The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth

Jawon Kim 1, Chanwoo Lee 2 and Hangbae Chang 3,*

1 Department of Convergence Security, Chung-Ang University, Seoul 06974, Korea; jjawon@cau.ac.kr
2 Information Security & International Business Division, Douzone Forensic Center, Seoul 04523, Korea; chanlee@douzone.com
3 Department of Industrial Security, Chung-Ang University, Seoul 06974, Korea
* Correspondence: hbchang@cau.ac.kr; Tel.: +82-2-820-5538

Received: 20 October 2020; Accepted: 14 December 2020; Published: 19 December 2020

Abstract: This research establishes a security evaluation model from the insider leakage perspective and suggests an objective evaluation measurement. Organizational security risks are fused and compounded both inside and outside the organization. Although multiple security controls are implemented to minimize an organization’s security risk, effective security control requires management to preemptively check the organization’s security level. Existing criteria for evaluating security level are limited to external security risks and have improper limit points for dealing with security risks that are fused and compounded within an organization. The focus of this study is the prevention of technical information leakage. Furthermore, we propose a method for measuring the level at which the objectivity of certain items is secured. We compiled 26 detailed evaluation items, considering the security requirements to prevent technical information leakage. We not only performed suitability, reliability, and factor analyses and statistical validation, but also established a method to measure the security level. This measurement method ensures the effectiveness and objectivity of the evaluation of security level, mitigating the risks of security incidents caused by insiders. The results serve as a reference for organizations when designing security evaluation criteria and automated tools based on our evaluation model for future research.

Keywords: insider threat; information leakage protection; security evaluation; sustainable growth

1. Introduction

An increasing number of security attacks that threaten organizations are occurring, and attacks targeting the main technical information of an organization may cause significant losses that can affect its continued existence. The early security attacks targeting the technical information of organizations were externally generated, such as by hackers from outside an organization capturing its major technologies. However, today’s security attacks are fused and compounded by both inside and outside parties. Alongside security attacks generated from outside the organization, attacks due to the leakage [1] of technical information by organization insiders have been increasing. According to Crowd Research Partners’ [2] Insider Threat Survey Report, 90% of 472 security experts believe they are vulnerable to insider security threats, as shown in Figure 1.
To protect themselves, organizations have applied security measures to prevent external cyberattacks and the leakage of technical information by insiders. To establish effective security measures, organizations must preemptively measure their security level [3], and must understand both the type and the level of necessary security measures. To measure and evaluate their security level, organizations adopt a security level diagnostic measurement index such as that recommended by the United States Department of Commerce’s National Institute of Standards and Technology (NIST), which is responsible for developing information security standards and guidelines. Its Special Publication SP 800 series reports—such as the SP 800-53, entitled Security and Privacy Controls for Federal Information Systems and Organizations [4]—provide a catalog of security and privacy controls for federal information systems and organizations, as well as a process for selecting controls to protect an organization’s operations, organizational assets, individuals, other organizations, and the United States from a diverse set of threats. However, current evaluation models focus on the response to external cyberattacks and have not yet focused on the prevention and detection of the leakage of technical information by insiders. Among 16 program management controls implemented by NIST, only one was identified as considering insider threats in practice. The program management control refers to security activities focused on information technology such as “Information Security Resources,” “Information System Inventory,” and “Information Security Measures of Performance,” but “Insider Threat Program” control is the only one related to insider attacks. This means that only 6.25% of program management controls mentioned in the standard consider insider threats. For the performance and long-term growth of an organization, technological development and protection activities are essential to protect information and information systems from access by unauthorized users and to prevent the use or destruction of information critical to organizational success [5]. This study aims to promote the sustainable growth of the organization through the following research questions. First, when designing the security evaluation model, what is the differential between being focused on outside attack and focused on insider threat? Second, what is the evaluation method for objective security level evaluation? To solve the research question, we aimed to design a reference model to measure security level and to establish an assessment model to support objective security evaluations based on digital information analysis. Proper security activities are essential to ensure the sustainable growth of organizations, and it is necessary to objectively measure their security level if security activities are to be initiated. Our model evaluates the technological protection level of an organization and may be used as a tool to aid in continuous security management.

The characteristics of internal technology information were derived through the analysis of prior studies, and the requirements necessary for the model’s development were established. Moreover, by analyzing precedent research related to the security evaluation model from the insider’s perspective as a control unit, a security evaluation model (suggestion) was derived from an insider perspective. Then, we performed a statistical validation of the suggested evaluation model through an expert survey and propose a statistically validated model through validation model, factor analysis, and reliability.
analysis. In addition, we established a digital trace analysis method using the digital forensic technique as an objective measurement for certain evaluation items and applied the feasibility test to confirm the applicability of the model in real-field companies.

2. Information Leakage Incidents and Evaluation of Security Level

2.1. Information Leakage Incidents

Corporations’ information leakage incidents have different characteristics from existing privacy issues. From the perspective of a corporation, internal technological information and privacy differ in terms of the relevant security activities, both before the occurrence of security incidents and activities and after the incident and the impacts on the organization. Prior to conducting security management, the distinguishing of information assets and graded security activities is performed according to level and private information handled by the corporation, including the private information of employees, customers and vendors, which are all graded as a single level [6]. However, in the case of internal technology information, patents, intellectual property rights, trade secrets, etc., are classified as multi-leveled, which results in different security activities being conducted according to each level [7]. After the occurrence of a security incident, impacts on the organization also differ in terms of privacy and internal technological information. In the case of a privacy leakage, the extent of the effects on the business is relatively small. However, in the case of internal technological information, this can directly affect business continuity at the level of deciding the existence of the organization, and this therefore incurs a larger amount of damage [7]. Security incidents that target this internal technological information caused by insider information leakage have different characteristics to external security incidents [8]. First, a privileged insider has a high level of legitimate access to sensitive data and knowledge, including where critical information is stored, extensions, existing cybersecurity measures, and methods of access; thus, an insider attack may go undetected for some time [9]. Furthermore, it may be difficult to determine if a security incident is caused by insiders with malicious intent or due to non-malicious human error [10]. Even if there is a leakage situation, it may be difficult to promptly identify a security incident, conduct an investigation, and contain the damage; in fact, security incidents caused by insider information leakage share certain characteristics with hidden crime in terms of the responsibility for the crime [11]. Thus, reputational damage can be significant following a data breach, and a company may seek to hide or delay publicizing the incident’s occurrence, potentially further damaging the organization’s reputation for reliability due to a perceived lack of transparency. Therefore, although the number of security incidents disclosed by organizations is small, the impact of the incidents on an organization is large, and while it is very difficult to recover the technology after the information has been leaked, it is also difficult to recover from the damage to an organization’s reputation [12]. Thus, the prevention of security incidents caused by insider information leakage is more important than post-incident analysis and evaluation. Table 1 summarizes the differences between internal and external security attacks on organizations.

| Table 1. Factors of internal and external security attacks. |
|---------------------------------------------------------|
| Attacks from Outside | Attacks from Inside |
| Recognizing the occurrence of a security incident | Easy (Network access log or system firewall) | Difficult (Difficulty identifying insider information leakage) |
| Security incident occurrences | More (Security incident from unspecified individuals) | Fewer (Security incident from insider, a specific person) |
| The scale of the security incident | Small (Access to system but hard to find and information leaked) | Large (Loss of market share, possibility of declining stock price, and/or eventual bankruptcy) |
| Recovery time | Short (Confirmation of the access point) | Long (Difficult to find leakage range) |
2.2. Evaluation of Security Level

Our study defines an organization’s security level by fusing and compounding their physical, managerial, and technical security activities. To effectively execute their security strategies, organizations should preemptively assess their security level, and the results of the assessment should be used when constructing or implementing a security system and environment. Periodic assessment of their security level helps to minimize vulnerabilities and enables the design of cost-effective security measures. To appropriately evaluate their security level, companies must have evaluation criteria that reflect their situation. Most security assessments today are conducted solely on the basis of organizations’ IT resources such as Personnel Computer, Server, Database, Information System; the most frequently studied security evaluation criteria are IT resource security evaluations, organizational networks, and investigations of vulnerabilities that may occur in data flows [13]. However, as security risks in organizations occur in a fused and combined manner, their security levels must be evaluated from a fused and combined perspective. To address this, companies use criteria for the evaluation of fused and combined security levels, such as NIST SP 800-53, which also focuses on external security incidents [14] of an organization but does not allow for internal security risks.

Furthermore, most evaluations of security level are measured by an evaluator who visits the organization, conducts an interview with a security officer, and evaluates the security policy and related documents (e.g., the access record ledger) to perform the evaluation. In order to measure the security level, the organization’s IT resources (e.g., PCs, servers, and databases) are randomly selected, and the degree to which the security criteria are satisfied is checked. However, these evaluators have great difficulty in ensuring the objectivity of the evaluation results. As the evaluation progresses, the evaluator’s subjectivity may intervene and—especially when evaluating IT resources—they may not look at the organization’s history of IT resource use. Since only a fragment of the system can be confirmed, the objective measurement of the organization’s security level is difficult. Therefore, our study provides a fusion/composite security evaluation standard that focuses on information leakage incidents and provides a method to measure security level that ensures objectivity for an organization’s IT assets.

3. Development of a Security Evaluation Model for Information Leakage Protection

Our study uses the methodology shown in Figure 2 to develop a security level evaluation model for information leakage protection. The research method was composed of the 4th step. In the first step, preceding research, we derive the characteristics of information leakage by insider threat. Subsequently, we derived requirements of security evaluation model focused on prevention of insider threat. We also analyzed precedent research about security evaluation models. In the second step, model design, we considered the result of requirements and analysis when designing a security evaluation model from the perspective of insiders.

![Figure 2. Research methodology.](image-url)
In the third step, model validation, we validated in a statistical way that suggested model. First, as a part of this step, we conducted expert survey for validation of the proposed model. Next, we checked whether the validity for proposed model’s criterion was suitable. Afterwards, we checked the convergent validity for measurement of the same concept between the proposed controls. Last, we checked the confidence interval analysis for validation of the consistency the survey results.

In the fourth step, after confirming the statistical relevance, we suggested the object security level evaluation measurement. After, we conducted a feasibility study about objective level of measurement, and we finally designed the security level evaluation controls and objective measurement method.

Referring to previous research that analyzed the security level from the perspective of technical information leakage to develop our evaluation model, the characteristics of technical information leakage incidents can be summarized as follows. First, it is difficult to recognize whether a security incident will occur. Second, the number of security incidents is small, but the impact is large. Third, organizations must consider post-incident damage, and recovery will take time. To design protection measures that reflect the characteristics of these technical information leakage accidents, several areas must be improved by adopting new protection measures, as shown in Figure 3.

![Figure 3. Results of the analysis of precedent studies.](chart)

First, if protection measures are executed centering on the built-in area that distinguishes the inside from the outside of an organization, the protection measures must focus on the organization’s existing information regarding the outflow of technical information. In addition, after the occurrence of a conventional technical information leakage incident, protection measures mainly focus on the use of the security system. For example, among the program management controls of NIST 800-53 [4], the 15 controls focused on the security system except only 1 control, senior information security officer. Similar to information system inventory, threat awareness program are focused on security system. Moreover, the standard systems consider security of organization’s territory. The contents of enterprise architecture control, critical infrastructure plan control are restricted to the organization’s boundary. However, to implement these protection measures, it is necessary to both categorize and evaluate the organization’s critical data to perform security activities. Third, protection measures focused on building existing security systems should be changed; instead, focus should be placed on the actions of organizational members. Thus, the security awareness of staff members must be improved and a digital trace analysis method for all staff members must be applied. Finally, the existing control center should adopt the protection measures of the recovery center to ensure the resilience of the organization after a technical information leakage incident, thus establishing the company’s business continuity plan (BCP) and creating a system of prevention and recovery from potential threats. Generally, security incidents are hard to recognize when an incident occurs [10,11]. If leakage incidents occur, it is hard for
the organization to know which information was leaked. So, the recovery time is very long and it is hard to recover normal operation.

We designed a control that evaluates the security level of an organization based on technical information of leakage incidents that can meet the security requirements based on the analysis results of previous studies; in other words, the security evaluation controls were collected with reference to previous research. Prior to analysis, precedent research regarding insider threats was selected; among the works, papers including evaluation items containing the possible evaluation of security level were selected for the performance of the analysis. The collected security evaluation controls are shown in Table A1 in Appendix A. A total of 26 security evaluation controls were derived from 23 prior studies, and the content of the evaluation controls described in these previous studies is shown in Table A1. In addition, the degree of commonality of the security evaluation controls in 23 prior studies is shown. The security evaluation control with the highest degree of commonality is “security level of personal computer,” with a share of 82.61%, reflecting that the security of insiders’ personal computers—where technical information is produced and distributed in the form of electronic files—is an important factor in the assessment of the security level of an organization. The security control with the lowest degree of commonality is “authentication of security management system,” with a share of 4.35%; this is mentioned only in one of the 23 previous studies.

4. Validation of the Security Evaluation Model for Information Leakage Protection

4.1. Statistical Validation of the Security Evaluation Model for Information Protection

In this research, an expert survey was conducted to verify the suggested model. The questionnaire was administered to 109 security experts who had experience of leakages of technical information. We conducted the survey over three months, both online and offline. The survey included questions regarding whether the controls suggested in this model are appropriate as items of a security evaluation model from the perspective of insiders and statistical analysis methods, which were applied according to the results of the survey. We then proceeded with validity, factor selection, and reliability validation. We used the statistical analysis tool SPSS Statistics 26 for statistical validation. For the statistical validation procedure, the validity was checked through the questionnaire fit, and the factor analysis was performed based on the validated controls. Factor analysis was used to measure the theoretical variables and could show the general direction of reliability, convergence validity, and discriminant validity of different controls. Using principal component analysis as the extraction method, the rotation method used was the varimax rotation method—a right-angle rotation method that achieves simplicity and clear interpretation between factors. We showed that the average value of each influencing factor (i.e., the validity of the standard) was 3.5 or more, which is suitable as a security evaluation control for preventing the leakage of technical information. The result of validity is as shown below in Table 2.

| ID | Controls                                                                 | Degree of Validity |
|----|--------------------------------------------------------------------------|--------------------|
| A  | Regulatory requirements of the industry                                  | 4.69               |
| B  | Degree of participation of management in security education              | 4.23               |
| C  | Degree of support for security organization by management                | 4.25               |
| D  | Practical security activities for security personnel                     | 4.31               |
| E  | (Considering security of the general staff) Degree of discomfort (security acceptability) | 4.13               |
| F  | Allocation of work to security personnel (installation of security department) | 4.54               |
| G  | General employee security management (security pledge and security training) | 4.48               |
| H  | Amount of investment in technology protection (security manpower + security education + security consulting + introduction and operation of the security system) | 4.49               |
Table 2. Cont.

| ID | Controls                                                                 | Degree of Validity |
|----|-------------------------------------------------------------------------|--------------------|
| I  | Research asset security management (e.g., researcher security pledge and research content security management) | 4.52               |
| J  | Joint (trust) research security management (e.g., consignor of the security contract and security activity check) | 4.41               |
| K  | Identification and evaluation of the importance of the research results  | 4.32               |
| L  | Research results (performance management)                                 | 4.41               |
| M  | Improvement of the research environment for researchers (e.g., regularization of researchers and operation of compensation for job incentives) | 4.45               |
| N  | Security zone (equipment) setup and management                            | 4.45               |
| O  | Security system introduction and utilization (access control + intrusion alarm + image detection) | 4.41               |
| P  | Security level of personal computer                                      | 4.61               |
| Q  | Server security (e.g., user authentication, management of (shared folder) access rights and updating versions) | 4.62               |
| R  | Database security (e.g., user authentication, version updating, security system introduction, and operation (access control + encryption)) | 4.63               |
| S  | Computer network security (e.g., user authentication, management of access rights, and security system introduction and operation (network access control (NAC))) | 4.58               |
| T  | Supply chain security (service security) guidelines and implementation    | 4.32               |
| U  | Guidance and implementation of production process security (prevention of work interruption and information leakage) | 4.23               |
| V  | Degree of internal security audit activity                               | 4.24               |
| W  | Efforts to improve the security system through analysis of cases of excellent external security | 4.10               |
| X  | Acquisition of objectified security certification by a third party (e.g., ISO 27001 certification, Korea-Information Security Management System (KISMS) certification) | 4.13               |
| Y  | System failure response activities (e.g., business continuity planning, system redundancy, and backup) | 4.42               |
| Z  | Measures to cope with technology leakage incidents (e.g., incident response plan, measures to prevent recurrence of accidents, and analysis of the causes of an accident) | 4.45               |

We conducted an exploratory factor analysis for the security evaluation controls that ensured conformance validity, and a total of eight factors were derived as a result of the factor analysis. In order to verify the reliability of each influencing factor, the reliability of the multi-control scale was analyzed by the Cronbach α coefficient. The Cronbach α coefficient is most often used to provide a more conservative value than other evaluation coefficients and to verify reliability (with consistent measurement accuracy for the same concept) [15]. The reliability of the influencing factors used in the empirical analysis of this study met the criterion of 0.7 or higher, as shown in Table 3 [16]. As a result, we confirmed the convergence and discriminant validity through factor analysis. The green shades in Table 3 represent the result of factory analysis. And the green shades also represented values of grouped by the same factor.

The security evaluation model from the perspective of technology leakage prevention through statistical validation is the same as shown in Figure 4 below. The evaluation controls of “industry legal requirements and regulations” were not classified into factors. The evaluation control of “legal requirement regulation by industry” is classified as a single factor. So, the control was rejected. However, the “Security culture” and “Managerial security system” factors can include the content of legal requirements.
Table 3. Results of the factor analysis.

| Controls  | 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8    | Cronbach's α |
|-----------|------|------|------|------|------|------|------|------|--------------|
| K         | 0.882 | 0.095 | -0.009 | -0.029 | 0.043 | -0.049 | 0.020 | 0.047 | 0.992        |
| L         | 0.872 | 0.033 | 0.007 | 0.024 | -0.015 | 0.223 | -0.032 | 0.147 | 0.890        |
| I         | 0.840 | 0.012 | 0.156 | 0.063 | -0.069 | 0.169 | 0.071 | -0.043 | 0.989        |
| J         | 0.799 | 0.131 | 0.019 | 0.144 | 0.008 | 0.311 | 0.022 | 0.136 | 0.880        |
| M         | 0.794 | 0.125 | -0.073 | -0.091 | -0.097 | -0.043 | 0.084 | 0.224 | 0.906        |
| B         | 0.204 | 0.908 | 0.130 | 0.077 | 0.146 | -0.016 | 0.034 | -0.036 | 0.909        |
| C         | 0.172 | 0.898 | 0.043 | 0.039 | 0.221 | 0.098 | -0.005 | 0.042 | 0.908        |
| E         | 0.003 | 0.882 | 0.142 | 0.050 | -0.013 | 0.131 | -0.002 | 0.044 | 0.922        |
| D         | 0.264 | 0.843 | 0.047 | 0.143 | 0.190 | 0.138 | 0.006 | 0.035 | 0.942        |
| Q         | -0.050 | 0.087 | 0.918 | 0.190 | 0.026 | 0.043 | -0.021 | -0.018 | 0.839        |
| R         | 0.049 | 0.091 | 0.865 | 0.147 | -0.017 | 0.092 | 0.031 | -0.061 | 0.799        |
| P         | 0.045 | 0.222 | 0.840 | 0.141 | 0.053 | -0.049 | -0.020 | -0.153 | 0.831        |
| S         | 0.023 | -0.045 | 0.720 | -0.026 | 0.162 | 0.271 | 0.227 | 0.096 | 0.904        |
| W         | -0.032 | 0.076 | 0.163 | 0.931 | 0.098 | 0.016 | 0.018 | -0.016 | 0.927        |
| X         | 0.028 | 0.022 | 0.170 | 0.924 | 0.092 | 0.064 | 0.023 | 0.116 | 0.933        |
| V         | 0.077 | -0.012 | 0.089 | 0.824 | -0.092 | 0.116 | 0.120 | 0.058 | 0.920        |
| F         | 0.015 | 0.121 | 0.072 | -0.047 | 0.908 | 0.018 | 0.033 | 0.024 | 0.802        |
| G         | 0.052 | 0.125 | 0.072 | 0.105 | 0.898 | 0.099 | -0.025 | 0.065 | 0.794        |
| H         | -0.078 | 0.187 | 0.129 | 0.008 | 0.807 | 0.016 | -0.034 | 0.198 | 0.876        |
| T         | 0.276 | 0.113 | 0.058 | 0.016 | 0.134 | 0.848 | 0.252 | 0.059 | 0.930        |
| U         | 0.264 | 0.178 | 0.170 | 0.079 | 0.119 | 0.809 | 0.226 | 0.024 | -          |
| A         | -0.021 | 0.116 | 0.083 | 0.470 | -0.127 | 0.574 | -0.146 | -0.004 | -          |
| O         | 0.064 | 0.022 | 0.072 | 0.053 | -0.017 | 0.073 | 0.080 | -0.020 | 0.939        |
| N         | 0.035 | -0.002 | 0.111 | 0.051 | -0.014 | 0.191 | 0.925 | 0.059 | 0.917        |
| Z         | 0.211 | -0.005 | -0.065 | 0.060 | 0.133 | 0.005 | -0.002 | 0.939 | -          |
| Y         | 0.203 | 0.069 | -0.072 | 0.088 | 0.143 | 0.067 | 0.043 | 0.921 | -          |

Figure 4. The proposed security evaluation model.

4.2. Proposal of an Objective Measurement for the Electronic Security System

Our study proposed an objective measurement for the evaluation of the “electronic security system” control in order to determine the security level that ensures objectivity. Detailed contents of the objective evaluation in the areas of “electronic security system” are described in Figure 5.
Figure 5. The range of objective evaluation.
Among the proposed models, only the electronic technology security system was conducted with the listed criteria. The objective security measurement proposed in our research was based on usage records by using a digital forensic technique when confirming the security level of the organization’s IT assets. Since it is difficult to ensure the objectivity of the evaluator, the security measurement of the digital trace analysis, which applies the digital forensics technique, was advanced only for IT assets that had a reliable digital trace. Thus, it was expected that the security evaluation results could be assured, and the actual business process-based security level could be measured, instead of confirming the fragmentary security level, on the evaluation day. Therefore, we measured the security level of the personal computers, as well as the computer networks of the IT assets used in the feasibility study. For the confirmation of the items of the objective evaluation, we applied digital forensics, the digital trace of which is shown in Table 4. For the e-mail (P2P messenger) items, we failed to generalize the routes’ digital traces, since the characteristics of e-mail systems and e-mail servers vary for each organization.

Table 4. The route of the hive file for objective evaluation.

| Type                        | Hive File Path                                                                 |
|-----------------------------|-------------------------------------------------------------------------------|
| Operating System            | Check on user password setting (Encryption set-up + change period)            |
|                             | HKLMSAM                                                                       |
|                             | Check on complexity of user authentication method (Electronic signature + biometric) |
|                             | HKCU\SOFTWARE\Classes\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache |
|                             | Check on updated version of Operating System (Check on updated security patch) |
|                             | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace |
|                             | Check on security system installation                                        |
|                             | HKCU\SOFTWARE\Classes\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache |
|                             | Check on security system uninstallation trace                                  |
|                             | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall       |
| Portable storage device     | Check on portable device connection trace                                     |
|                             | SYSTEM\ControlSet00x\Enum\USBSTOR                                            |
|                             | Check on fixed storage device (hard disk driver, compact disk)                |
|                             | SYSTEM\ControlSet00x\Enum\USBSTOR                                            |
|                             | Check on updated version of application program (Driver)                      |
|                             | SYSTEM\ControlSet00x\Enum\ROOT\XKmdfDriver\0000                             |
|                             | Check on security system installation                                        |
|                             | HKCU\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache |
|                             | Check on security system uninstallation trace                                  |
|                             | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall       |

Accordingly, a route for the hive file regarding detailed items of the operating system and portable storage device—with e-mail (P2P messenger) excluded—was organized as shown in Table 4 above. The hive file is a file that can identify a computer’s digital traces and the log value and can also identify the value of a digital trace by accessing each route [17]. This route was surveyed by targeting a PC that used the Windows operating system and had a valid value in Windows 10.1809 build version.

The checked value for each detailed item is as follows. The detailed diagnostic controls of the personal computer were configured as an operating system (OS), e-mail (e-mail and P2P messenger), and portable storage device. In the OS control, user authentication was performed using the checking of user password setting, the latest version of OS, and latest security patch to diagnose the latest story (software update) of the environment. In addition, we checked the traces of the security system installation and uninstallation. The diagnostic controls for portable storage device could be checking the traces of storage device connections, checking fixed storage devices such as hard disk driver and compact disk, and checking the latest version of the application (driver) and traces of the installation...
and uninstallation of the security system. This study’s method of measuring feasibility used digital forensics tools; however, for some evaluation controls, a database against which the evaluation results must be compared has not been established, and these were thus manually confirmed.

4.3. The Results of Feasibility Test in Objective Measurement for the Electronic Security System

We proceeded with a feasibility study based on the security evaluation model for the protection of the proposed technology, and we attempted to verify the adequacy of the application for the actual corporate environment. The feasibility study period was from 20 November 2017 to 4 December 2017. The target company was a medium-sized Korean manufacturing enterprise with 200 employees. The survey was conducted on personal computers used in the business of the surveyed companies. As shown in Table A2 in Appendix A, we checked that the five detailed controls were not observed. The main contents of the digital trace analysis using the digital forensic tool are shown in Figure 6 below. First, the control “checked on security system installation” checked that the program was installed and evaluated normally. Second, the control “checked on portable device connection trace” was abnormally evaluated by checking the connection trace of 20 storage devices.

5. Results and Discussion

As the results on this study, we derived a security evaluation model. For the model proposal, we analyzed precedent research about security evaluation standard and the model focused on insider threat. The proposed model has 26 detailed controls focused on insider threat. Afterwards, through expert survey, we statistically proved the model. The survey included questions regarding whether the controls suggested in this model were appropriate as items of a security evaluation model from the perspective of insiders. Moreover, we proposed an objective measurement method. We checked the applicable the proposed method, through feasibility test.
From the perspective of preventing the leakage of technical information in this research, the security evaluation model comprised the evaluation of the information of security requirements derived through analysis of previous research, which were business continuity, digital evidence, information classification and security culture. We derived a security evaluation model for the prevention of the leakage of technical information through both the administration of questionnaires to security experts and a demonstration case. Table 5 shows the detailed evaluation controls and factors that reflected the security requirements. First, we met the requirements of the business continuity such as business continuity plan by implementing a security system failure response and an information leakage incident response through the “Security change management” factor. Second, the “Electronic security system” factor was subjected to a digital trace analysis through digital forensics techniques to meet the “digital evidence” requirement. Third, the “Classification of developed technology” factor allowed the identification and management of assets to meet the “information classification” requirement. Finally, due to the “Security culture” factor, it was possible to meet the requirements of “security culture” by developing the security awareness of management and internalizing the receptivity of general employees.

Table 5. The proposed security evaluation model focused on insiders.

| Type                                      | Controls                                      | Requirement for Evaluation Model Focused on Insider |
|-------------------------------------------|-----------------------------------------------|----------------------------------------------------|
| Measuring and improving security level    | Degree of internal security audit activity    |                                                    |
|                                           | Acquisition of objectified security certification by a third party (e.g., ISO 27001 certification and Korea-Information Security Management System certification) |                                                    |
|                                           | Efforts to improve security system through analysis of cases of excellent external security |                                                    |
| Security change management                | System failure response activities (e.g., business continuity planning, system redundancy, and backup) | Business continuity plan                           |
|                                           | Measures to cope with technology leakage incidents (e.g., incident response plan, measures to prevent recurrence of accidents, and analysis the causes of an accident) |                                                    |
| Incident response                         | Security zone (equipment) setup and management |                                                    |
|                                           | Security system introduction and utilization (access control + intrusion alarm + image detection) |                                                    |
| Physical security system                  | Security level of personal computer           |                                                    |
|                                           | Server security (e.g., user authentication, management of (shared folder) access rights, updating versions) |                                                    |
| Security operation management             | Electronic security system                    |                                                    |
|                                           | Database security (e.g., user authentication, updating versions, security system introduction, and operation (access control + encryption)) |                                                    |
|                                           | Computer network security (e.g., user authentication, management of access rights, security system introduction and operation, and network access control (NAC)) |                                                    |
| Managerial security system                | Supply chain security (service security) guidelines and implementation |                                                    |
|                                           | Guidance and implementation of production process security (prevention of work interruption and information leakage) |                                                    |
By satisfying the security requirements for the derived evaluation controls, we established a security evaluation standard for organizations that focused on the prevention of the leakage of technical information. In addition, to meet the security requirements, we proposed a digital trace analysis using a digital forensics technique as a security measurement; thus, it was possible to secure the objectivity of the evaluation results. The conventional external attack showed the discrimination of the security level at the center of the evaluation control.

### 6. Conclusions and Future Work

We have two research questions, as follows. First, when designing the security evaluation model, what is the difference between focusing on outside attack and focusing on insider threat? Second, what is the evaluation method for objective security level evaluation? To solve the research question, our study developed a security level evaluation model to prevent the leakage of technical information and proposed a method of measuring the level at which the objectivity of some items was secured. To develop the evaluation model, we compiled 26 detailed evaluation items, considered the security requirements to prevent the leakage of technical information and referred to 23 previous studies. Through the subsequent questionnaire administered to 109 security experts, we performed conformity, reliability, and factor analyses and statistical validation, and ensured security level measurement for some evaluation items (e.g., “electronic technology protection system”). We proposed a research method and conducted a demonstration feasibility test.

### Table 5. Cont.

| Type                        | Controls                                                                 | Requirement for Evaluation Model Focused on Insider Threats |
|-----------------------------|--------------------------------------------------------------------------|------------------------------------------------------------|
| Security operation          | Research asset security management (researcher security pledge and research content security management) | Information classification                                  |
| management                  | Joint (trust) research security management (e.g., consignor of the security contract and security activity check) |                                                            |
|                             | Identification and evaluation of the importance of research results       |                                                            |
|                             | Research results (performance management)                                 |                                                            |
|                             | Improvement of the research environment for researchers (e.g., regularization of researchers and operation of compensation for job incentives) |                                                            |
| Security support            | Allocation of work to security personnel (installation of security department) |                                                            |
| environment                 | General employee security management (security pledge and security training) |                                                            |
|                             | Amount of investment in technology protection (security manpower + security education + security consulting + introduction and operation of the security system) |                                                            |
| Security culture            | Degree of participation of management education in security education      | Security culture                                           |
| Internal/External security  | Degree of support for security organization by management                 |                                                            |
| culture                     | Practical security activities for security personnel (Considering security of the general staff) |                                                            |
|                             | Degree of discomfort (security acceptability)                             |                                                            |
As security incidents and financial damage are increasing, our study’s contributions are as follows. First, our proposed model considered sustainable growth. This study minimizes the security threats which have an effect on an organization’s research, development, and profit. Second, we derived the weights of all controls. The weights were deduced by experts’ survey so the model has value at the business level. Third, the proposed measurement method solved the subjective evaluation problem. Fourth, through the results of security evaluation, the organizations make a decision to ensure security in investment. Lastly, this study is a first step in leakage protection diagnostic evaluation.

Future research should apply the proposed evaluation model to real industry groups considering industrial type and scale. Through the proposed measurement method, organizations could run periodic and automatic evaluation. As the computing environment changes, the proposed model could adopt new technology such as cloud computing and Internet of Things.

**Author Contributions:** Conceptualization, H.C.; methodology, H.C.; validation, J.K.; formal analysis, J.K.; investigation, C.L.; resources, C.L.; data curation, J.K.; writing—original draft preparation, J.K. and H.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703).

**Conflicts of Interest:** The authors declare no conflict of interest.
### Appendix A

**Table A1. Common derived security evaluation controls.**

| ID | Controls                                                                 | [18] | [19] | [20] | [21] | [22] | [23] | [24] | [25] | [26] | [27] | [28] | [29] | [30] | [31] | [32] | [33] | [34] | [35] | [36] | [37] | [38] | [39] | [40] |
|----|--------------------------------------------------------------------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| A  | Regulatory requirements of the industry                                  | •    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| B  | Degree of participation of management in security education             | •    | •    | •    | •    | •    | •    | •    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| C  | Degree of support for security organization by management               | •    | •    | •    | •    | •    | •    | •    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| D  | Practical security activities for security personnel                    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| E  | (Considering security of the general staff) Degree of discomfort (security acceptability) |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| F  | Allocation of work to security personnel (installation of security department) | •    | •    | •    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| G  | General employee security management (security pledge and security training) |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| H  | Amount of investment in technology protection (security manpower + security education + security consulting + introduction and operation of the security system) | •    | •    | •    | •    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| I  | Research asset security management (e.g., researcher security pledge and research content security management) |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| J  | Joint (trust) research security management (e.g., consignor of the security contract and security activity check) |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| K  | Identification and evaluation of the importance of the research results | •    | •    | •    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
Table A1. Cont.

| ID | Controls                                                                 | [18] | [19] | [20] | [21] | [22] | [23] | [24] | [25] | [26] | [27] | [28] | [29] | [30] | [31] | [32] | [33] | [34] | [35] | [36] | [37] | [38] | [39] | [40] |
|----|--------------------------------------------------------------------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| L  | Research results (performance management)                                | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| M  | Improvement of the research environment for researchers (e.g., regularization of researchers and operation of compensation for job incentives) | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| N  | Security zone (equipment) setup and management                           | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| O  | Security system introduction and utilization (access control + intrusion alarm + image detection) | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| P  | Security level of personal computer                                      | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Q  | Server security (e.g., user authentication, management of (shared folder) access rights, and updating versions) | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| R  | Database security (e.g., user authentication, version updating, security system introduction, and operation (access control + encryption)) | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| S  | Computer network security (e.g., user authentication, management of access rights, and security system introduction and operation (network access control (NAC)) | ⬤    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| T  | Supply chain security (service security) guidelines and implementation    | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| U  | Guidance and implementation of production process security (prevention of work interruption and information leakage) | ⬤    | ⬤    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |

---
| ID | Controls | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
|----|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| V  | Degree of internal security audit activity | • |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|    | Efforts to improve the security system through analysis of cases of excellent external security |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| W  | Acquisition of objectified security certification by a third party (e.g., ISO 27001 certification and Korea-Information Security Management System (KISMS) certification) |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| X  | System failure response activities (e.g., business continuity planning, system redundancy, and backup) |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Y  | Measures to cope with technology leakage incidents (e.g., incident response plan, measures to prevent recurrence of accidents, and analysis of the causes of an accident) |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
Table A2. Results of the feasibility study.

| Controls                     | Sub-Controls                                                                 | Result |
|------------------------------|------------------------------------------------------------------------------|--------|
| Operating system (OS)        | Check on user password setting (Encryption set-up + change period)           | ○      |
|                              | Check on complexity of user authentication method (Electronic signature + biometric) | ○      |
|                              | Check on updated version of Operating System (OS)                            | ○      |
|                              | Check on updated security patch                                              | ○      |
|                              | Check on security system installation                                        | ○      |
|                              | Check on security system uninstallation trace                                 | ○      |
| Personal Computer            | Check on usage trace of mail on business (Sent offsite)                      | X      |
| E-mail (P2P messenger) only use own e-mail program                           | Check on updated version of application program                             | X      |
|                              | Check on security system installation                                        | -      |
|                              | Check on security system user authentication (Delete-Change on account + password change period) | -      |
|                              | Check on security system uninstallation trace                                 |        |
| Portable storage device      | Check on portable device connection trace                                     | X      |
|                              | Check on fixed storage device (hard disk driver, compact disk)               | ○      |
|                              | Check on updated version of application program (Driver)                     | -      |
|                              | Check on security system installation                                        | ○      |
|                              | Check on security system uninstallation trace                                 | ○      |

- symbol: Some (security) program databases, when compared to digital evidence, have not been built. So, we could not check the controls using digital evidence.

References

1. Wong, W.P.; Tan, H.C.; Tan, K.H.; Tseng, M.L. Human factors in information leakage: Mitigation strategies for information sharing integrity. *Ind. Manag. Data Syst.* 2019, 119, 1242–1267. [CrossRef]
2. Crowd Research Partners. *Insider Threat 2018 Report*; Haystax: Kansas, MO, USA, 2018.
3. Gontar, A.A.; Lomakin, N.I.; Gorbacheva, A.S.; Chekrygina, T.A.; Tokareva, E.V. Methods of data intellectual analysis in assessment of economic security level. In *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*; Springer: Cham, Switzerland, 2019; pp. 455–464.
4. *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST Special Publication 800-53 Revision 4; Joint Task Force Transformation Initiative; National Institute of Standards and Technology: Boulder, CO, USA, 2014.
5. Liggett, R.L. The Effects of Information Security on Business Continuity: Case Study. Ph.D. Thesis, University of Phoenix, Phoenix, AZ, USA, 2020.
6. Council of the European Union. *General Data Protection Regulation*; Council of the European Union: Brussels, Belgium, 2016.
7. Na, O.; Park, L.W.; Yu, H.; Kim, Y.; Chang, H. The rating model of corporate information for economic security activities. *Secur. J.* 2019, 32, 435–456. [CrossRef]
8. Yassin, W.M.; Ahmad, R.; Mohammad, N.A.N. An Insider Threat Factors and Features Categorization for Manufacturing Execution System. In *Advances in Electronics Engineering*; Springer: Singapore, 2020; pp. 329–337.
9. Azaria, A.; Richardson, A.; Kraus, S.; Subrahmanian, V.S. Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. *IEEE Trans. Comput. Soc. Syst.* 2014, 1, 135–155. [CrossRef]
10. Suman, R.; Far, B.; Mohammed, E.A.; Nair, A.; Janbakhsh, S. Visualization of Server Log Data for Detecting Abnormal Behaviour. In Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, USA, 7–9 July 2018; pp. 244–247.
11. Parrot, A.; Bechhofer, L. *Acquaintance Rape: The hidden Crime* (No. 157); Wiley: New York, NY, USA, 1991.
12. EKRAN. *Insider Threat Statistics for 2020: Facts and Figures*; EKRAN: Newport Beach, CA, USA, 2019.
13. Moon, S.J. A Study on Security Level Assessment Methodology Development for Internal Information Leakiness Control: Centering on National & Public Agency. Master’s Thesis, Department of Business Administration Graduate School of Business Administration, Chosun University, Gwangju, Korea, 2008.

14. Drtil, J. Impact of information security incidents—Theory and reality. *J. Syst. Integr.* 2013, 4, 44–52.

15. Bland, J.M.; Altman, D.G. Statistics notes: Cronbach’s alpha. *BMJ* 1997, 314, 572. [CrossRef]

16. Corbett, R.J.T.; Loptook, A.R.; Nunnally, R.L.; Hassan, A.; Jackson, J. Intracellular pH, lactate, and energy metabolism in neonatal brain during partial ischemia measured in vivo by 31P and 1H nuclear magnetic resonance spectroscopy. *J. Neurochem.* 1988, 51, 1501–1509. [CrossRef]

17. Kim, J.S.; Eun, C.; Jeong, I.Y. Automatic user analysis using artifact of Windows environment. In Proceedings of the Symposium of the Korean Institute of communications and Information Sciences, Jeju Island, Korea, 21–23 June 2017; pp. 1437–1438.

18. Han, D.-S. Proposal of information security management system specialized in industrial security. *Korea Ind. Saf. Res.* 2016, 6, 143–172.

19. Ministry of Trade, Industry and Energy; Korea Industrial Technology Protection Association. *Industrial Technology Protection Guidelines and Manuals*; Ministry of Trade, Industry and Energy: Seoul, Korea, 2017.

20. Chang, H.-B. Design of information security management system for prevention of industrial technology leakage in small and medium business. *J. Korea Multimed. Soc.* 2010, 13, 111–121.

21. Bae, S.; Kim, J.H. A study on the development of security level evaluation model for national R & D project research. *J. Korea Comput. Assoc.* 2013, 16, 73–80.

22. Choi, M.-G.; Lee, D.H.; Hwang, W.J. Design of security protocol for collaborative workflow management system. *J. Korea Acad. Ind. Cooper. Soc.* 2008, 9, 1271–1278.

23. Korea Federation of SMEs. 2016 SME Technical Statistics Survey Report; Korea Federation of SMEs: Seoul, Korea, 2016.

24. Korea Federation of SMEs; Large and Small Enterprises Cooperation Foundation. 2016 Survey of Technical Protection Level of SMEs; Korea Federation of SMEs: Seoul, Korea, 2017.

25. Mbowe, J.E.; Zlotnikova, I.; Msanjila, S.S.; Oreku, G.S. A conceptual framework for threat assessment based on organization’s information security policy. *J. Inform. Secur.* 2013, 5, 166–177. [CrossRef]

26. Shamala, P.; Ahmad, R.; Yusoff, M. A conceptual framework of info structure for information security risk assessment (ISRA). *J. Inf. Secur. Appl.* 2013, 18, 45–52. [CrossRef]

27. Laura, S. Cyber Security Assessment Tool. *Nuclear Plant. J.* 2016, 34, 43–45.

28. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* 2016, 56, 1–27. [CrossRef]

29. Kim, I.-H.; Lee, K.H. Evaluation model of contractor security management using DEA model. *J. Korea Inst. Inf. Secur.* 2017, 27, 687–704.

30. Noh, S.Y.; Lim, J.I. A study on corporate security management system. *J. Korea Inst. Inf. Secur.* 2016, 26, 541–550.

31. Park, G.; Yeom, H.Y. A Study on the improvement of information protection level of electronic financial infrastructure: Through the analysis of information security management level. *J. Korea Inst. Inf. Secur.* 2016, 26, 1605–1618.

32. Kotenko, I.; Chechulin, A. Fast network attack modeling and security evaluation based on attack graphs. *J. Cyber Secur.* 2014, 3, 27–46. [CrossRef]
37. Stouffer, K.; Falco, J.; Scarfone, K. *Special Publication 800-82 Revision 1, Guide to Industrial Control. Systems (ICS) Security*; National Institute of Standards and Technology: Gaithersberg, MD, USA, 2015.

38. US Department of Energy; Applied Communication Sciences; DTE Energy; Electric Power Research Institute; University of Illinois at Urbana-Champaign. *Tools & Methods for Hardening Communication Security of Energy Delivery Systems: Final Report*; Applied Communication Sciences; US Department of Energy: Basking Ridge, NJ, USA, 2014.

39. Galloway, B.; Hancke, G.P. Introduction to industrial control networks. *IEEE Commun. Surv. Tutor.* 2013, 15, 860–880. [CrossRef]

40. Soh, W.Y.; Kim, W.K.; Kim, S.S. Development of security level evaluation tool (ISSPET) based on information protection system. *J. Korea Acad. Ind. Coop. Soc.* 2009, 10, 1911–1919.

**Publisher’s Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).