





A Study on Analyzing Risk Scenarios About Vulnerabilities of Security Monitoring System: Focused on Information Leakage by Insider

Kunwoo Kim  and Jungduk Kim 

Chung-Ang University, Seoul 06974, Republic of Korea
kunwoo.kim317@gmail.com, jdkimsac@cau.ac.kr

Abstract. Information leakage by insider results in financial losses and ethical issues, thus affects business sustainability as well as corporate reputation. In Korea, information leakage by insiders occupies about 80% of the security incidents. Most companies are establishing preventive and prohibited security policies. Nevertheless, security incidents are unceasing. Such restrictive security policies inhibit work efficiency or make employees recognize security negatively. Due to these problems, the rapid detection capability of leakage signs is required. To detect the signs of information leakage, security monitoring is an essential activity. This study is an exploratory case study that analyzed the current state of security monitoring operated by three companies in Korea and provides some risk scenarios about information leakage. For the case analysis, this study collected each company's security policy, systems linked with security monitoring system, and system log used. As a result, this study identified vulnerabilities that were difficult to be detected with the current security monitoring system, and drew 4 risk scenarios that were likely to occur in the future. The results of this study will be useful for the companies that are planning to establish effective security monitoring system.

Keywords: Insider threat · Information leakage · Security monitoring

1 Introductions

With the development of information technology and the improvement of personal capacity in computing ability, the business efficiency using information technology is improving, whereas the security incident like information leakage is increasing. According to statistics, information leakage affects both the companies and customers, and in case of companies, customer confidence declines and market share reduces and in case of customers, secondary damage is expected by personal information leakage [1]. This means that information leakage is highly relevant to the sustainability of the company. One interesting fact is that there is a difference in the subject who involves in information leakage between Korea and foreign countries. In case of foreign countries, information leakage by hackers occurs three times more than information leakage by insider, on the other hand, in case of Korea, about 80% of the subjects who leaked information appear as insider [2]. As can be seen in the result of study, the current

security system in Korean companies has limitations in preventing insiders from leaking information although it is appropriate for defending external threats.

Currently in Korea, most companies are establishing and operating various security systems to prevent security incidents. However, despite such efforts, it is impossible to prevent security incidents perfectly as can be seen in the cases of the past. In other words, Korea has a high level of dependence on prevention-centered security measures including access control, document encryption by DRM (Digital Right Management), storage device control and email control. Nevertheless, security incident like information leakage inevitably occurs. Also, prevention-centered security measures involve various problems including hindrance to business efficiency and increase in negative awareness of security [3]. Of course, preventing security incident like information leakage is important, but it is necessary to improve the ability to detect and respond to the signs of leakage as quickly as possible.

However, it is not easy to detect the information leakage by insider quickly at all. The amount of event (access log, usage log, etc.) that is occurred by employees are vast and false positive also occurs often [4]. Also, the focus was on detecting unusual behavior in the past, but analyzing the misuse cases of employees who have an authority and look normal is a difficult task particularly in Korea [5]. Therefore, to monitor the signs of information leakage by insider effectively, it is necessary to analyze the current state of monitoring by companies and draw the improvement direction. This study is a case study on security monitoring to detect the signs of information leakage, among insider threats as quickly as possible. For the case study, this study collected the information related to security monitoring system being operated by companies in fields of finance, manufacturing, and information communication technology in Korea where information leakage incident occurs relatively frequently. And this study draws some limitations and suggestions by analyzing to which system the security monitoring system is linked and which logs are collected and utilized.

2 Theoretical Background

2.1 Insider Threat and Information Leakage

This section describes the definition and types of insider threat and looks at why insider threat is important and especially through which routes the information is leaked. There are various definitions on insider and in general, insider is defined as a person who can access IT system legitimately [6]. Therefore, an insider can be defined as a person who has the legal right to access the information assets of an organization logically or physically and thus may have a negative influence on confidentiality, integrity, and availability of information assets. In addition, the term can be distinguished from external attacker like hacker, by the term 'legitimately'.

As can be seen in the definition above, insider means a person who knows the internal affairs of an organization. Therefore, an insider is more threatening than an outsider, as an insider knows the value of confidential information held by an organization, how to use a system and its vulnerabilities, and how to detour security control

[7]. In addition, an insider's misbehavior is an ethical issue and if known to the outside, may have a bad influence on corporate reputation [1]. Therefore, security measures should be prioritized by focusing on security threats like insider's leakage of confidential information, even though incidents by a hacking attack have recently been increasing.

In general, an insider threat means the abuse and misuse of the authority given oneself to access the assets of an organization and use them [8]. The term 'abuse and misuse' includes unintended behavior like making a mistake as well as inappropriate behavior stemming from malicious intent. Therefore, an insider's security threat is an act that accesses a system or treats information and data in violation of an organization's security policy, either intentionally or unintentionally [9]. For example, when an employee accessed a vulnerable website and got infected by malignant code by mistake including leakage of company secrets to the outside, the leakage of secrets by hacking also belongs to insider's security threat.

An insider's security threat can be classified into Intentional Destruction, Detrimental Misuse, Dangerous Tinkering, and Naive Mistakes, depending on the behavior intention that may cause damage [10]. Intentional Destruction includes the act to destroy an IT system maliciously or delete information and data and Detrimental Misuse means the use of the authority given for a purpose of making personal gains or damaging the company. Dangerous Tinkering and Naive Mistakes mean an act to set up a system without using a strong password or considering the security, although there is no malicious intent. The information leakage is a malicious violation of security policy for personal gains and thus belongs to detrimental misuse and is classified as high-risk group. In addition, a recent study suggests the relevance between attitude and security [11]. However, there was no explanation about how to detect the deliberate risk-inclined behaviors.

2.2 Security Monitoring

Most companies in Korea are establishing and operating various security systems to prevent information leakage. If a lot of security system is established, the risk level of information leakage will be lowered, but business efficiency will also decline and thus the current trends are that they establish proper number of security system and detect unusual signs quickly. To detect unusual signs, monitoring is essential, and in general, the term monitoring is defined as collecting the information related to an individual [12]. Therefore, security monitoring can be defined as collecting the information related to whether employees are complied with security policies. The security monitoring can be divided largely into the following two dimensions [13]. The first is collecting the logs of the security system that protects information assets from the external attack using Intrusion Detection System, firewall and anti-virus, and detecting whether there was an attack or not. The second is collecting the logs of the security system that protects information assets from mistakes or malicious intention of internal employees and detecting unusual signs against organization's security policy.

For security monitoring, it is essential to collect and analyze a large amount of system logs, and in general, security monitoring is performed in four steps: log collection, log analysis, correlation analysis, and risk calculation [13]. A single log is

significant, but it is difficult to determine the signs of information leakage with single log only exactly and there might be a lot of false positive. Therefore, currently in Korea, most companies determine unusual signs by analyzing the correlation with single log and multiple log [14]. Logs for security monitoring can be collected at network level, system level, and application level [15]. In other words, logs can be collected from business system, electronic approval system, and personnel information system as well as security system, and the system linked with security monitoring may depend on the type and size of company.

As an analysis result of the past security incident cases in Korea, it appeared that information was leaked largely via internet, email and removal storage device [16]. Most companies block the use of commercial messenger services and restrict email sending via commercial email accounts or control the use of groupware email. Companies in Korea also detect the access and file upload to unauthorized web sites, and control the use of removal storage device such as USB and CD to prevent information leakage. The information leakage can be detected by setting threshold values based on employee's average file system access and use history [17]. In addition, symptoms of information leakage include use patterns of removal storage device, email sending patterns, document extension conversion, and unusual searches of data stored within the DB that happened in PC [18].

Meanwhile, a recent study suggested insider threat detection techniques such as anomaly based approach, role based access control, scenario based, using Decoys & Honey pots and risk analysis using psychological factors [19]. However, the study did not contain what kind of data use and how to detect the malicious behavior in detail. In addition, overseas studies related security monitoring did not consider some security systems like digital right management and removal storage device control and thus are different from the environment of Korea. Studies in Korea related security monitoring conduct research on single security system or are not specific on which logs are utilized and thus for conducting research from comprehensive perspective, it is necessary to analyze the actual monitoring cases by companies and draw improvement measures.

3 Research Methodology

There are three types in a case study. The exploratory case study is a way to look at the scale or extent of an unfamiliar problem or to suggest ideas for solving problems. The descriptive case study is a method of observing a specific phenomenon and systematically recording the result. The explanatory case study is a method of observing specific phenomena and explaining causal relationships. This study belongs to exploratory case study with a flexible design according to Yin's classification and includes semi-structured interviews with document analysis [20]. Since Yin's classification is the most cited representative case study, this study was referred to as a research methodology. For a case study, this study analyzed the current state of security monitoring operated by three companies in Korea. Three companies, targets of this study are in fields of finance, information communication technology and manufacturing, and the companies that could have a big ripple effect at the national and

individual level in case of occurrence of information leakage were selected. For collecting companies' data, we pledged to ensure companies' anonymity and use the data for research purposes only.

3.1 Industrial Background

Company A is a bank that provides various banking services including deposit, loan, foreign exchange, and investment. It belongs to a large-sized bank that holds about 25 million customers and critical information includes customer information and credit information. As the company has experience with security incident in the past, it is enforcing considerably strict and limited security policy. Company B belongs to field of information communication technology industry that now provides internet portal service, mobile community service, and cloud service. Major information includes customer information and service development information. As the company thinks employees' creativity and speed of service development important, its organizational culture is relatively freewheeling. Company C is a company that manufactures belongs to large-sized company. The critical information is parts design drawing because the company involves in B2B business, and the number of individual customers is less than other companies. An organizational culture is hierarchical, but as the company requires employees to be creative, the intensity of security policy is between company A and B.

3.2 Data Collection and Analysis

For the case study, we visited three companies and collected data and information about security monitoring system. At the first, systems linked with security monitoring system were identified to check the coverage of security monitoring system against information leakage. Company A has 15, Company B has 11, and Company C has 8 systems linked with security monitoring system. Of these, 4 security systems, Storage device control, Digital right management(DRM), Email control and Website access control system are linked with security monitoring system operated by all three companies. Table 1 shows a list of systems linked with security monitoring system operated by three companies and its function.

The four security systems mentioned above have similar main functions, but can be different in their operation depending on the policy. In case of Company A, most security policies are based on blocking as default because its organizational culture is hierarchical and rigid. Thus, an approval for exception is necessary. Specially the internal network is separated from the external network, the company is blocking so that the external network cannot be accessed with the computer connected to the internal network.

Company B requires employees to be creative and relatively freewheeling organizational culture is formed and thus when it comes to security policy, its security policy is opposite to the Company A's. Use of storage device and DRM decryption are possible by entering reason only and the number of sending emails is not restricted. Also, when it comes to website access, it is permitted to access all sites that are even not registered in blacklist including harmful website.

Company C is applying security policy at intermediate level between Company A and B. For example, prior to use of storage device, pre-approval is necessary like company A. On the other hand, DRM decryption is possible as long as the document is created by the user, and in case of email sending, approval is required only if the data over 10 MB are attached. Also, it is possible to access all websites that are not registered in blacklist like Company B.

Table 1. A list of system linked with security monitoring system and its function

No.	Linked system	Function	Company		
			A	B	C
1	Information asset mgmt.	To manage hardware and software asset	O	O	O
2	Storage device control	To control unauthorized storage device use	O	O	O
3	Digital right mgmt.	To manage document encryption and decryption	O	O	O
4	Email control	To control groupware and commercial email sending	O	O	O
5	Website access control	To control unauthorized website access and file transfer	O	O	O
6	N/W access control	To control of unauthorized access to internal network	O	O	O
7	HR mgmt.	To manage information about employees	O	O	O
8	Physical access control	To control in and out of authorized and unauthorized people	O	O	-
9	Personal info. identification	To identify document that contains customer's information stored in PC	O	O	X
10	Server access control	To control unauthorized access to server of business application	O	O	-
11	DB access control	To control unauthorized access to DB of business application	O	O	-
12	Illegal software block	To control installation of illegal software	O	-	-
13	Printer control	To control document printout	O	-	-
14	Wireless intrusion prevention	To identify and block unauthorized wireless AP	O	-	-
15	Customer info. processing	To manage collection, use, storage and destruction of customer information	O	X	X
16	Design drawing mgmt.	To control read, screen capture, download of design drawing	X	X	O

* O: linked with security monitoring system/X: not established/-: not linked

Analysis of the policies of the three security monitoring systems and the security systems of the three companies shows that there is a difference in operation of the security monitoring system according to environmental factors such as the field of the company and the culture of the organization. This means that analyzing the logs collected and used by the security monitoring systems of the three companies makes it possible to generalize the monitoring status and to conduct in-depth analysis. In the other word, it is possible to identify vulnerabilities that are hard to detect using security monitoring system by analyzing logs collected for security monitoring.

4 Results

The logs collected by the linked system in the Table 2 were analyzed and the vulnerabilities difficult to detect in common by three companies and the weak points by each company were drawn. At the first, the three companies all appeared not having collected the file types from the removable device control system. In this case, employees can change file type that not supported to DRM encryption and the leakage is difficult to detect because it is hard to conduct the correlation analysis of the logs collected from removable device control, DRM, and email control system. In case of company A and B, both are not collecting the HDD (Hard Disk Drive) information from the information asset management system. Thus, employees can release information by connecting the detachable HDD to PC where security software is not installed with slave. In case of company B, attached files and related logs are collected from the email control system, however a log related to the body of the message is not collected. Thus, it still has vulnerability in that email can be sent by attaching the service development information including source code to the body. In case of Company C, as the company does not collect access log and output log, it is difficult to detect the behaviors to print out and export the document to the outside. Therefore, based on the above log analysis results, it is possible to derive scenarios related to information leakage.

Table 2. Linked system and collected log

No.	Linked system	Collected log	Company		
			A	B	C
1	Information asset mgmt.	Employee name, user ID, Dept., position, PC name, MAC, IP, OS info., on/off status, power on time, power off time	O	O	O
		HDD serial number, number of HDD, HDD detachment code	X	X	O
2	Storage device control	PC name, MAC, IP, employee number, employee name, user ID, Dept., position, media type, start time, end time, file name, file size, number of file, download time, upload time, fail time	O	O	O
		Exception type, use request time, approval time, approval code	O	X	O
		Reason of use	X	O	X

(continued)

Table 2. (continued)

No.	Linked system	Collected log	Company		
			A	B	C
3	Digital right mgmt.	Employee name, user ID, Dept., position, document name, document type, creation time, creation user name, edit time, encryption time, decryption time, number of decryption, number of decryption fail, number of print, online/offline login code	O	O	O
		Exception type, decryption request time, approval time, approval code	O	X	X
		Reason of decryption	X	O	X
4	Email control	Employee name, user ID, Dept., position, sender name, send time, send IP, title, attached file name, attached file size, number of attached file, receiver name, receive time, receive IP, CC	O	O	O
		E-mail message, approval time, approval code	O	X	O
5	Website access control	Host address, access URL, access time, client IP, server IP, user ID, attached file name, attached file size, number of attached file, block URL, access time of block URL, search history	O	O	O
		Exception type, access request time, approval time, approval code	X	X	O
6	N/W access control	User ID, MAC address, IP, OS info., start time, session time, end time, policy code, access approval code, access fail code, security S/W installation code	O	O	O
7	HR mgmt.	Employee name, Dept., position, e-mail address, phone number, mobile phone number, fax number, address, birth date, gender, employment date, resignation date, employment status	O	O	O
		Attendance time	X	O	X
8	Physical access control	Employee name, employee number, Dept., position, badge number, access time, gate number, access fail time	O	O	-
9	Personal info. identification	Employee number, Dept., PC name, MAC, IP, search time, number of identification, information grade, number of personal information, file path, file name, file size, file creation time, file edit time	O	O	-
10	Server access control	User ID, access time, end time, system name, sever IP, client IP	O	O	-
11	DB access control	DBMS IP, DBMS server port, service number, policy number, login time, logout time, query number, query execution time, query end time	O	O	-

(continued)

Table 2. (continued)

No.	Linked system	Collected log	Company		
			A	B	C
12	Illegal software block	S/W ID, S/W type, S/W name, manufacturer, license type, license duration, expire date, serial number, user ID, blocked S/W name, blocked S/W code, installation time, installation block time	O	-	-
13	Printer control	User ID, user name, Dept., document, title, number of page, print date, number of copy, printer ID, printer port, printer IP, personal information inclusion code, print request time, reason of print, approval time, approval code, approval after print, expected document discard date	O	-	-
14	Wireless intrusion prevention	Time, host name, host location, IP, SSID, event code, event block, AP category, access time, end time	O	-	-
15	Customer info. processing	Processing ID, Processing name, customer name, user ID, user IP, use time, use category (creation, edit, read, download, print)	O	-	-
16	Design drawing mgmt.	Employee name, user ID, Dept., position, IP, design drawing number, design drawing name, authority code, read time, print time, print screen time, download time, reason of download	-	-	O

* O: collected/X: not collected/-: not linked

As seen in the above section, three companies all are operating the security monitoring system, but have still some vulnerability difficult to detect information leakage. This section draws risk scenarios about information leakage by using such vulnerability and provides improvement directions. Risk scenarios and related companies are summarized in Table 3.

The first risk scenario belongs to information leakage using the vulnerability related to change of file type. If employees recognize that their behaviors are being monitored, they can export information to the outside using approved storage device by changing the file type to graphic file (JPG, GIF etc.) or text file (txt), i.e. by deceiving the file as personal data rather than work data in order to minimize the doubts of administrator or security staff. To detect such scenario, it is necessary to collect additional file type logs from removable device control, DRM, and email control system and track the history of document change of the same name, size, and type.

The second risk scenario belongs to information leakage using the vulnerability related to detachable HDD. In case of company A's security policy, approval is necessary for DRM decryption and company B should enter reason for decryption. Also, if the decryption pattern increases, this can be detected as unusual sign through security monitoring system. However, if DRM decryption is conducted in constant patterns, the

security monitoring system has limitations in that it is difficult to detect by recognizing this as normal behavior. Moreover, the use of removable device is being controlled, however the security monitoring system does not collect the HDD related logs. Thus, there is a possibility to decrypt DRM in constant patterns and keep important document in storage and then export the detachable HDD to the outside. Lock can be installed to the frame of PC however employees might release the lock arbitrarily, and security staffs have to put a lot of time and effort to regular check of lock on PC used by all employees. Therefore, company A and B need to collect additional HDD information to detect whether HDD is detached or not as quickly as possible.

Table 3. Risk scenarios about information leakage

No.	Scenario	Company
1	Information leakage using approved removal device after changing file type	A, B and C
2	Information leakage detaching HDD after decryption of DRM in regular pattern	A and B
3	Information leakage via email after copying contents of document to the body of the email	B
4	Taking document out on weekends after printing the document on weekdays	C

The third risk scenario is related to information leakage via email. Company B is monitoring the email sent to the outside, but unlike company A and C, there are no restrictions on the email sending. Also, email sending monitoring focuses on attached file and does not collect the body of email and related logs. Therefore, company B's important information such as customer information and system development information can be sent to the outside through the body of email. Therefore, to detect such leakage, it is necessary to add rules to detect the type of important information like Social Security Number or if major scripts used for coding in case of system development are inserted into the body of email to detect information leakage.

The final risk scenario is related to information leakage through printout. In case of company C, the history of printout is left when printing the encoded document with DRM, however it is difficult to detect if storing the document that decrypted DRM in constant patterns and then going to work during holidays and printing out in quantity, because the security monitoring system does not collect separate logs from the printer. Moreover, as access logs are not collected from the physical access control system, it is difficult for the employees who do not go to work during holidays to go to work during the holidays and look for the abnormal signs. Of course, it is difficult to install individual access control devices residing in several companies within one building, but the attendance patterns during holidays can be identified if utilizing the other logs including document work history and website access history that occur during holidays. Also, if decrypted document ends, DRM is automatically encoded and thus if a lot of document are encoded with DRM suddenly, it is necessary to add the rules to detect this into the security monitoring system.

5 Conclusions

Information leakage by insider is recognized as the company's ethical issue and known to have bigger ripple effects than the information leakage by external attack like hacking. Especially in Korean companies, 80% of the subjects who involve in information leakage are insiders and so information leakage by insider emerges as a serious social problem. On one hand, most Korean companies are establishing preventive security policies but security incidents are occurring every year, and to overcome this, it is necessary to improve the ability to detect the signs of leakage as quickly as possible. The security monitoring is a necessary task for detecting the signs of information leakage. Overseas security monitoring related studies were conducted focusing on the methods to detect the attack from the outside and did not consider the security system operated by Korean companies. On the other hand, Korean security monitoring related studies conducted research on single security system or were not specific on which logs were utilized, and so to study from comprehensive perspective, it is necessary to analyze the actual monitoring cases of the companies.

This study analyzed the current state of security monitoring system operated by three companies in Korea. For a case study, company's security policies, systems linked with security monitoring system and logs were collected. Also, after identifying the vulnerability difficult to detect with the current security monitoring system, the risk scenarios that were likely to occur in the future were drawn and the methods to detect this were proposed. In this study we collected the security monitoring cases of the companies that held different industrial field, organizational culture, and security policy and generalized them to some extent. The result of this study will be useful for the companies that are planning to establish security monitoring system. Also, overseas companies that have similar security policies to Korean companies are expected to improve the detection performance of security monitoring system by referring to the risk scenarios.

Acknowledgments. This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2014-1-00636) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

1. Garrison, C.P., Ncube, M.: A longitudinal analysis of data breaches. *Inf. Manag. Comput. Secur.* **19**(4), 216–230 (2011). <https://doi.org/10.1108/09685221111173049>
2. Chang, H.B.: A study on the countermeasure by the types through case analysis of industrial secret leakage accident. *J. Inf. Secur.* **15**(7), 39–45 (2015)
3. Scholtz, T.: Consider a people-centric security strategy (2013). Gartner G00249357
4. Barnes, D.J., Hernandez-Castro, J.: On the limits of engine analysis for cheating detection in Chess. *Comput. Secur.* **48**, 58–73 (2015). <https://doi.org/10.1016/j.cose.2014.10.002>
5. Cho, S.K., Jun, M.S.: Privacy leakage monitoring system design for privacy protection. *J. Korea Inst. Inf. Secur. Cryptol.* **22**(1), 99–106 (2012)

6. Magklaras, G.B., Furnell, S.M.: A preliminary model of end user sophistication for insider threat prediction in IT systems. *Comput. Secur.* **24**(5), 371–380 (2005). <https://doi.org/10.1016/j.cose.2004.10.003>
7. Walton, R.: Balancing the insider and outsider threat. *Comput. Fraud Secur.* **11**, 8–11 (2006). [https://doi.org/10.1016/S1361-3723\(06\)70440-7](https://doi.org/10.1016/S1361-3723(06)70440-7)
8. Magklaras, G.B., Furnell, S.M.: Insider threat prediction tool: evaluating the probability of IT misuse. *Comput. Secur.* **21**(1), 62–73 (2001). [https://doi.org/10.1016/S0167-4048\(02\)00109-8](https://doi.org/10.1016/S0167-4048(02)00109-8)
9. Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E.: The insider threat to information systems and the effectiveness of ISO17799. *Comput. Secur.* **24**(6), 472–484 (2005). <https://doi.org/10.1016/j.cose.2005.05.002>
10. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. *Comput. Secur.* **24**(2), 124–133 (2005). <https://doi.org/10.1016/j.cose.2004.07.001>
11. Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., Calic, D.: Assessing information security attitudes: a comparison of two studies. *Inf. Comput. Secur.* **24**(2), 228–240 (2016). <https://doi.org/10.1108/ICS-01-2016-0009>
12. Stalla-Bourdillon, S.: Online monitoring, filtering, blocking.... What is the difference? Where to draw the line? *Comput. Law Secur. Rev.* **29**(6), 702–712 (2013). <https://doi.org/10.1016/j.clsr.2013.09.006>
13. Ambre, A., Shekokar, N.: Insider threat detection using log analysis and event correlation. *Procedia Comput. Sci.* **45**, 436–445 (2015). <https://doi.org/10.1016/j.procs.2015.03.175>
14. Park, S.J., Lim, J.I.: A study on the development of SRI (Security Risk Indicator)-based monitoring system to prevent the leakage of personally identifiable information. *J. Korea Inst. Inf. Secur. Cryptol.* **22**(3), 637–644 (2012)
15. Furnell, S.: Enemies within: the problem of insider attacks. *Comput. Fraud Secur.* **2004**(7), 6–11 (2004). [https://doi.org/10.1016/S1361-3723\(04\)00087-9](https://doi.org/10.1016/S1361-3723(04)00087-9)
16. Park, J.S., Lee, I.Y.: Log analysis method of separate security solution using single data leakage scenario. *Trans. Comput. Commun. Syst.* **4**(2), 65–72 (2015)
17. Thompson, H.H., Whittaker, J.A., Andrews, M.: Intrusion detection: perspectives on the insider threat. *Comput. Fraud Secur.* **2004**(1), 13–15 (2004). [https://doi.org/10.1016/S1361-3723\(04\)00087-9](https://doi.org/10.1016/S1361-3723(04)00087-9)
18. Liu, A., Martin, C., Hetherington, T., Matzner, S.: A comparison of system call feature representations for insider threat detection. In: *Proceedings from the Sixth Annual IEEE SMC*, pp. 340–347 (2005). <https://doi.org/10.1109/IAW.2005.1495972>
19. Sanzgiri, A., Dasgupta, D.: Classification of insider threat detection techniques. In: *Proceedings of the 11th Annual Cyber and Information Security Research Conference*. ACM (2016). <https://doi.org/10.1145/2897795.2897799>
20. Yin, R.K.: *Case Study Research Design and Methods*, 5th edn. Sage Publications, Thousand Oaks (2014)