most basic and important element in determining impact of data in times of data leakage, and financial and business functioning factors add to the severity of data leakage which disrupts confidentiality. Therefore, it is reasonable to calculate the impact of data i by multiplying C, F, and B (1).

$$Impact\,of\,Data\,i = C \times F \times B$$

$$such\,that\,F = Confidentiality\,Impact\,of\,Data\,i \quad F = Financial\,Impact\,of\,Data\,i$$

$$B = Business\,Functioning\,Impact\,of\,Data\,i$$

The surveys revealed that among 11 kinds of IT banking data employees dealt with at least one kind of data and some had access maximum 6 kinds of data. Here, Max logic is used to calculate the impact of data accessed by an employee, because the result of Max operation represents the maximum amount of consequences or effects that occur in times of data leakage.

$$(Impact\,of\,Data\,Accessed\,by\,an\,Employee) = Max(Impact\,of\,Data1, \ldots, Impact\,of\,Data\,n)$$

$$such\,that\,n = Number\,of\,Kinds\,of\,Data\,Accessed\,by\,an\,Employee$$

Now, personal data leakage risk in scenario N can be calculated as shown in (3). Data leakage risk of an employee in scenario N is calculated as a product of impact of data accessed by an employee, likelihood of scenario N, and threat degree of scenario N.

$$(Data\,Leakage\,Risk\,of\,an\,Employee\,in\,Scenario\,N) = (I.D.A.E.) \times (L.S.) \times (T.D.S.)$$

$$such\,that\,I.D.A.E\;\; Impact\,of\,Data\,Accessed\,by\,an\,Employee,$$

$$L.S. = Likelihood\,of\,Scenario\,N, \quad T.D.S = Threat\,Degree\,of\,Scenario\,N$$

Based on the formulas above, we analyzed further to formulate combined-scenario-based methodology for risk analysis. Possible scenarios were chosen from each stage (query / collection stage, query result processing stage, and leakage stage) and combined to generate a combined risk scenario (Figure 7).

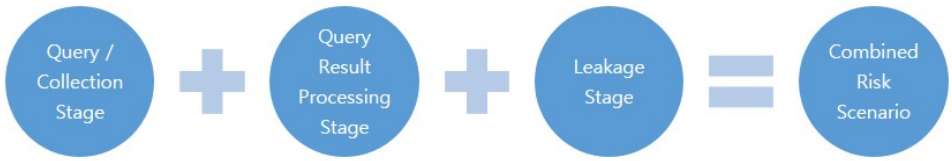


Figure 7: Combined Risk Scenario Generation

Then, the risk of a combined scenario is calculated as a sum of personal data leakage risk in the scenarios of query / collection stage, result processing stage, and leakage stage.

$$(Personal\,Data\,Leakage\,Risk\,in\,a\,Combined\,Scenario) = (A+B+C)$$

$$Such\,that\,A = Personal\,Data\,Leakage\,Risk\,in\,Query/Collection\,Stage\,Scenario$$

$$B = Personal\,Data\,Leakage\,Risk\,in\,Query\,Result\,Processing\,Stage\,Scenario$$

$$C = Personal\,Data\,Leakage\,Risk\,in\,Leakage\,Stage\,Scenario$$

In order to apply the new methodology, four combined scenarios were generated by choosing possible scenarios for each stage (Table 10).

| Stage | Query/Collection Stage | Query Result Processing Stage | Leakage Stage |
|---|---|---|---|
| Scenario Number | 2, 5 | 15 | 18 |
| | 1, 3 | 7 | 19 |
| | 16 | 21 | 18 |
| | 2, 14 | 15 | 22 |

Table 10: Personal Data Leakage Scenarios for Combined Scenario Analysis

In Figure 8, 9, 10 and 11, each combined scenario shows different distributions and scopes of personnel risk. This can help determine which risk scenario is more of significance than others and draw up different countermeasures according to the relative significance. On top of this, among the combined risk scenarios above, risk management officials may pinpoint the second scenario which contains person 18 of highest risk 14,259, identify him or her, and effectively come up with and practice countermeasures like detailed monitoring, separation of duty, etc. Also, the risk scenarios can be combined with enterprise

personnel risk appetite so that not only those with highest risk [4] but also unacceptably risky groups may be identified and specific controls be imposed upon them by considering their position levels, jobs, job-related information, access authority, and so forth. Furthermore, the database of scenario-based personnel risk will assist organizations in visualizing and managing personnel security status in a way that prevents data leakage by employees.

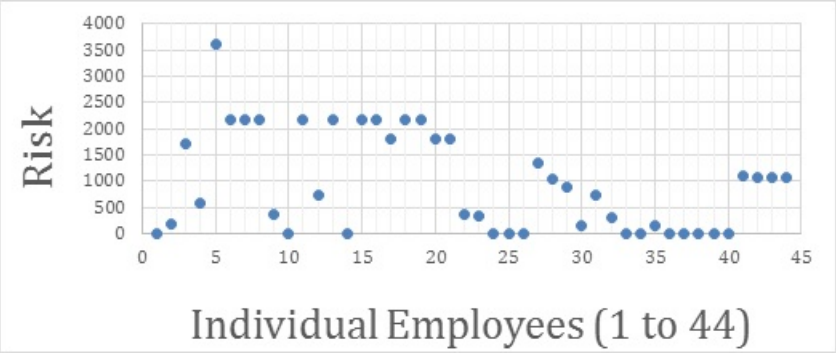


Figure 8: Combined Risk Scenario 1(2, 5, 15, and 18)

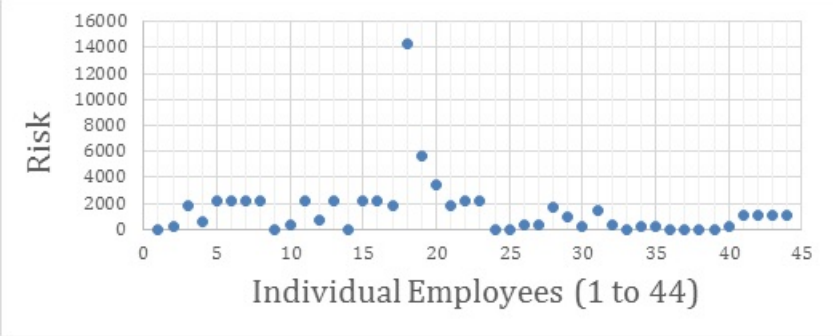


Figure 9: Combined Risk Scenario 2(1, 3, 7, and 19)

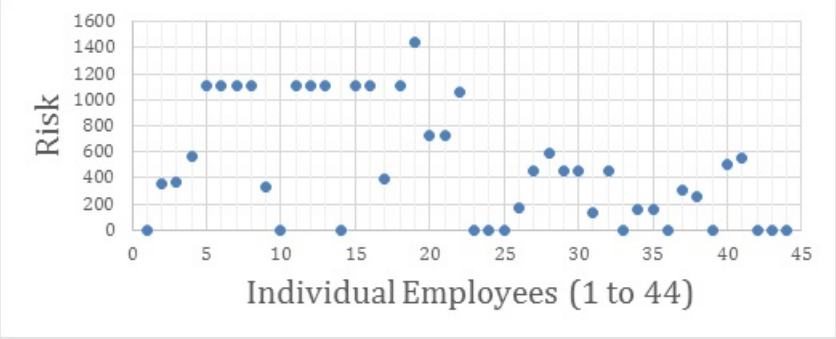


Figure 10: Combined Risk Scenario 3(16, 21, and 18)

[4]Person 5 in scenario 1 and 4, person 18 in scenario 2, and person 19 in scenario 3

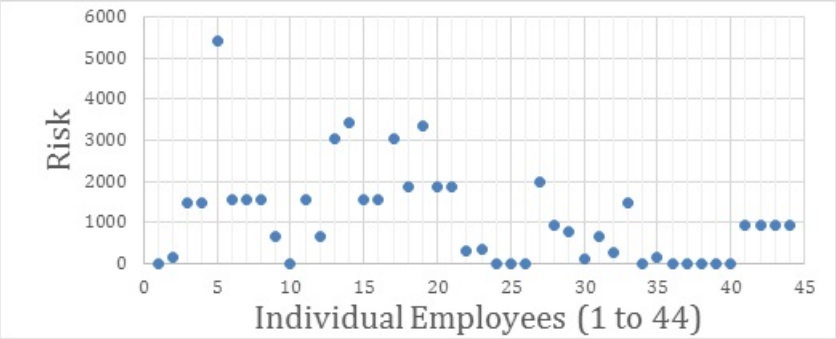


Figure 11: Combined Risk Scenario 4(2, 14, 15, and 22)

## 5 Conclusion

We started this study from the fact that the existing ISMS risk analysis centers on IT system assets and shows weaknesses in dealing with the personnel security issue, and that the governmental countermeasure against data leakage have a fundamental problem of not dealing with the risk of individuals. Thus, we reinterpreted ISACA's scenario-based risk analysis to analyze personnel data leakage risk. This research found out that scenario-based personnel risk analysis makes it possible to allow for data leakage risk of personnel from the perspective of combined risk scenarios. The methodology suggested in this paper can be used to effectively come up with and practice controls, or policy measures against personnel risk. We admit that the new methodology has a weak point of not considering human factors like personality in assessing data leakage risk of employees, which may cause a setback in drawing up and implement proper controls against certain risky employees. Therefore, the future research will be done to combine human factors with the scenario-based methodology. Also, personnel security issue is a matter of significant impact not only to financial industry but also IT manufacturing industry. Therefore, the future research will be conducted to generate data leakage scenarios in IT manufacturing industry, analyze personnel risk, and come up with countermeasures against possible incidents and risky employees.

## Acknowledgement

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA2014H0301141004) supervised by the NIPA (National IT Industry Promotion Agency)

## References

[1] Changlai Choi. Study on it outsourcing policy based on operational risks of financial industries. *Journal of the Korea Institute of Information Security and Cryptology*, 24(4):681–694, August 2014.

[2] Korean Statistical Information Service. Population Statistics based on Resident Registration. http://www.kosis.kr, October 2014.

[3] Financial Supervisory Service. Best Practice Standards for IT Security Tasks in Financial Companies. http://www.fss.or.kr, October 2012.

[4] Korea Communications Commission. Article 47 and 49 of Information Communications Network Act and Notification. http://www.kcc.go.kr, February 2013.

[5] Rex K. JR. Rainer, Charles A. Synder, and Houston H. Carr. Risk analysis for information technology. *Journal of Management Information Systems Archive*, 8(1):129–147, June 1991.

[6] Soo young Lee. Special report: Risk analysis and security consulting trend. Technical Report 118, TTA, South Korea, 2008.

[7] Charles Roxburgh. The use and abuse of scenarios. Technical report, McKinsey, 2009.

[8] Urs Fischer. It scenario analysis in enterprise risk management. *ISACA Journal*, 2:1–4, 2009.

[9] ISACA. The it practitioner guide. Technical report, ISACA, USA, 2009.

[10] Peng Liu, Meng Yu, and Jiwu Jing. Information assurance.

[11] Seoung woo Seo. *The Economics of Information Security*, volume 1, chapter 3, pages 224–261. Seoul National University Press, Reading, Massachusetts, second edition, may 2008.

---

## Author Biography

**Inhyun Cho** is working on a Matster's Degree in the Department of Information Security at the Graduate school of Information Security, Korea University. His research interests are in the areas of risk management, ISMS and consulting, and security engineering. He is also interested in personnel security issue in industry sectors, and IT governance.

**Jaehee Lee** is working on a Matster's Degree in the Department of Information Security at the Graduate school of Information Security, Korea University. His research interests are in the areas of risk management and quantum cryptology. He is researching SCADA Honeynet recently.

**Kyungho Lee** is a accociate professor in graduate school of information security, Korea university. He received his B.S. degree in Mathematics from Sogang University. He received his M.S. degree in Information and communications from sogang university. He received is Ph.D in information security from Korea university, seoul, Korea.He was Vice president of STG security corporation in 1999,CEO of culsulting house corporation form 2002 to 2007, director of NHN corporation from 2007 to 2008, SEO of secubase corporation form 2008 to present time. He has been assistanct professor from 2011 to 2014 and associated professor form 2014 to present time. His research interests are in the areas of Risk Management, Information Security Consulting, Privacy Policy and Privacy Impact Assessment.