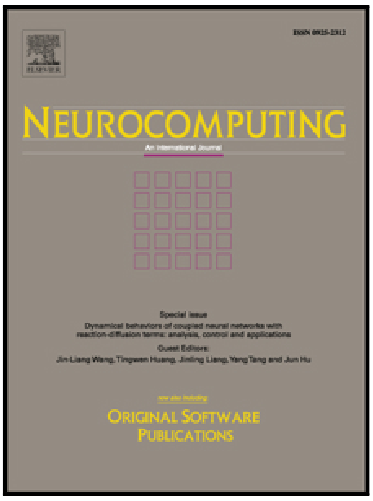


Performance Evaluation of the Recommendation Mechanism of Information Security Risk Identification

Yu-Chih Wei, Wei-Chen Wu, Ya-Chi Chu

PII: S0925-2312(17)31780-0
DOI: 10.1016/j.neucom.2017.05.106
Reference: NEUCOM 19086

To appear in: *Neurocomputing*

Received date: 6 September 2016
Revised date: 2 April 2017
Accepted date: 31 May 2017

Performance Evaluation of the Recommendation Mechanism of Information Security Risk Identification

Yu-Chih Wei[a], Wei-Chen Wu[b], Ya-Chi Chu[a]

[a] *Telecommunication Laboratories, Chunghwa Telecom Co., Ltd, Taoyuan, Taiwan, R.O.C*
[b] *Computer Center, Hsin Sheng Junior College of Medical Care and Management, Taoyuan, Taiwan, R.O.C*

Abstract

In recent decades, information security has become crucial for protecting the benefits of a business operation. Many organizations perform information security risk management in order to analyze their weaknesses, and enforce the security of the business processes. However, identifying the threat-vulnerability pairs for each information asset during the processes of risk assessment is not easy and time-consuming for the risk assessor. Furthermore, if the identified risk diverges from the real situation, the organization may put emphasis on the unnecessary controls to prevent the non-existing risk. In order to resolve the problem mentioned above, we utilize the data mining approach to discover the relationship between assets and threat-vulnerability pairs. In this paper, we propose a risk recommendation mechanism for assisting user in identifying threats and vulnerabilities. In addition, we also implement a risk assessment system to collect the historical selection records and measure the elapsed time. The result shows that with the assistance of risk recommendations, the mean elapsed time is shorter than with the traditional method by more than 21 %. The experimental results show that the risk recommendation system can improve both the performance of efficiency and accuracy of risk identification.

Keywords: Threat, Vulnerability, Risk Recommendation, Security

Email addresses: `vickrey@cht.com.tw` (Yu-Chih Wei), `wwu@hsc.edu.tw` (Wei-Chen Wu), `gyh2211@cht.com.tw` (Ya-Chi Chu)

1. Introduction

More and more organizations rely on information technology to assist them in achieving their business goals such as faster service response or better quality. However, focusing on ease of use in terms of system configuration and operation makes systems more vulnerable and easily compromised. This is why information security is of paramount importance to organizations. A systematic approach for information security risk management is necessary to help identify information security requirements and to create an effective management system. Risk is the effect of uncertainty on objectives, and information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood of occurrence [1]. The object for assessment also called information asset, which means anything that has value to organization. It is noting that information asset of an information system consists of more than hardware and software [1]. In this paper, we classify the information asset into five categories: hardware, software, people, information and service. Risk assessment, both the process and associated techniques, offers an analytical and structured walk-through of the organization's security state [2]. Risk identification is an important step in risk assessment, to determine what could cause a potential loss, and to gain insight into how and why the loss might happen. Thus, if a corporation expects to perform risk assessment successfully, finding the appropriate threat-vulnerability pair of each asset is a crucial step. However, in the process of identifying threat-vulnerability pairs, it is difficult for the risk assessor, especially one who lacks information security competence, to recognize the feasible combinations.

Without the support of a recommendation system, a risk assessor may encounter at least three challenges: First, in spite of the threat and vulnerability list being provided as a candidate list for risk assessors, it is still time-consuming to choose the appropriate one from more than a hundred combinations. Second, the threat-vulnerability pairs may be irrational if the root cause is not considered discreetly. For example, a physical server appliance may have some vulnerability due to the lack of physical protection. Theoretically, environmental damage and physical breakage are reasonable threats. However, a mistake may be made when people choose another irrational threat such as ”insufficient software testing”. Third, not all the users have the ability to find the security issue for the information asset, and may choose non-existing risks. Non-existing threat-vulnerability pairs may make organizations spend unnecessary time and money to prevent a risk that may not happen, which may lead the manager to neglect the real weaknesses, or invest in improper security measures.

There are a number of information risk assessment approaches that have been proposed. These methods of identifying threats and vulnerabilities are based on the International Organization for Standardization (ISO) stands, such as ISO 31000:2009 [3], ISO/IEC 27001:2013 [4] and ISO/IEC 27005:2011 [1]. Stølen presented a risk assessment model called CORAS [5], which uses a threat diagram and structured brainstorming to analyze risks. These methods are always performed with expert guidance and may take too much time to complete. Some researchers have identified threats and vulnerabilities according to the security requirements, such as OCTAVE [6], which only addresses the security requirements of information asset onlys but lacks comprehensive consideration. Another mechanism uses business processes to complete the risk assessment [7]. However, in their work, it is hard for common users to determine each asset’s risk on their lifecycle. In addition, other researchers [8] identify risk by building a security ontology. However, it is complicated for users who lack of security knowledge and also impossible to build on their own. There are still some researchers who recommend threats or vulnerabilities for users, but this only suitable for specific domains, such as cloud computing [9].

Due to the deficiencies mentioned above, we propose a recommendation approach for risk identification iterations to resolve the problem. In this paper, the asset category is classified after the asset identification step. By the use of a data mining technique, the threat-vulnerability pairs for each asset category were identified by the predictive aprori algorithm and provided as a recommendation list. The risk assessor can choose the appropriate pairs that correspond to the real encountered problems from the recommendation list. The main contribution of our proposed approach is to improve the efficiency and accuracy of identifying the threat-vulnerability pairs. In order to evaluate the performance of the efficiency improvement, we first invited information experts to evaluate the accuracy of the threat-vulnerability pairs on the recommendation list. In addition, we designed a risk assessment system that can provide the recommendations of threat-vulnerability pairs for the risk assessor, and can measure the elapsed time of the risk assessor's selections.

The remainder of the paper is organized as follows: Section 2 describes relevant research on risk assessment and the problems in the past. Section 3 presents our research model, which recommends threat-vulnerability pairs for different categories of asset. Section 4 contains the experimental design and results. Conclusions and future directions are given in Section 5.

2. Related work

The international standards on information security risk assessment, such as ISO/IEC 27005:2011 [1] and NIST SP800-30 [10] , not only form the basis of the general information security risk assessment standard framework but also enable the development of risk assessment approaches. However, they may not explicitly provide suggestions of the potential threat and vulnerability for each asset. In the risk identification phase, the threats and vulnerabilities must be identified by a risk assessor through brainstorming, questionnaires or other technical tools. This may take too much time and not intuitive for users.

Other existing risk assessment mechanisms such as CORAS [5], OCTAVE [6], and CRAMM [11] also propose their own methods of risk assessment based on standards. In CORAS, a Platform for Risk Analysis of Security Critical Systems is proposed. It uses threat and vulnerability modeling along with threat diagrams and structured brainstorming to identify risks. These approaches suggest some common security principles or security best practices. However, they do not determine and evaluate the specific security needs of assets to identify their risks. The other approaches, such as OCTAVE, determine the criticality and impact of vulnerabilities from the review of security requirements. OCTAVE considers the possible conditions or situations that could threaten an organization's information assets using existing security checklists, standards or brainstorming. Although OCTAVE uses security requirements, they only determine the impact of the vulnerabilities of security requirements or the requirements of a product; Asset unspecific security standards can also be used.

CRAMM is a qualitative risk analysis and management tool developed by the British government organisation the Central Computer and Telecommunications Agency in 1985 to provide government departments with a method for information system security reviews. CRAMM is currently in version 5, which has three stages including: identification and valuation of assets, threat and vulnerability assessment, and countermeasure selection and recommendation. CRAMM computes the risks for each group of assets versus the threats to which the are vulnerable on a scale of 1 to 7, utilizing a risk matrix with the default values by comparing it with the activity level of threat and vulnerability [11]. The necessary data for the risk assessment is collected via interviews with stakeholders. In [2], Shamala et al. considered aforementioned risk assessment methodologies, and provide a conceptual framework of info-structure ISRA was provided. They concluded that any organization must ensure that the details, including management requirements, organizational context, threats and vulnerabilities of assets, and risk management improvement, are gathered accurately.

In addition to the models mentioned above, there are some models that use different ways to identify risks. AURUM is an ontology-based method [12]. It helps the decision maker to answer the following questions: Which threats threaten critical assets? Which threat is a multiplier? Which vulnerabilities have to be exploited by a threat to become effective? Additionally, it shows the potential threat of selected asset by threat tree. For each threat highly granular vulnerabilities, which a threat could exploit, have been modeled in the ontology. All the threats AURUM provided are recommended from standard, and may lack of flexibility to adapt the new information technology. Furthermore, it is complicated for users to build new ontology on their own. Webb et al.[13] presented situation aware information security risk management (SA-ISRM) process model that can be used to facilitate improved situation awareness in information security risk management. Using an intelligence-driven process, it provides accurate, relevant, and complete information in a timely manner to enable quality decision-making. However, the whole risk management process is complicated; it is not easy to consider all the elements without system implementation.

3. Risk pair recommendation mechanism

In [1], the information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist. In addition, it also including identifies the existing controls and their effect on the risk identified, determines the potential consequences. Finally, prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment. In this paper, we focus on risk identification, which is to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen. A threat is the potential to harm assets. The presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it [1]. We call the combination pair of threat and vulnerability as threat-vulnerability pair. The processes to find the threat-vulnerability pairs for each asset are shown in Fig. 1. We will describe each step in the remaining subsections.

3.1. Asset collection and classification

In this paper, in order to produce a high-qualify threat-vulnerability recommendation list, the original data source were collected from the business

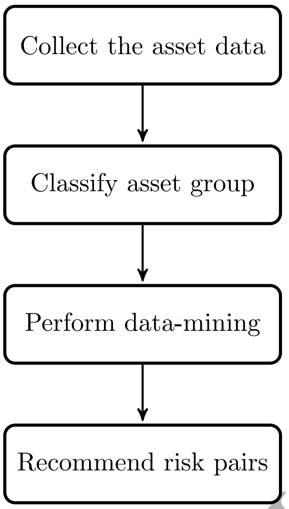


Figure 1: The procedure of the proposed risk pair recommendation mechanism.

units in the same organization, which was certified as compliant with ISO/IEC 27001:2013. The threat- and vulnerability- list, which was provided to the risk assessor, contained hundreds of items. All the threats and vulnerabilities were extended from ISO/IEC 27005:2011. We collected many information assets, and each asset had several threat-vulnerability pairs.

Information assets can be classified into a number of categories, such as hardware, software, people, etc [1]. Therefore, we classified the information assets into five categories: hardware, software, people, information and service. In addition,we classified several groups with similar functioning similar for each category of information assets. For example, Ubuntu and Open Office are both belong to the software category. However, they play different roles in system operation. Ubuntu is a kind of operation system software, and Open Office is a kind of package software. Due to their different functions, we established the operation system group and package software group respectively. Ubuntu belongs to the operation system, and Open Office belongs to the package software group. In this paper, we created many groups in each category, as shown in Table 1.

Table 1: Illustration of the groups of asset categories

Hardware	Software	Information	People	Service
Web server	Operation system	SOP	System manager	Electric service
Application server	Application program	Installation manual	Network manager	Air conditioning
Database server	Application system	User manual	Security manager	Network service
Log server	Development tool	Operation manual	Help desk	MIS
Personal computer	Package	Planning	Operator	Email service
Laptop	Network tool	Design document	DBA	VPN service
Network device	Compression tool	Testing report	System analyst	LDAP service
End point device	Audit tool	Contract	Quality manager	TeleCom
Printer	Analysis tool	Confidential consent	End point user	Security service
Scanner	Statistics tool	Audit report	Auditor	VPN
Storage equipment	Execution file	System log file	File manager	Maintenance service
Server room	Utility program	Parameter file	Supplier	LDAP
Office	Execution files	Database	Safeguard	Login service
Control room	Self-developed tool	Source code	Administrative	System operation

3.2. Mining the recommendation list

After classifying each information asset into a different group, each group contained many assets, and each asset contained several threat-vulnerability pairs, which were chosen by the risk assessor. For example, in Table 2, the risk assessor of end point device $PC01$ identified three threat-vulnerability pairs in $TID \in \{1, 2, 3\}$. However, the risk assessor of $PC02$ choose different pairs. It is worth noting that the list of threat-vulnerability pairs are not high dimensional data [14]. Therefore, we performed data mining to learn the association between the threats and vulnerabilities of each group. In this paper, in order to discover the threat-vulnerability pairs on the recommendation list, association rule mining was chosen. Association rule mining is a popular and well-researched methodology for discovering the interesting relations between variables. A typical and widely-used example of association rule mining is market basket analysis. The Waikato Environment for Knowledge Analysis (Weka) [15] is one of the most popular tools for performing data mining. It provides a general-purpose environment for data preprocessing, classification, regression, clustering, association rules and visualization. Using Weka can assist users in extracting useful information from data and enable them to easily identify a suitable algorithm for generating an accurate predictive model [16]. In this paper, three association rule mining algorithms including, Apriori, Predictive Apriori and Tertius, were used for evaluation. Eventually, Predictive Apriori had chosen due to the outstanding results.

Predictive Aprori can generate best n associate rule depending on the n selected by the user. It combines the standard confidence and support statistics into a single measure called Predictive Accuracy [17]. The *support* is used to measure the accuracy, and the $confidence$ can be counted by the number of transactions that match the rule. Essentially, the algorithm successively increases the support threshold because the value of predictive accuracy depends on it. Predictive Apriori can enable mining the potential association rules to fulfill the better performance even though the support value is not big enough.

In Weka, it only supports specific file formats, so before mining association rule, we must transform the original data from csv into arff. And then we choose Predict Apriori alogorithm, and the processes show below. First, we arrange the data of each group, and translate the file to ARFF form. Second, users can set the parameters provide by Weka GUI to find the results they want. Because Predictive Apriori algorithm aims to discovery of n most predictive association rules, we adopt the default settings. Finally, it may output the top n relevant rule in Weka. Take the end point equipment as an example, the top 10 association rules for the recommendation list are shown in Table 3.

4. Experiment & Evaluation

4.1. Evaluation

The data source of the historical threat-vulnerability selection record were collected from three business units in the same organization: billing operation, system management, and network management. These business units have been certified compliant with ISO/IEC 27001:2013, which illustrates that the risk

Table 2: Sample raw data of threat-vulnerability pairs of end point device

TID	*AssetID*	*Threat*	*Vulnerability*
1	PC01	Leak confidential information or programs	Lacking or inadequate of information security advocacy
2	PC01	Breach of organization law or contract	The lack of proper controls on software installation of system
3	PC01	Unauthorized access to system programs or data	Lack of security mechanisms and control for external data exchange
4	PC02	Improper use - Violation of operating procedures	Lack of effective audit review and management
5	PC02	Infected by a virus	Not inspect or update the virus definitions or virus database
6	PC02	Use or log in as someone else	Lack of system identity authentication and identification mechanism
7	PC03	Natural consumption or damage	Equipment lacks maintenance and support mechanisms
8	PC03	Breach of organization law or contract	The lack of proper controls on software installation of system
9	PC03	Leak confidential information or programs	Lacking or inadequate of information security advocacy
10	PC04	Natural consumption or damage	Equipment lacks maintenance and support mechanisms
11	PC04	Breach of organization law or contract	The lack of proper controls on software installation of system
12	PC04	Leak confidential information or programs	Lacking or inadequate of information security advocacy
13	PC05	Natural consumption or damage	Equipment lacks maintenance and support mechanisms
14	PC05	Breach of organization law or contract	The lack of proper controls on software installation of system
15	PC05	Leak confidential information or programs	Lacking or inadequate of information security advocacy
16	PC06	Opernational failure	Insufficient equipment or system maintenance or maintenance mechanism
17	PC06	Theft of system equipment, programs or data	Lack of a movable device and media control
18	PC06	Infected by a virus	Not inspect or update the virus definitions or virus database
19	PC07	Natural consumption or damage	Equipment lacks maintenance and support mechanisms
20	PC07	Breach of organization law or contract	The lack of proper controls on software installation of system

Table 3: The sample results of threat-vulnerability pairs of end point equipment obtained by Predictive Aprori

Rule	Recommendation list	Accuracy
Rule 1	vul= The lack of proper controls on software installation of system 12 ⇒ threat= Breach of organization law or contract, such as using pirated software 12	0.98954
Rule 2	vul= Not inspect or update the virus definitions or virus database 6 ⇒ threat= Infected by a virus 6	0.97675
Rule 3	threat= Theft of system equipment, programs or data 4 ⇒ vul= Lack of a movable device and media control 4	0.95678
Rule 4	threat= Unauthorized access to system programs or data 2 ⇒ vul= Lack of security mechanisms and control for external data exchange 2	0.88147
Rule 5	threat= Arbitrarily change the setting of program or system 2 ⇒ vul= Lacking or inadequate of information security advocacy 2	0.88147
Rule 6	threat= Dust 2 ⇒ vul= Easily affected by environmental factors, such as temperature, humidity, dust, pollution and electromagnetic 2	0.88147
Rule 7	threat= Spread malware or virus 2 ⇒ vul= Not inspect or repair the technical weaknesses in the system operation 2	0.88147
Rule 8	threat= Leakage of personal data 2 ⇒ vul=Not implement appropriate network isolation or other security mechanisms according to the importance of system data 2	0.88147
Rule 9	vul=Not implement appropriate network isolation or other security mechanisms according to the importance of system data 2 ⇒ threat= Leakage of personal data 2	0.88147
Rule 10	vul= Lacking or inadequate of information security advocacy 2 ⇒ threat= Arbitrarily change the setting of program or system 2	0.88147

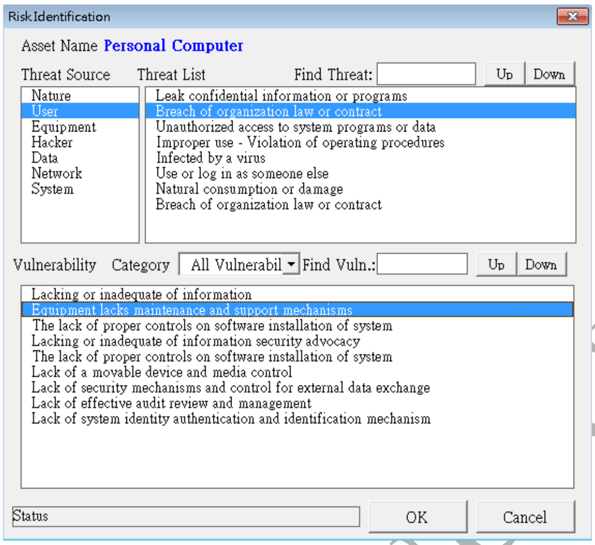
management of these business units are more mature than others that are not certified.

In order to evaluate the threat-vulnerability pairs of the recommendation list, first, we invited two risk assessment experts to determine whether the recommendation list actually improves the efficiency and accuracy of identifying threat-vulnerability pairs. One of the two experts has a lot of experience in consulting with organizations about risk assessment approach and has ISO/IEC 27001 lead auditor certification. The other is a professional auditor of ISO/IEC 27001 with a great deal of maturity. After reviewing the threat-vulnerability pairs of the recommendation list, the domain experts confirmed that the recommendation list can help risk assessors to determine the appropriate risk pair.

After the accuracy of the threat-vulnerability pairs of the recommendation list were confirmed by the domain experts, we then put the list in the risk assessment system. When the risk assessor begins with the risk identification process, a pop-up window, as shown in Fig. 2, helps in selecting the appropriate threat-vulnerability pair. The threat-vulnerability pairs in the recommendation list have been ranked according to the group of the information asset, the system first provided and ranked by the accuracy learned by the Preditive Apriori association rule. When the risk assessor selects either threat or vulnerability from the selection list, the system automatically provides the ranked recommendation list for increasing the identification efficiency. If the risk assessor disagrees with the provided recommendation list, he or she can choose the other suitable risk pair from the list. Each of the elapsed times MT_{sel} while performing risk identification by risk assessors have been measured according to Eq. 1, where t_s is the timestamps of the decision making, and t_p is the timestamps of the selection providing.

$$MT_{sel} = \sum_{sel \in \{Tradition, Adoption, NonAdoption\}} \frac{t_s^{sel} - t_p^{sel}}{|N_{sel}|} \tag{1}$$

Three types of the selection have been classified in the evaluation: $Tradition$, $Adoption$, and $NonAdoption$. $Tradition$ means that the selection on the pop-up



Asset Name **Personal Computer**

Threat Source:
- Nature
- User
- Equipment
- Hacker
- Data
- Network
- System

Threat List:
- Leak confidential information or programs
- Breach of organization law or contract
- Unauthorized access to system programs or data
- Improper use - Violation of operating procedures
- Infected by a virus
- Use or log in as someone else
- Natural consumption or damage
- Breach of organization law or contract

Category: All Vulnerabil

- Lacking or inadequate of information
- Equipment lacks maintenance and support mechanisms
- The lack of proper controls on software installation of system
- Lacking or inadequate of information security advocacy
- The lack of proper controls on software installation of system
- Lack of a movable device and media control
- Lack of security mechanisms and control for external data exchange
- Lack of effective audit review and management
- Lack of system identity authentication and identification mechanism

Figure 2: The risk identification form for selecting the threat-vulnerability pair which provided by the risk management system.

risk identification window which does not provide any recommendation list. The risk assessor must select the most suitable one from the threat- and vulnerability-list. In *Adoption* and *NonAdoption*, both of them provide threat-vulnerability pairs from the recommendation list according to the asset groups. *Adoption* means that the threat-vulnerability pair chosen by the risk assessor is included in the provided recommendation list. However, if the chosen threat-vulnerability pair does not belong to the recommendation list, this will be recognized as *NonAdoption*.

4.2. Experimental result

In order to evaluate the contribution of the recommendation list, we selected more than one hundred critical information systems in a corporation with more than twenty thousand employees. To prevent the risk assessors relying on the recommendation list while performing risk identification, they were not informed that the risk assessment system can provide recommended threat-vulnerability pairs or any other selection suggestion during the training course. In addition, while performing risk identification, the system provides the recommendation threat-vulnerability pair randomly with a probability of 50%.

The experiment was conducted between June 10 and July 24, 2015. At the beginning, each risk assessor was required to take the training course. The basic domain knowledge of risk assessment and how to operate the risk assessment system were both introduced in the course. While the risk assessor selected the threat-vulnerability pair, the risk assessment system classified the selection and measured the elapsed time of the decision, as shown in Eq. 1. Each of the selections of threat-vulnerability pairs was logged into the risk assessment system, including $\{Name, Group, Threat, Vulnerability, Elasped\ time, Classification\}$. During the experiment, the number of $5,470$ selection logs were recorded in the system log.

However, some circumstances encountered in risk identification phase. Some risk assessors may choose threat-vulnerability pairs without any thinking. The elapsed time in this circumstance may seem very short but meaningless. Another problem is that risk assessors may be distracted by unexpected event or task while performing risk identification, which may prolong the elapsed time and interfere with the evaluation result. In order to prevent these two circumstances while performing risk identification, a pre-test was performed in order to determine o_{low} and o_{up}. Elapsed time lower than o_{low} or higher than o_{up} are both recognized as outliers, and the outliers were excluded in this experiment. In the pre-test, firstly, each testee had to select a threat-vulnerability pair as soon as possible without thinking about the reasonability of the pair for determining o_{low}. Then, the testee had to carefully identify the threat-vulnerability pair carefully and think about the reasonability of the pair, and the maximum elapsed time was recognized as o_{up}. After the pre-test, the criteria of outlier $\{o_{low},\ o_{up}\}$ has been determined to $\{5.0\ sec\ ,\ 250\ sec\}$.

About 864 (about 15.8 %) items were excluded from the experimental result. Then, as shown in Fig. 3, we used a boxplot to perform second phase outlier exclusion, and 361(about 6.6 %) items were excluded in this phase. The summary of the evaluation results is shown in Table 4. From the experimental results, we can see that with the assistance of a recommendation list while performing risk identification, the mean elapsed time is shorter than when using traditional method of selecting threat-vulnerability pairs by about 21.5 %. However, if the provided recommendation list does not meet the risk assessor's requirement, it may take more than 14.1% to choose a suitable threat-vulnerability pair.

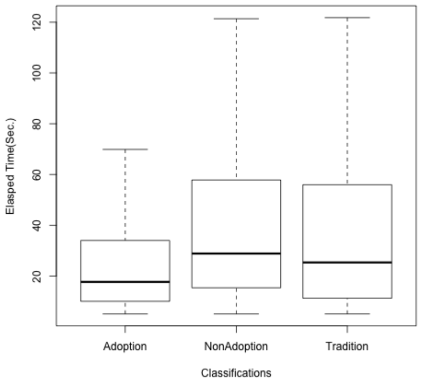
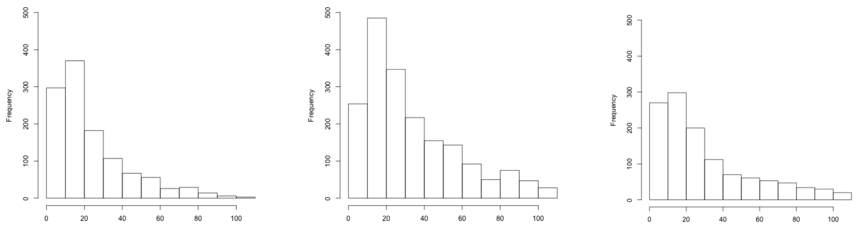


Figure 3: The boxplot of the elapsed time for each classification.

Table 4: The summary of the log of the risk identification on the risk assessment system.

Classification	N	*mean*	*sd*	*max*	*min*
Adoption	$1,157$	23.960	19.500	105.990	5
NonAdoption	$1,893$	33.560	24.630	108.390	5
Tradition	$1,195$	30.530	25.710	108.260	5.010

We can say that with the assistance of the recommendation list, the risk assessor can shorten the elapsed time while performing risk identification. As shown in 4(a), with the assistance of the recommendation list, we can see that over 57 % decision-making by risk assessors occurred within 20 sec. However, in 4(c), that is merely 47.5% occurred within 20 sec.



(a) *Adoption* (b) *NonAdoption* (c) *Tradition*

Figure 4: The histogram of the elapsed time for each classification on risk identification.

5. Conclusion and Future work

In this paper, we propose a recommendation mechanism to assist the risk assessor in selecting the most suitable threat-vulnerability pairs while performing risk identification. The recommendation list is created through the use of Predictive Apriori with the historical selection data of the ISO/IEC 27001:2013 certified business unit. The results of a prior experiment performed by security experts confirmed that the recommendation list can help risk assessors in selecting the appropriate risk item.

In addition, in order to evaluate the elapsed time of the risk identification, we implemented a risk assessment system for helping risk assessors in the whole risk management cycle. Meanwhile, the system collects the historical selection records from risk assessors. More than a hundred of critical information systems were selected for performing the experiment. According to the experimental results, with the assistance of the recommendation list, risk assessors can shorten the elapsed time of decision-making. Finally, this not only improves the efficiency, but also enhances the accuracy of selecting the appropriate threat-vulnerability pair in the process of risk identification.

In the future, we intend to expand the scope of the experiment, which will ensure that more data can be collected and analyzed . The more data we collect, the more the model will be complete. In addition, the algorithm of the association rule adopted in this paper can be refined and extended so as to improve the performance and accuracy. Finally, much more research in general needs to be done to assist organizations in protecting their assets from harm within an acceptable price range.

References

[1] Information technology - security techniques - information security risk management, ISO/IEC 27005:2011 (2011) 1–68.

[2] P. Shamala, R. Ahmad, M. Yusoff, A conceptual framework of info structure for information security risk assessment (isra), Journal of Information Security and Applications 18 (1) (2013) 45 – 52, sETOP'2012 and FPS'2012 Special Issue. doi:http://dx.doi.org/10.1016/j.jisa.2013.07.002.

[3] Risk management – principles and guidelines, ISO 31000:2009 (2009) 1–24.

[4] Information technology - security techniques - information security management systems – requirements, ISO/IEC 27001:2013 (2013) 1–23.

[5] M. S. Lund, B. Solhaug, K. Stølen, Model-Driven Risk Analysis - The CORAS Approach, Springer Berlin Heidelberg, 2011. doi:10.1007/978-3-642-12323-8.

[6] C. Alberts, A. Dorofee, J. Stevens, C. Woody, Introduction to the octave approach.
URL https://resources.sei.cmu.edu/asset_files/UsersGuide/2003_012_001_51556.pdf

[7] S. Taubenberger, J. Jürjens, Y. Yu, B. Nuseibeh, Resolving vulnerability identification errors using security requirements on business process models, Information Management & Computer Security 21 (3) (2013) 202–223.

[8] A. Ekelhart, S. Fenz, T. Neubauer, Ontology-based decision support for information security risk management, in: Systems, 2009. ICONS '09. Fourth

International Conference on, 2009, pp. 80–85. doi:10.1109/ICONS.2009.8.

[9] M. Almorsy, J. Grundy, A. S. Ibrahim, Collaboration-based cloud computing security management framework, in: Cloud Computing (CLOUD), 2011 IEEE International Conference on, 2011, pp. 364–371. doi:10.1109/CLOUD.2011.9.

[10] Guide for conducting risk assessments, Tech. rep. (2012). doi:10.6028/nist.sp.800-30r1.

[11] Z. Yazar, A qualitative risk analysis and management tool–cramm, SANS InfoSec Reading Room White Paper.

[12] A. Ekelhart, S. Fenz, T. Neubauer, Aurum: A framework for information security risk management, in: System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on, 2009, pp. 1–10. doi:10.1109/HICSS.2009.82.

[13] J. Webb, A. Ahmad, S. B. Maynard, G. Shanks, A situation awareness model for information security risk management, Computers & Security 44 (2014) 1 – 15. doi:http://dx.doi.org/10.1016/j.cose.2014.04.005.

[14] W. Fan, T. Watanabe, K. Asakura, Mining underlying correlated-clusters in high-dimensional data streams, International Journal of Social and Humanistic Computing 1 (3) (2010) 282–299.

[15] Weka 3: Data mining software in java.
URL http://www.cs.waikato.ac.nz/ml/weka/

[16] E. Frank, M. Hall, L. Trigg, G. Holmes, I. H. Witten, Data mining in bioinformatics using weka, Bioinformatics 20 (15) (2004) 2479–2481.

[17] E. Frank, M. Hall, G. Holmes, R. Kirkby, B. Pfahringer, I. H. Witten, L. Trigg, Data Mining and Knowledge Discovery Handbook, Springer US,

Boston, MA, 2010, Ch. Weka-A Machine Learning Workbench for Data Mining, pp. 1269–1277. doi:10.1007/978-0-387-09823-4_66.

u Chih ei is a researcher in Information & Communication Security Lab., Telecommunication Laboratories, Chunghwa Telecom Co. Ltd. He received his Ph.D. in Department of Information Management, National Central University, Taiwan in 2013. His research interests include Vehicle Ad-Hoc Network Security and Information Security Management.

ei Chen u received his Ph. D. degree in Information Management from National Central University in 2016. From 2004 to now, he is also the Director of the Computer Center at Hsin Sheng College of Medical Care and Management. His current research interests include information & security, cryptography and computer communications.

a Chi Chu is a researcher in Information & Communication Security Lab., Telecommunication Laboratories, Chunghwa Telecom Co. Ltd. He received his M. S. degree in Department of Information Management, National Central University, Taiwan in 2010. His research interests include Information Security Risk Management.