Process-Oriented Approach for Validating Asset Value for Evaluating Information Security Risk

Shi-Cho Cha
National Taiwan University of Science and Technology
Taipei, Taiwan 106
Email: csc@cs.ntust.edu.tw

Li-Ting Liu
National Taiwan University of Science and Technology
Taipei, Taiwan 106
Email: M9609307@mail.ntust.edu.tw

Bo-Chen Yu
National Taiwan University of Science and Technology
Taipei, Taiwan 106
Email: M9709210@mail.ntust.edu.tw

Abstract—To provide a systematic means of identifying and assessing information security risks, organizations typically adopt asset-driven (or asset-oriented) risk assessment schemes. These schemes require organizations to identify their information assets, find out potential incidents to those assets, and assess expected losses associated with those incidents. While asset value is important in determining loss expectancies for associated incidents, the accuracy of asset valuation is crucial. Although numerous guidelines exist regarding how best to evaluate asset value, current risk assessment schemes generally overlook how to validate assessments of asset value. Consequently, this work presents a process-oriented approach that organizations can employ to validate and adjust asset value. The approach presented in this study can help organizations represent their business processes and information assets used in those processes using flowcharts, and also mark dependencies among assets based on confidentiality, integrity, and availability requirements on flowcharts. Organizations can use the markings of dependencies to validate and correct results associated with asset valuation. If organizations can more accurately evaluate asset value, they can improve the effectiveness of their risk assessment. Therefore, the approach presented in this study can hopefully help improve organizational information security.

I. INTRODUCTION

Organizations attempting to secure their information systems frequently require effective information security risk management processes to balance information security and convenience. Essentially, risk management processes help organizations identify potential security incidents. Organizations can then adopt suitable countermeasures based on their expected losses. To systematically identify potential incidents involving an organization and assess associated expected losses, current risk assessment approaches, such as ISO27005 [1], BS7799-3 [2], OCTAVE [3], CRAMM [4], and so on, generally view potential incidents to an organization as the aggregation of incidents involving each asset of the organization.

In asset-driven (or asset-oriented) approaches, incidents related to a single asset are usually assessed together rather than independently. For an incident involving an asset, it is only necessary to determine the expected exposure factor. This factor represents the average proportional loss of asset value resulting from the incident. Consequently, the loss expectancy of the incident can be calculated based on the asset value and the expected exposure factor. In this case, evaluating asset value is important in risk assessment.

Although current standards, such as ISO 13335-3 [5], BS7799-3 [2], and so on, provide principles for evaluating asset value, these standards generally do not address the details of how to validate estimated asset value. If the organization decides value its assets based on these standards, it may find that the accuracy of the estimated results is still heavily reliant on the experiences and skills of the individual performing the evaluation.

For this reason, this study proposes a process oriented approach for validating the results of asset valuation for risk assessment: First, the proposed approach provides a means for organizations to depict their business processes and information assets used in those processes with flowcharts, and to mark the dependency among the assets based on their confidentiality, integrity and availability requirements. Furthermore, this study also provides a means for organizations to validate and correct the evaluated value of their assets based on the markings of dependency among the assets. In this way, organizations can better evaluate the values of information assets and perform more precise risk assessments. Therefore, the study results can hopefully contribute to improving organizational information security.

The remainder of this paper is organized as follows: Section II introduces preliminary knowledge. Section III then presents an overview of the proposed approach. Subsequently, sections IV and V explain the proposed approach in detail. Section VI evaluates the effectiveness of the proposed approach. Conclusions are finally drawn in Section VII, along with recommendations for future research.

II. BACKGROUND KNOWLEDGE AND RELATED WORK

A. Risk Management

The RM processes enable an organization to discover and assess its risks and to determine how to control or mitigate the risks as follows [6], [7], [8]:

- Risk identification. Risk identification is the process of finding out the incidents that may damage information systems and associated business processes [9]. In accordance with ISO/IEC 13335-3 [5], the following approaches can be used to identify risks. In the baseline...
Risk treatment. After identifying and assessing a potential incident, an organization must decide how to treat the risk. Possible options include the following [14]: (1) Doing nothing and accepting the risk. (2) Avoiding potential incidents by changing or terminating associated actions or business processes. (3) Relying on appropriate security safeguards to mitigate the risks to an acceptable level. Several safeguards are possible [13], [15]. If more than one security safeguard option can be applied to the same potential incident, an organization can use cost-benefit analysis or other approach to optimize its security investment [9], [16], [17]. However, these issues are beyond the scope of this article.

Monitoring and re-assessing the risks. The residual risks and identified acceptable risks should be regularly monitored and reviewed to ensure the accuracy and effectiveness of risk assessment and treatment, respectively [2], [18]. Additionally, an organization may need to re-assess its risks to reflect major organizational changes.

B. Asset-driven Risk Assessments and Information Asset Valuation

Although organizations may use fault trees [19], misuse cases [20], attack trees [21] and other tools to analyze potential incidents, organizations may have difficulty directly applying these tools to identify and assess incidents. Therefore, current risk assessment schemes generally adopt asset-driven approaches. Based on the requirements of ISO 27001, current asset-driven risk assessment schemes usually enable organizations to identify assets related to the scope of organizational activities. Identify threats or potential causes of incidents to the assets that may harm the organization. Determine the vulnerabilities or weakness of the asset that may be exploited by the identified threats. Estimate loss expectancy when a threat related to an asset exploits a vulnerability of that asset.

Generally, identified assets guide the asset-driven risk assessment processes in two ways: (1) to determine potential incidents to an organization; (2) to evaluate expected loss expectancy and loss impact of potential incidents. First, current asset-driven risk assessment schemes generally help organizations consider the incidents that may occur in relation to its assets and the origin of those incidents. For example, [5] and [13] lists common threats and vulnerabilities related to threat and vulnerability identification. OCTAVE presents a set of generic threat profiles that organizations can use to identify and analyze threats to their assets [3]. CORAS gives an organization a means of visualizing threats to its assets and vulnerabilities of those assets using diagrams [22].

On the other hand, organizations can use asset information, especially asset value, to reduce the work of risk assessment. For example, when an organization calculates ALEs for every potential incident in the organization, it may need to analyze its SLE and ARO based on related threats and vulnerabilities [11]. At this point, an organization can assess incidents affecting the same asset together rather than assessing them separately. For an incident to an asset, an organization can simply determine an expected exposure factor, which represents the average proportion of the asset value that is likely to be lost as a result of the incident. The single loss expectancy of the incident can be calculated by simply multiplying the value of the asset and the expected exposure factor. Although different asset-driven risk assessment schemes may model risks differently, these schemes, including [2], [4], [5], [13], [23], and so on, usually use asset value for risk estimation. Furthermore, instead of evaluating the loss expectancies of incidents to every organizational asset, organizations can select critical assets based on their value and only assess the risks involving critical assets [3].

As described above, asset value is important in asset-driven risk assessment schemes. When an organization performs risk assessment using such schemes, it should consider asset valuation accuracy. However, current standards generally only
provide principles for evaluating asset value. For example, ISO 13335-3 provides a list of issues, such as legal and business requirements, damages resulting from the loss of confidentiality, integrity, availability, and so on, to determine asset value [5]. When an organization values its assets based on the principles in current standards, that organization may find that certain assets are in-deliberately undervalued. For example, a person may forget that a desktop is used to process confidential data and overlook its importance. In this case, dependencies among assets and the roles of assets in business processes can be considered to reduce the likelihood of ignorance. For example, Suh and Han proposed an IS methodology for an organization to determine value of an asset based on whether the asset is critical to an important process [24]. However, current works generally fail to address the details of how to clarify dependency or role information and use it to adjust asset value. Consequently, this study aims to complement current asset-driven risk assessment schemes by presenting a systematic approach for validating and adjusting asset value based on dependencies among assets and asset roles in business processes.

III. APPROACH OVERVIEW

Figure 1 shows how the proposed approach can be employed to complement current asset-driven risk assessment schemes. The left column gives the typical processes of asset-driven risk assessment schemes based on BS7799-3 [2]. The figure shows that the proposed approach is composed of two main components:

First, this study assumes that an organization identifies its asset by listing its business processes and using a flowchart to identify assets used in each business process as follows: From Fig. 2, an organization can represent activities of the business process. For each activity, organizations identify associated inputs and outputs, related information systems, and responsible participants. Organizations thus can identify assets based on inputs, outputs, information systems, and participants relevant to organizational business processes. This study goes one step further and creates a system of symbols that an organization can use to mark the roles of assets in business processes, as well as the dependencies among assets on flowcharts. Notably, this study did not restrict an organization to using the above approach to identify assets. That is, organizations can use the proposed approach to independently clarify dependencies among assets and the roles of assets in business processes.

Following asset identification, an organization values its assets in asset-driven risk assessment schemes. Suppose that an organization identifies assets based on business processes as described above. There should be several flowcharts along with markings of dependencies among assets. The proposed approach provides a means for organizations to validate and modify the value of its assets based on flowcharts and associated markings.

IV. MARKING ASSETS IN FLOWCHARTS

As mentioned in Section II, asset value is usually assessed based on damage resulting from breaches of confidentiality, integrity, and availability associated with the asset. Therefore, the approach presented in this study visualizes the roles of assets in business processes and the dependencies among assets in flowcharts from the perspectives of confidentiality, integrity, and availability, respectively.

A. Availability Markings

This study denotes an asset critical to the continuity of a business process as a critical asset for that process. When an organization uses the flowcharts mentioned in Section III to identify assets associated with a business process, it can use circles as availability markings to indicate critical assets for the business process, as illustrated in Fig. 3. Therefore, for any business process \( P_i \), an organization can identify a set of critical assets \( \{a_j\} \).

Furthermore, to provide a basis for validating the estimated asset values, the proposed approach requests organizations to assess the importance of their business processes. The importance of business processes can be determined based
on losses resulting from process unavailability. This study demonstrates how to use these values later.

Finally, current availability marking schemes can only reflect whether or not an asset is critical to a business process. However, damage to an asset may partially disrupt a business process. How to extend current marking schemes to illustrate this situation is left to our future work.

B. Confidentiality Markings

According to Fig. 4, this study uses the symbol ⋄ to indicate confidentiality markings based on asset categories:

- If data or documents are generated from confidential data, they may have the same confidentiality value as the confidential data. In this case, this study assumes that an activity $ACT_i$ in a business process $P_j$ outputs an asset $a_i$ based on a set of input assets $\{a_j\}$. If the confidential value of $a_i$ cannot be smaller than the biggest confidential value of assets in $\{a_j\}$, a symbol ⋄ is drawn below the arrow that outputs $a_i$ in the flowchart of $P_j$.

- If an organization uses an information system to process confidential data, the system may have the same confidentiality value as the data. Suppose that an activity $ACT_i$ needs to be executed using an information system $a_i$ based on a set of input assets $\{a_j\}$. If system $a_i$ is required to equal the highest confidential value of assets in $\{a_j\}$, a symbol ⋄ is indicated in the top left corner of the system in the flowchart of $P_j$.

- Similarly, if an individual can access confidential data, he or she may share the same confidentiality value as the data. If the confidential value of person $a_i$ should not be below the confidential value of assets $\{a_j\}$ when the individual deals with the assets in an activity $ACT_i$ of a business process $P_j$, a symbol ⋄ is drawn in the top left corner of the person in the flowchart of $P_j$.

No matter what category an asset belongs to, a set of tuple $\{(ACT_i, a_i)\}$ can be identified to reflect the positions of ⋄ in a flowchart.

C. Integrity Markings

Take Fig. 5 for example, the proposed approach uses ■ for integrity markings. Because the data integrity depends on what is used for data generation, instead of considering what data are generated from confidential data, this study focuses on the data used as inputs for generating data with high integrity value. If input data $a_i$ during activity $ACT_i$ in business process $P_j$ strongly affects the integrity of output, the data $a_i$ is indicated with a ■ symbol above the associated input arrow.

Moreover, when an individual or an information system $a_i$ are used to process a set of data in an activity $ACT_i$ of an business process $P_j$, a symbol ■ is drawn in the top right corner of the person or system if its integrity level should equal or exceed that of the associated data. Finally, a set of tuple $\{(ACT_i, a_i)\}$ can be obtained for the positions of ■ in a flowchart.

D. Put it All Together

This section summarizes the results of the markings schemes with an example. Figure 6 partially illustrates the
process flowchart of scholarship applications for a certain school, during which process the applicant first uses the application system to complete an application form with his/her personal profiles on the Web and then print out the application form. The applicant then applies for past transcripts using the transcripts management system and obtains other necessary data, such as household certificates, before sending out the application. During the process, missing information, or the breakdown of any part of the system, will result in the failure of the application to proceed. Consequently, all the assets are circled. Because application forms, transcripts, and household certificates all contain personal information, the data has the same level of confidentiality as the personal profiles. Therefore, the symbol ★s are drawn below the associated arrows.

During the process, the integrity of the application form or transcripts depends on the information provided by the applicant. For example, if the input information is incorrect, the output will also be incorrect. Hence, the input information is marked with ■. Additionally, the confidentiality and integrity of the information inputted by the applicant is extremely important, and thus the scholarship and transcript management systems for handling documents related to personal profiles are marked with symbol ★ and ■. Furthermore, the applicant should provide a correct personal profile. Therefore, ■ is used to represent the integrity requirement.

V. Asset Value Validation

This Section details how to validate asset valuation. As noted in Section II-B, an organization usually values an asset based on damages resulting from the loss of asset confidentiality, integrity and availability. This study assumes that an organization evaluates asset confidentiality, availability, and integrity value, respectively, and uses this information to summarize asset value. This study thus proposes validating asset value from the perspectives of availability, confidentiality, and integrity, as follows:

1. For each business process \( P_i \)
2. Obtain the process importance \( V_{Pi} \) for \( P_i \)
3. Obtain the set of \( \{a_j\} \) that is circled in the associated flowchart
4. For each asset \( a_j \) in \( \{a_j\} \)
5. If the availability value of \( a_j \) \( AV_{a_j} \) is below \( V_{Pi} \)
6. Set \( AV_{a_j} = V_{Pi} \)
7. End If
8. End For
9. End For

Fig. 7. Algorithm for adjusting asset value from the availability perspective

A. Validate Asset Value from Availability Perspective

The concept of validating the availability value or level of an asset that is critical to a business process is to not permit the availability value of that asset to be lower than the process importance. Figure 7 shows that when an organization wishes to validate the availability value of assets associated with a business process \( P_i \), it should first obtain the flowchart of the process. As described in IV-A, an organization can obtain the importance value \( V_{Pi} \) of the process and a set of assets \( \{a_j\} \) critical to that process. For each critical asset \( a_j \), an organization can compare its availability value \( AV_{a_j} \) with \( V_{Pi} \). If \( AV_{a_j} < V_{Pi} \), the organization can automatically or manually set \( AV_{a_j} \) to \( V_{Pi} \).

B. Validate Asset Value from Confidentiality and Integrity Perspective

Figure 8 shows that an organization can validate the confidentiality value of assets related to a business process \( P_i \) by activity. For each activity \( ACT_j \) in the process, the organization first checks the confidentiality value of all input data or document assets and selects the largest. Supposing that the largest confidentiality value among all inputs of \( ACT_j \) is \( MCV_{ACT_j} \), the organization can adjust the confidentiality value of assets associated with \( ACT_j \) as follows:

- For a data asset marked with ★, the organization must compare the confidentiality value of the asset with \( MCV_{ACT_j} \), and let its confidentiality value exceed or equal \( MCV_{ACT_j} \).
- If a ★ is drawn in the top left corner of an associated system \( a_i \), it means that the system responds by doing activity \( ACT_j \) in relation to the confidentiality of this data. Therefore, the organization should ensure that the confidentiality value of the asset \( CV_{a_i} \) is no less than \( MCV_{ACT_j} \).
- Organizations should check the confidentiality value of people who perform \( ACT_j \). For a person \( a_m \) marked with ★, the organization should ensure that its confidentiality value \( CV_{a_m} \) is greater than or equal to \( MCV_{ACT_j} \).

An organization can use a similar method for validating the integrity value of assets. Because garbage inputs lead to garbage outputs, integrity validation begins with the integrity value of the output data associated with an activity. First, the proposed approach request an organization to ensure that no input data marked with ■ has a lower less integrity value than
1. For each business process \( P_i \),
2. For each activity \( ACT_j \) in \( P_i \),
3. Identify the largest confidentiality value \( MCV_{ACT_j} \) from the input assets of \( ACT_j \).
4. For each output data \( a_k \) marked with ★, if the confidentiality value of \( a_k \) (or \( CV_{a_k} \)) is less than \( MCV_{ACT_j} \),
5. Set \( CV_{a_k} = MCV_{ACT_j} \),
6. End If
7. End For
8. End For
9. For each system \( a_j \) used in \( ACT_j \) and marked with ★, if the confidentiality value of \( a_j \) (or \( CV_{a_j} \)) is less than \( MCV_{ACT_j} \),
10. Set \( CV_{a_j} = MCV_{ACT_j} \),
11. End If
12. End For
13. End For
14. For each participant \( a_m \) who performs \( ACT_j \) and is marked with ★, if the confidentiality value of \( a_m \) (or \( CV_{a_m} \)) is less than \( MCV_{ACT_j} \),
15. Set \( CV_{a_m} = MCV_{ACT_j} \),
16. End If
17. End For
18. End For
19. End For
20. End For

The consultants usually use asset-driven approach for risk identification and assessment: First, they assist an organization to identify its assets into a table like Table II. The table usually contains basic information about information assets, including IDs, descriptions, custodians, users, and so forth. For each asset, the organization then evaluates the asset’s confidentiality, integrity, and availability levels based on damages resulting from the loss of confidentiality, integrity, and availability respectively. In this case, the consultants usually assist an organization to establish guidelines to determine confidentiality, integrity, and availability levels of an asset. For example, an organization can classify loss value into different ranges as illustrated in Table III. The organization can then evaluate confidentiality, integrity, and availability levels of an asset based on the table and estimate value of the asset based on the levels. For example, the organization can choose the maximal value among confidentiality, integrity, and availability levels of an asset as value of the asset. Consequently, the organization can calculate risk or loss expectancy of an incident to an asset by matching value of the asset, and the associated threat and vulnerability levels in a matrix such as that illustrated in Table IV, which is provided in BS7799-3 [2].

Most of the interviewees agreed that the proposed approach may enable an organization to verify values of its assets in the above process. Several interviewees mentioned that the approach may further be used to aid risk assessors in explaining the results of asset valuation. Even though, they still provided several suggestions for future enhancement. The major suggestions include:

- The cost of the proposed approach may be too high to be implemented in real cases. Therefore, an organization may need tools to manage flowcharts of its business processes.
- Current approach only covers some simple rules to verify results of asset valuation. More complicated rules should be considered. For example, when an organization store...
personal data into a database, value of the database may be much higher than the value of a person’s data.

The suggestions are left to our future work.

VII. CONCLUSION AND FUTURE WORK

To overcome the deficiencies of the current asset-driven risk assessment approach, this study proposes a systematic approach via which an organization can validate and adjust the value of its information assets: First, when an organization identifies its assets and business requirements, it can depict its business processes and assets in flowcharts. This study enables organizations to mark their assets on flowcharts to represent dependencies among assets and the roles of assets in business processes. After valuing organizational assets, an organization can use the markings of asset roles and dependencies to validate the results of asset valuation from the perspectives of confidentiality, integrity, and availability. If organizations can more accurately assess the value of their assets, they can perform more effective risk assessment. Therefore, the results of this study can hopefully contribute to improving overall information security.

Future research can pursue the following directions. First, tools can be created to help individuals draw flowcharts based on the proposed approach, as well as to manage such flowcharts. Additionally, tools can be linked with organizational asset databases, thus helping organizations to automatically validate organizational asset value.

This study observed that current marking schemes do not consider the degree of asset interdependency or the degree of importance to a business process. In this case, we may label markings with numbers to represent the degree information. For example, we may add a number 50% next to an availability marking to show that the availability value of an asset should be bigger than 0.5 times the importance of the associated business process. However, an asset valuation methodology may need to be designed for the extension, and thus the usability of the proposed approach could be reduced. Therefore, how to extend the marking scheme remains an important and interesting direction for future research.

Last but not least, this study only evaluated the effectiveness of the proposed approach by interviewing several consultants that have experience in information security risk assessment. Empirical data can be used to perform formal validation. However, an organization usually hesitates to provide information about information security. Therefore, we may have troubles in obtaining data to determine whether the proposed approach provides correct validation results. Further studies are needed to explore these important questions.

ACKNOWLEDGMENT

This work was supported in part by NSC 97-2221-E-011-064 and NSC 98-2219-E-011-001.

REFERENCES