Abstract

With the increasing importance of system security risk assessment, a number of system security risk assessment methods or models have already appeared and more are emerging every day. Therefore it is difficult for organizations to select a method that best suits their requirements. The difficulty of selection drives the need toward a comparative framework to evaluate system security risk assessment methods.

In the underlying research-in-progress paper we propose a comprehensive framework for comparing system security assessment methods. Unlike most of the existing comparative framework, the proposed framework covers the whole process of system security risk assessment based on the evaluation criteria of completeness and effectiveness.

In our future research, three current system security risk assessment methods will be evaluated using the proposed comparative framework. This framework will highlight the strengths and weaknesses of the methods compared.

Key words
System Security Risk Assessment, Comparative Framework, SSR Assessment Method

Introduction

Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. As a consequence of cyber intrusions and attacks, organizations have to pay more attention to protect their work systems. Recently, companies are making a great effort to protect their data, spending a lot of money and resources to implement system security assessment methods such as COBIT and also engaging auditors to verify these methods (Manhart and Thalmann 2013). The topic of system security risk (SSR) assessment has been around for more than twenty years(Frohman 1995) and the practice of SSR assessment is still evolving and changing for both practitioners and researchers alike. The SSR assessment literature has several security frameworks, models, methods, and guidelines (Alter and Sherer 2004; Siponen 2007; Sun et al. 2006; Yadav and Dong 2014; Zhang et al. 2012).

A major task for an organization is to determine which method to use for SSR assessment. Currently, however, there are very few comparative studies to help organizations in determining which SSR assessment methods are effective.

In this research-in-progress paper we propose a comprehensive framework for comparing system security assessment methods. Unlike most of the existing comparative frameworks, the proposed framework covers the whole process of system security risk assessment based on the evaluation criteria of completeness and effectiveness.
This paper will contribute to the SSR assessment literature in several ways. First, the paper presents a viable and comprehensive comparative framework for practitioners to effectively compare different SSR assessment methods. Second, the study will provide insight into the development of more effective SSR assessment methods.

The article proceeds as follows. In the next section, literature on the models and methods and comparative frameworks of SSR assessment are reviewed. Next, the comprehensive framework for comparing different SSR assessment methods is presented. Finally, possible limitations to the study and possible avenues for future research are discussed.

**Literature Review**

**System Security Risk (SSR) Assessment Methods**

The main purpose of system security risk (SSR) assessment is to evaluate and improve the security of a work system under study. Its process involves several activities spanning from ascertaining security objectives and requirements to measuring the evidence of existing security mechanisms to evaluating and suggesting improvements in the security of a work system (Yadav and Dong 2014). The current research on (SSR) assessment has made very good progress. Several research works (Alter and Sherer 2004; Baker et al. 2007; Karabacak and Sogukpinar 2005; Yadav 2010) have focused on assessment models to support the ascertainment phase of the security risk assessment process while other researchers (Caralli et al. 2007; Stoneburner et al. 2002; Suh and Han 2003) have emphasized steps and methods to support the ascertainment phase. Other researchers (Feng and Li 2010; Sun et al. 2006) have focused on the measurement and evaluation phases of the assessment process. Most of the research on work system security risk, however, has taken only a partial view of the SSR assessment except (Yadav and Dong 2014). The proposed method—Multi-View Work System Security Assessment (MVWSSA)—in (Yadav and Dong 2014) covers the whole process of system security risk assessment spanning all three phases—ascertainment of security requirements, measurement of evidence for security requirements, and evaluation of evidence against the needed security mechanisms (Ohia 2011).

**Comparative Frameworks for System Security Risk Assessment Methods**

In the past two decades, a number of comparison frameworks for SSR assessment methods have appeared. For example, the one proposed by Eloff et al. (1993), utilized criteria that focus on information technology, information security and risk approach completeness. Even though the framework proposed by Eloff et al. indicated whether a methodology addresses a criterion or not, it does not use scales, or trade-offs which can aid the organization in selecting a method which will best meet their needs (Vorster and Labuschagne 2005). To address this problem, Vorster et al. (2005) presented a comparative framework based on five criteria with scaling. The criteria are as follows: 1) whether risk analysis is done on single asset or groups of assets; 2) where in the methodology risk analysis is done; 3) who are involved in the risk analysis; 4) the main formulae used; 5) whether the results of the methodology are relative or absolute. Almost at the same time, Borman et al. (2004) provided a comparative framework based on COBIT’s Planning and Organization Control Nine, Assess Risks, which can be used as evaluation criteria for work system security risk management methods. Both comparative frameworks are not flawless and have some limitations. Both frameworks ignore the existence of other criteria. There are some other SSR methods such as CRAMM (Eloff et al. 1993) and MVWSSA (Yadav and Dong 2014) which cover a wider process of SSR assessment.

To overcome this issue, a comprehensive framework is proposed to provide a better comparison between different SSR assessment methods.

**A Comprehensive Framework for Comparing SSR Assessment Methods**

The proposed framework for comparing different SSR assessment methods is shown in Table 1. The assessment phases in Table 1 are based on an SSR assessment method developed in (Yadav and Dong 2014). This method is selected because it covers the whole process of work system security risk
assessment spanning all three phases: ascertainment of security requirements, measurement of evidence for security requirements, and evaluation of evidence against the needed security mechanisms (Ohia 2011). There are two criteria, Completeness and Effectiveness, to evaluate the outcomes of each phase. Each criterion has a scaling, which indicates the level of a criterion based on certain outcomes of each phase. Below is a description of each criterion and its scaling.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Outcome of Phases</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Completeness</td>
</tr>
<tr>
<td>Ascertainment</td>
<td>Risk Identification</td>
<td>To what degree a method can evaluate different kinds of assets and risks factors</td>
</tr>
<tr>
<td>Ascertainment</td>
<td>Risk Analysis</td>
<td>To what degree a method can consider different factors when it computes the priority level of each risk factor</td>
</tr>
<tr>
<td>Ascertainment</td>
<td>Security Requirement Recommendation</td>
<td>To what degree a method can identify a complete set of security requirements</td>
</tr>
<tr>
<td>Ascertainment</td>
<td>Security Mechanism Requirement</td>
<td>To what degree a method can identify a complete set of security mechanisms</td>
</tr>
<tr>
<td>Measurement</td>
<td>Collection of Data on Existing Security Mechanism Assessment</td>
<td>To what degree a method can collect data for existing security mechanisms</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Comparison Results</td>
<td>To what degree a method can comprehensively compare existing security mechanisms against needed security mechanisms</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Evaluation Results</td>
<td>To what degree a method can identify a complete set of security mechanisms based on the risk of each asset</td>
</tr>
</tbody>
</table>

**Table 1. A Comprehensive Framework for Comparing SSR Assessment Methods**

**Completeness**

The completeness of each assessment phase is measured by the comprehensiveness of the outputs of each phase. Completeness assesses the degree to which the outputs are comprehensive. Organizations must take into consideration all information security dimensions including technical, organizational, human, and conformity aspects in order to be competitive while providing stakeholders detailed information about the complete structure of the organizations’ information security and risk treatment processes (Tashi and Ghernaouti-Hélie 2007). Therefore, SSR assessment methods should ensure the identification of different kinds of assets, threats, vulnerabilities, security requirements and mechanisms, and comprehensive comparison of existing security mechanisms against the needed security mechanisms.
Below is a description of how to use the two criteria to measure a method’s performance at each phase of SSR assessment and its scaling.

**Risk identification**

In the process of risk identification, the main objective is to identify all the assets belonging to a work system (Alter and Sherer 2004) under study and all sources of risks for assets. The criterion of completeness at this stage evaluates different kinds of assets and risks factors a method can identify.

The criterion of completeness on risk identification can take on a value of 1-3 as follows, and a higher value means a method can identify a more complete set of assets and risk factors:

1: the degree of completeness in identification of assets and risk factors is low;
2: the degree of completeness in identification of assets and risk factors is moderate;
3: the degree of completeness in identification of assets and risk factors is high.

**Risk Analysis**

The process of risk analysis is evaluation and prioritization of security risks from various risk factors which are identified from the previous process. The completeness of risk analysis measures how many factors such as a risk factor’s likelihood of occurrence and severity impact, are put into consideration when a method computes the priority level of each risk factor.

The criterion of completeness based on risk analysis can take on a value of 1-3 as follows, and a higher value means a method can consider more factors when it ranks risk factors:

1: the degree of completeness in risk analysis is low;
2: the degree of completeness in risk analysis is moderate;
3: the degree of completeness in risk analysis is high.

**Security Requirement Recommendation**

Security requirement recommendation is a process of identifying appropriate security requirements to mitigate the impact from risk factors identified from previous steps. The completeness of security requirement recommendation measures the degree of the comprehensiveness of security requirements a method can identify.

The criterion of completeness regarding security requirement recommendation can take on a value of 1-3 as follows, and a higher value means a method can recommend a more complete set of security requirements:

1: the degree of completeness in security requirement recommendation is low;
2: the degree of completeness in security requirement recommendation is moderate;
3: the degree of completeness in security requirement recommendation is high.

**Security Mechanism Recommendation**

Security mechanism recommendation is a process of identifying appropriate security mechanisms to help manage security risk. The completeness of security mechanism recommendation evaluates the degree of the comprehensiveness of security mechanisms a method can identify.

The criterion of completeness regarding security mechanism recommendation can take on a value of 1-3 as follows, and a higher value means a method can recommend a more complete set of security mechanisms:

1: the degree of completeness in security mechanism recommendation is low;
2: the degree of completeness in security mechanism recommendation is moderate;
3: the degree of completeness in security mechanism recommendation is high.

**Collection of Data on Existing Security Mechanism Assessment**

The main objective of this process is to collect data on security mechanisms that have existed in the work system under study. The completeness of data collection on existing security mechanism measures the degree of the integrity of the data a method can collect for existing security mechanisms.

The criterion of completeness on data collection on existing security mechanism can take on a value of 1-3 as follows, and a higher value means a method can collect:

1: the degree of completeness in data collection on existing security mechanism is low;
2: the degree of completeness in data collection on existing security mechanism is moderate;
3: the degree of completeness in data collection on existing security mechanism is high.

**Comparison**

The objective here is to compare the work system’s existing security mechanism against the needed security mechanisms. Based on the comparison, the overall risk level of the work system is computed. The completeness of comparison process evaluates the degree of comprehensiveness of comparison between existing and needed security mechanisms.

The criterion of completeness on comparison can take on a value of 1-3 as follows, and a higher value means a method can compare existing with needed security mechanisms more comprehensively:

1: the degree of completeness in comparison is low;
2: the degree of completeness in comparison is moderate;
3: the degree of completeness in comparison is high.

**Evaluation**

Evaluation is a process of recommending preventive and/or mitigation security mechanism based on the risk of each asset. The completeness of evaluation process measures the degree of the comprehensiveness of security mechanisms a method can recommend.

The criterion of completeness can take on a value of 1-3 as follows, and, a higher value means a method can identify a more complete set of assets and risk factors:

1: the degree of completeness in evaluation is low;
2: the degree of completeness in evaluation is moderate;
3: the degree of completeness in evaluation is high.

**Effectiveness**

The method effectiveness is most commonly measured by a method’s ability to achieve the goals of each process under a method. Numerous studies (Calder and Van Bon 2006; Peláez and Wanner 2010; Qureshi 2012) on measuring effectiveness of security policy provide an insight for measuring effectiveness of SSR assessment methods. To measure if a method is effective, we need to set up the Key Performance Indicators (KPI) for each process (Qureshi 2012). KPIs determine the achievement of the goals of a process. They determine what has to be realized, and measure how successfully the process realizes the goals. It is possible to design KPIs for all kinds of businesses but here the focus will be on KPIs related to process/method effectiveness. The KPIs for each process of SSR assessment methods are shown in Table 2.
<table>
<thead>
<tr>
<th>Phases</th>
<th>Outcome of Phases</th>
<th>KPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascertainment</td>
<td>Risk Identification</td>
<td>A method is able to identify right assets, threats and vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>Risk Analysis</td>
<td>A method is able to estimate the impact of risk factors by considering different factors.</td>
</tr>
<tr>
<td></td>
<td>Security Requirement Recommendation</td>
<td>A method is able to identify the right security requirements.</td>
</tr>
<tr>
<td></td>
<td>Security Mechanism Recommendation</td>
<td>A method is able to identify right security mechanisms.</td>
</tr>
<tr>
<td>Measurement</td>
<td>Collection of Data on Existing Security Mechanism Assessment</td>
<td>A method is able to correctly collect data on existing security mechanisms.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Comparison Results</td>
<td>A method is able to fully compare existing security mechanisms against needed security mechanisms.</td>
</tr>
<tr>
<td></td>
<td>Evaluation Results</td>
<td>A method is able to recommend right security mechanisms based on the risk of each asset.</td>
</tr>
</tbody>
</table>

**Table 2. KPIs of Each Process under SSR Assessment Methods**

Based on these KPIs, we can measure the effectiveness of each process under an SSR assessment method. The criterion of effectiveness can take on a value of 1-3 as follows, and a higher value means a method is more proficient to achieve the goal of the process:

1: the method is not effective;
2: the method is partially effective;
3: the method is effective.

**Conclusion and Outlook**

Numerous SSR assessment methods are currently available, and many organizations face the daunting task of determining which one to use. The goal of this paper was to develop an easy-to-use framework that organizations can employ to compare different SSR assessment methods. The framework was developed by analyzing three phases of SSR assessment in detail based on two criteria.

Even though this comparative framework put into consideration all phases of SSR assessment based on multiple dimensions, it still needs empirical studies to investigate its applicability.

In our future research, we will use the proposed comparative framework to compare three SSR assessment methods (Josang et al. 2007; Sun et al. 2006; Zhang et al. 2010). Each SSR assessment method in these papers has different application backgrounds. Based on the comparative framework in this article, the strengths and weaknesses of the methods compared will be highlighted. Following, a revised and more detailed framework for comparing SSR assessment methods should be developed on the basis of the results from the multiple case studies.

**REFERENCES**


