Communications of the Association for Information Systems

Volume 34 Article 8

1-2014

A Comprehensive Method to Assess Work System Security Risk

Surya B. Yadav Ph.D.
Texas Tech University, Surya.Yadav@ttu.edu

Tianxi Dong
Dept. of Information Systems and Quantitative Sciences, Rawls College of Business, Texas Tech University

Communications of the Association for Information Systems

CAIS

A Comprehensive Method to Assess Work System Security Risk

Surya B. Yadav

Dept. of Information Systems and Quantitative Sciences, Rawls College of Business, Texas Tech University

Surya.Yadav@ttu.edu

Tianxi Dong

Dept. of Information Systems and Quantitative Sciences, Rawls College of Business, Texas Tech University

Abstract:

This article presents a comprehensive method to assess system security risks. The method includes a cohesive set of steps to not only identify a more complete set of security risks but also assess them in a systematic manner. The method is based on the integration of two kinds of models: (1) qualitative models emphasizing security risk factors and security requirement determination and (2) quantitative models that focus on formal evaluation and assessment of system security risks. Unlike most of the existing methods, the proposed method 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. The article extends existing work on system security risk methods by incorporating new ideas of multifaceted security view and work system in a coherent set of steps. The article demonstrates the application of the proposed method to a real application and discusses the major results.

Keywords: security risk assessment, security risk determination, multifaceted work system security requirement, Security Risk Assessment Method, work system security mechanism

Volume 34, Article 8, pp. 169-198, January 2014

I. INTRODUCTION

More and more businesses are operating in a cyber-world. This phenomenon is presenting bigger challenges as well as opportunities to businesses. One of these challenges is maintaining a secure and stable business infrastructure for a smooth operation of business activities. Managing security risks to business systems is getting more and more complex and time consuming. Companies are facing security risks from multiple sources. According to a recent Bloomberg government study [Engleman and Strohm, 2012], “spies, criminals and hacker-activists are stepping up assaults on U.S. government and corporate systems, spurring efforts by Congress and President Barack Obama to shield infrastructure essential to U.S. national and economic security, such as power grids and water-treatment plants.” Furthermore, the security capabilities of many companies are lagging behind in dealing with the increased security risks [Deloitte, 2012a, 2012b]. Companies must evaluate their security capabilities and improve them effectively in order to deal with the increased threats to business systems. This article makes an attempt to provide a comprehensive method to assess security risks to systems.

The main purpose of system security risk assessment is to evaluate and improve the security of a system under study. Just like any assessment [Ohia, 2011], system security risk assessment is a process involving 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 system. A complete system security risk assessment process is shown in Figure 1.

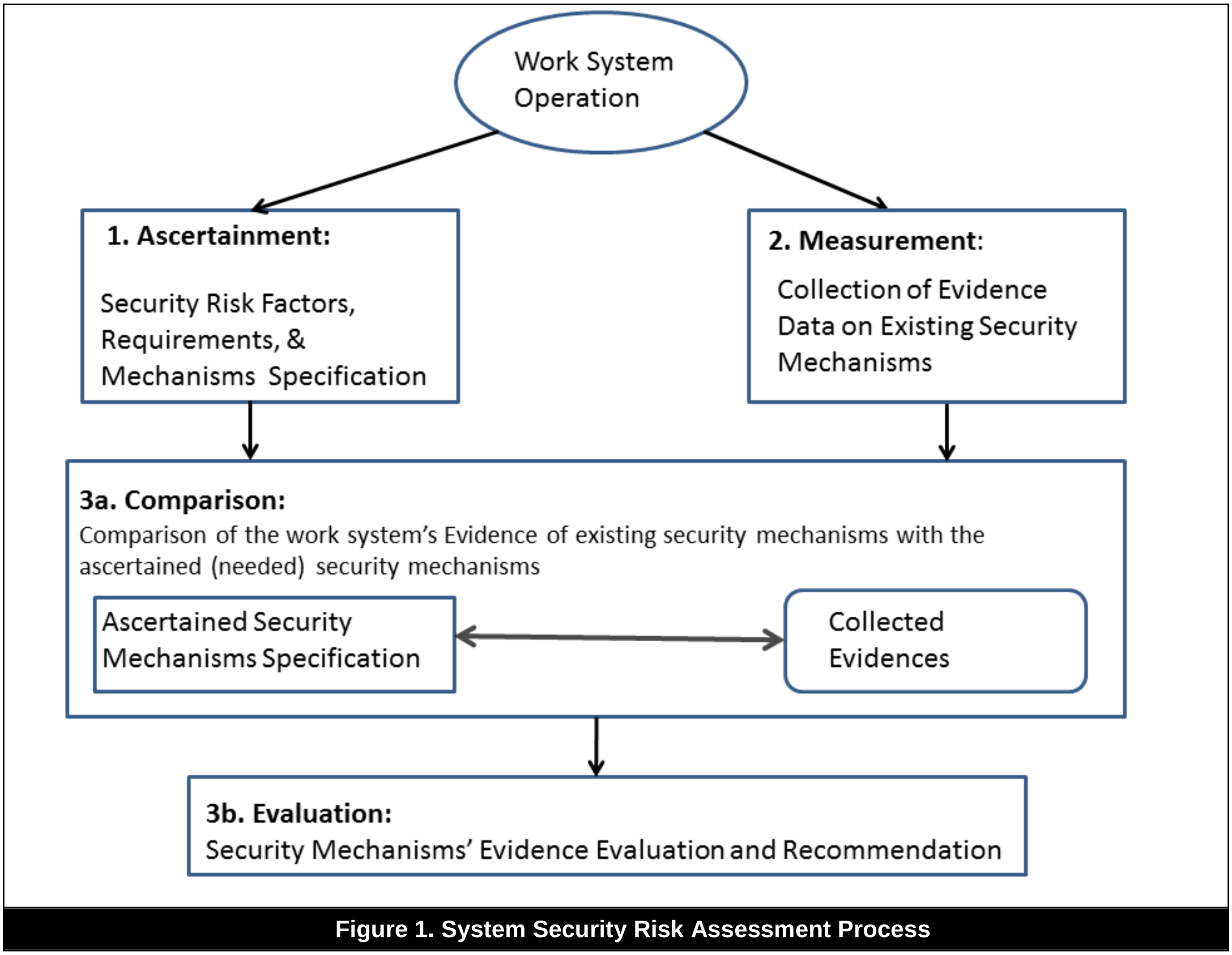

Work System Operation
1. Ascertainment:
Security Risk Factors, Requirements, & Mechanisms Specification
2. Measurement:
Collection of Evidence Data on Existing Security Mechanisms
3a. Comparison:
Comparison of the work system’s Evidence of existing security mechanisms with the ascertained (needed) security mechanisms
Ascertained Security Mechanisms Specification
Collected Evidences
3b. Evaluation:
Security Mechanisms’ Evidence Evaluation and Recommendation

Figure 1. System Security Risk Assessment Process

The process in Figure 1 has three major phases. In the first phase, a work system's [Alter, 2006, 2008] security risk factors are identified based on its scope and the work elements. A set of necessary security requirements are specified to help minimize the impact of the risk factors. An appropriate set of security mechanisms (controls) are then identified to support the security requirements. In the second phase, the security requirements are treated as assertions, and the security mechanisms are treated as evidences. It is assumed that these evidences exist in the work system under study. An appropriate data collection method is used to collect the strength of evidences presumed to be present in the work system. In the third phase, the evidences and their strength are analyzed and compared against the specified security mechanisms. An evaluation of the existing evidences is carried out and a recommendation is made, if necessary, to improve the security of the work system.

As the diagram in Figure 1 suggests, a system security risk assessment process should cover all three phases—(1) the ascertainment of security risk factors, security requirements, and security mechanisms, (2) the measurement or the observation of security evidences present in the work system, and (3) the evaluation of the overall security of the work system.

The current research on system security risk (SSR) assessment has made very good progress. Several research works [Alter and Sherer, 2004; Karabacak and Sogukpinar, 2005; Baker, Rees, and Tippett, 2007; Yadav, 2010] have focused on assessment models to support the ascertainment phase of the security risk assessment process. Other researchers [Stoneburner, 2002; Suh, 2003; ISO 27001; Karabacak, 2005; Caralli, Stevens, Young, and Wilson, 2007] have emphasized steps and methods to support the ascertainment phase. Other researchers [Sun, Srivastava, and Mock, 2006; Feng and Li, 2010] have focused on the measurement and evaluation phases of the assessment process. Most of the research on system security risk, however, has taken only a partial view of the system security risk assessment. A system security risk assessment method should follow the process described in Figure 1 and address the following basic questions:

1. Does it provide guidelines to ascertain the needed security requirements and mechanisms of a work system?
2. Does it provide a way to collect empirical evidence on the security mechanisms present in the work system?
3. Does it provide a way to evaluate the incongruence between the existing and the desired security mechanisms of the work system?

The first question deals with the ascertainment of security goals and requirements of a work system. The second question deals with the collection of evidence on the existing security mechanisms in the work system. The third question deals with the evaluation of the differences between the existing and the desired security mechanisms of the work system. These three questions cover the entire cycle of an assessment process.

This article presents a comprehensive method to determine risk-factor-based security requirements of a system and use them to assess the system's security risks. The method is useful not only for identifying security requirements but also for evaluating the existing security mechanisms against a set of security requirements and assessing the overall system security risks.

The article is organized as follows. Section II presents the literature review. Section III discusses the proposed system security risk method. Section IV demonstrates the application of the method to a real business case. Section V compares the proposed method with the extant methods. Section VI discusses the future research and conclusions, and Section VII presents the limitations.

II. SSR ASSESSMENT LITERATURE REVIEW

Several researchers [Rainer, Snyder, and Carr, 1991; Alter and Sherer, 2004; Vorster and Labuschagne, 2005; Schneider, 2010] have presented an extensive review of the literature on information system security risk assessment. Rainer et al. [1991] have discussed IT risk analysis methods that try to measure loss exposure to IT assets from various threats. They classified methods into two categories—quantitative and qualitative. Quantitative methods require quantitative data and use a mathematical function to relate an IT asset's loss-exposure to its vulnerability to a threat multiplied by the probability of the threat being realized [Rainer et al., 1991]. Qualitative methods use descriptive variables instead of numbers to express IT assets' values and the threat likelihood. Qualitative methods save time and effort but are inexact in nature [Rainer et al., 1991]. Rainer et al. suggest using a combination of various methods in order to achieve the best results. They propose an eight-step risk analysis process that incorporates quantitative and qualitative methods and uses a value chain to identify IT components of each value activity, IT assets, threats, and IT assets' exposure to threats. However, an application of the risk analysis process was not shown. Furthermore, it seems that there is an overuse of the value chain. Alter and Sherer

[Alter and Sherer, 2004; Sherer and Alter, 2004] have focused on IS risk models. They have clarified several IS risk management-related issues. Alter and Sherer studied forty-six articles about IS risk and categorized these articles in terms of definition of risk, model or methods used, type of system or project, and number and type of risk variables. They have proposed a more comprehensive model for analyzing and managing risks. The model provides a good framework for identifying, evaluating, and responding to risks of a work system [Alter, 2002] under various sources of uncertainties, given the goals and expectations of the work system. Vorster and Labuschagne [2005] developed a framework to compare various information security risk analysis methods. First, they used five existing methods—two qualitative methods (OCTAVE [Caralli et al., 2007] and CORAS [Stolen et al., 2002]) and three quantitative methods (ISRAM [Karabacak and Sogukpinar, 2005], CORA—International Security Technology Inc. [IST Inc., 2000], and Information Systems [IS] analysis based on a business model [Suh and Han 2003]) to develop the criteria for their framework. Then, they use the criteria to compare other information security risk analysis methods. Some of the criteria are: whether risk analysis is done on single assets or groups of assets, where in the methodology risk analysis is done, the people involved in the risk analysis, and the main formulae used. The criteria, as can be seen, are based on what some of the extent methods provide and are not based on what organizations need in order to conduct an effective information security risk analysis. Schneider [2010] discusses information security risk management models and analysis techniques within the context of e-government. The security risk faced by an e-government is expansive because of the open nature of e-government [Schneider, 2010]. He has reviewed two security risk assessment processes—the National Institute of Standards and Technology (NIST) assessment process [Stoneburner, Goguen, and Feringa, 2010] and Whitman and Mattord's [2010] assessment process. He concludes that the overarching theme of the risk management processes is the emphasis on the risk assessment and the risk mitigation plan. He also discusses criminological threat assessment techniques and finds an abundance of similarities between the two. Most of the assessment methods have focused on doing risk analysis and planning. Very few researchers [Sun et al., 2006; Feng and Li, 2010] have focused on the risk measurement and its evaluation.

In this article, we present a review of the SSR literature with respect to the overall security risk assessment process presented in Figure 1.

For the ascertainment phase, we examine models and methods to see if they provide:

- Any guidelines to help find security requirements and mechanisms. Some methods and models include very clear and detailed guidelines to help find security requirements and mechanisms, while others provide few guidelines. We use the scale of No Guideline, General Guideline, and Clear Guideline to compare various methods.
- Any output at the end of the ascertainment. Methods produce different kinds of outputs (results) at the end of the ascertainment phase. Some methods produce a listing and others produce a profile of the needed security requirements and mechanisms.

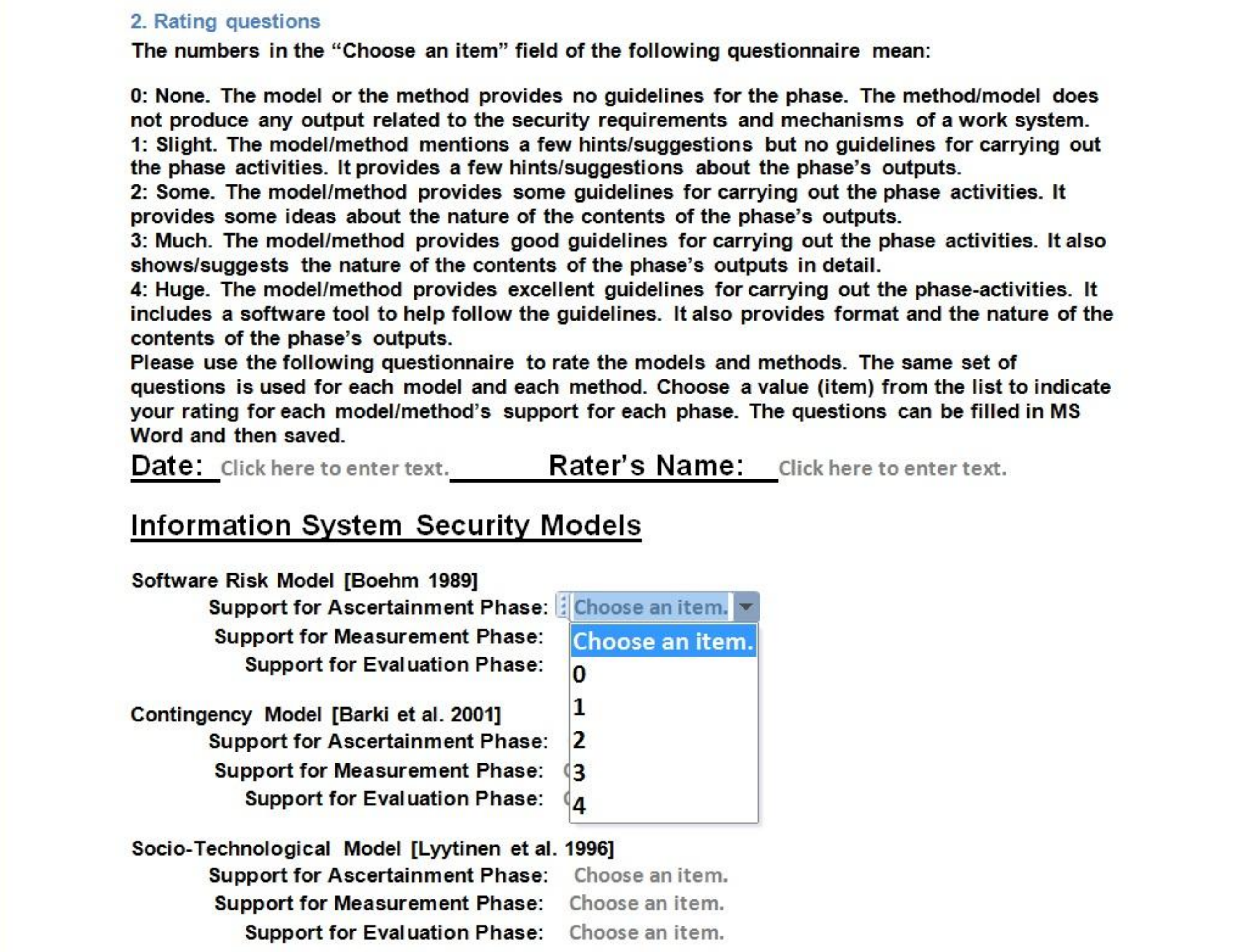
For the measurement phase, we reviewed models and methods to see if they provided any technique for measuring and collecting data as evidence of existing security mechanisms. We also examined the output format of the measurements.

For the evaluation phase, we reviewed methods and models to see if they provided any guidance for analyzing the existing security mechanisms and comparing them with the needed security mechanisms in order to determine the incongruence between them. We also examined the end result of the evaluation phase supported by the methods and models.

Comparison of Extant System Security Risk Assessment Methods and Models

We compared various SSR models against the criteria of ascertainment, measurement, and evaluation phases. We also compared several SSR methods against the same set of criteria. We found that most of the SSR models and methods emphasized mainly the ascertainment phase of the SSR assessment process. For example, Alter and Sherer [2004) have developed a comprehensive model of information system risk. The model clarifies the concept of risk factors and its temporal nature and clearly recognizes the risk management activities. The model [Alter and Sherer, 2004; Sherer and Alter, 2004] provides guidelines in identifying various risk factors. However, the model provides few guidelines for conducting risk analysis and identifying security requirements and mechanisms. We also found that few methods emphasized the measurement and evaluation phases but ignored the ascertainment phase. For example, Sun, Srivastava, and Mock [2006] present a set of steps for measuring and evaluating system security risks. However, their method provides few guidelines for the ascertainment phase of the assessment process. Very few extant models and methods address all three phases of the SSR assessment process.

In addition to our own qualitative comparison of SSR models and methods, three security risk experts also compared the methods and models. To improve the scientific rigor of a qualitative comparison of models and methods, an inter-rater reliability testing of three experts' independent comparison results was performed. We invited three experts (two MIS professors and one MIS Ph.D. student) in the security risk assessment field to compare seven models and nine methods using the ascertainment, measurement, and evaluation criteria. A forty-eight-question survey—with three questions per model/method—was prepared. Figure 2 shows the scale and a few sample questions from the survey. Questions relate to ascertainment, measurement, and evaluation phases. Each question has five possible choices—0, 1, 2, 3, and 4—as defined in Figure 2. The forty-eight-question survey was emailed as an attachment to each expert on April 5, 2012. A link to a Dropbox folder containing literature related to the seven models and nine methods was also provided to the experts for easy reference. The survey was completed by April 16, 2012. Each of the three experts (raters) answered all forty-eight questions.



2. Rating questions

The numbers in the "Choose an item" field of the following questionnaire mean:

0: None. The model or the method provides no guidelines for the phase. The method/model does not produce any output related to the security requirements and mechanisms of a work system.
1: Slight. The model/method mentions a few hints/suggestions but no guidelines for carrying out the phase activities. It provides a few hints/suggestions about the phase's outputs.
2: Some. The model/method provides some guidelines for carrying out the phase activities. It provides some ideas about the nature of the contents of the phase's outputs.
3: Much. The model/method provides good guidelines for carrying out the phase activities. It also shows/suggests the nature of the contents of the phase's outputs in detail.
4: Huge. The model/method provides excellent guidelines for carrying out the phase-activities. It includes a software tool to help follow the guidelines. It also provides format and the nature of the contents of the phase's outputs.
Please use the following questionnaire to rate the models and methods. The same set of questions is used for each model and each method. Choose a value (item) from the list to indicate your rating for each model/method's support for each phase. The questions can be filled in MS Word and then saved.

Date: Click here to enter text. Rater's Name: Click here to enter text.

Information System Security Models

Software Risk Model [Boehm 1989]
Support for Ascertainment Phase: Choose an item.
Support for Measurement Phase:
Support for Evaluation Phase:

Contingency Model [Barki et al. 2001]
Support for Ascertainment Phase:
Support for Measurement Phase:
Support for Evaluation Phase:

Socio-Technological Model [Lyytinen et al. 1996]
Support for Ascertainment Phase: Choose an item.
Support for Measurement Phase: Choose an item.
Support for Evaluation Phase: Choose an item.

Figure 2. The Rating Scale and a Few Sample Survey Questions

Survey Results

Based on the data from the questionnaire, mean scores for each model and each method for different criteria were calculated, and an inter-rater reliability was determined by using the method in James' [1984] work. The overall inter-rater reliability for the comparison of SSR Models and Methods was 0.99 and 0.98, respectively. Even though there are no established standards for an acceptable level of reliability, Neuendorf [2002] reviewed "rules of thumb" set out by several methodologists and concluded that "inter-rater reliability coefficients of .90 or greater would be acceptable to all, .80 or greater would be acceptable in most situations, and below that, there exists a great disagreement" (p. 145). The overall inter-rater reliability score for the comparison of SSR Models and Methods shows that all experts gave the same or similar scores to each of the survey items. Table 1 separately show the comparison of SSR Models and Methods. The numbers in parentheses show the inter-rater reliability scores for the corresponding average score. The survey results confirm our comparative analysis of various extant models and methods.

Table 1: Comparison of SSR Models

Phase		Ascertainment	Measurement	Evaluation
Variable		Support for Ascertainment phase: Guidelines to help find security requirements, mechanisms, and outputs	Support for Measurement phase: Guidelines for data collection and outputs	Support for Evaluation phase: Guidelines for evaluating the incongruence and outputs
SSR Models	Software Risk Model [Boehm, 1989]	1[a] (1)[b]	0 (1)	0 (1)
	Contingency Model [Barki et al., 2001]	1 (1)	0 (1)	0 (1)
	Socio-technological Model [Lyytinen et al., 1996]	1.33 (0.83)	0 (1)	0 (1)
	Options Model [Benaroch, 2002]	1 (1)	0.33 (0.83)	0.33 (0.83)
	Performance Model [Nidumolu, 1995; Nidumolu, 1996]	0.67 (0.83)	0 (1)	0 (1)
	Risk Analysis Framework [Alter et al., 2004]	1.33 (0.83)	0 (1)	0 (1)
	Security Requirement Framework [Yadav, 2010]	3.33 (0.83)	0 (1)	0 (1)
SSR Methods	OCTAE Allegro [Caralli, 2007]	2[a] (0.5)[b]	0.33 (0.83)	0 (1)
	CORAS [Stolen et al., 2002]	2.33 (0.83)	0.33 (0.83)	0 (1)
	ISRAM [Karabacak et al., 2005]	2.33 (0.83)	0 (1)	0 (1)
	IS business model [Suh et al., 2003]	1.67 (0.83)	0.33 (0.83)	0 (1)
	PDCA [ISO, 27001]	2 (0.5)	0.33 (0.83)	0 (1)
	NIST [Stoneburner et al., 2002]	2 (0.5)	0.33 (0.83)	0 (1)
	SSRA Model [Sun et al, 2006]	0 (1)	3 (0.5)	2.67 (0.83)
	Metric-driven Threat Scenarios [Baker et al., 2007]	1 (0.5)	0.3 (0.83)	0 (1)
	Combined Risk Analysis [Rainer et al., 1991]	1.33 (0.83)	0.33 (0.83)	0 (1)

a: the mean of rating scores; b: Inter-rater reliability of three experts

III. COMPREHENSIVE METHOD FOR SSR ASSESSMENT

Here we discuss a comprehensive method, henceforth called the Multi-View Work System Security Assessment (MVWSSA) method, for assessing the security risks of a work system. We start with the identification of the assets and determine a complete set of security risks. An appropriate set of security requirements are then identified to counter the security risks. A set of security mechanisms is determined to implement the security requirements. For evaluation, we turn around and treat the security requirements as assertions and the associated security mechanisms as evidence to develop an assertion–evidence diagram. The strength of evidence is collected for the work system under study. The assertion–evidence diagram is then used to analyze and evaluate the security risks, and a recommendation report is prepared. The proposed method consists of the following steps:

1. Establish the target work system and the scope of the risk assessment.
2. Identify assets belonging to the work system's elements.

3. Identify risk factors for each asset using Six-View Perspective of System Security (SVPSS).
4. Evaluate and prioritize security risk from risk factors.
5. Identify security requirements (assertions) to prevent and mitigate the security risks.
6. Establish preventive and mitigation security mechanisms (evidences) present in the system to help manage the security risks.
7. Develop security assertion-evidence diagram for each asset.
8. Collect and represent the strength of evidence.
9. Assess the overall level of security risk to each asset.
10. Recommend preventive and mitigation security mechanisms.

Each step is discussed below in details.

Step 1. Establishment of Target Work System and the Risk Assessment Scope

This step establishes the purpose and the context of the assessment effort. The purpose relates to the reason as to why we want to conduct certain activities. The context relates to the subject matter of the assessment under consideration. A clear understanding of the purpose and context results in a more precise boundary and scope of the assessment activities. A work system should be identified with a well-defined boundary. Identification of the security risks of a system requires a deep understanding of its processing environment. The work system-related information, such as the system's mission, security policies, system interfaces, business processes, etc., should be collected. Steve Alter [2006, 2008] provides a comprehensive work system framework for understanding and defining organizational systems. We use his definition of a work system and its elements to collect information on the boundary and the scope of the risk assessment of a system.

Step 2. Identification of Assets Belonging to the Nine-Elements of Work System

Identification of all the assets that might face security threats is one of the most critical activities in assessing security risks. We use the Work System framework [Alter, 2006, 2008] to provide a more complete guideline for identifying all assets that might be under security risk. Table 2 lists typical assets under the integration of these two frameworks. In order to identify a more complete set of assets under each work element, each work system element [Alter, 2006, 2008] can be viewed from multiple perspectives such as the management, process, and resource perspectives. Table 2 can be used as a guide by system analysts to identify a more complete set of assets belonging to a work system under study.

Step 3. Identification of Risk Factors for Assets Using Six-View Perspective of System Security (SVPSS)

Risk factors, here, represent various sources of risks to assets [Alter, 2002]. In this step, we use the SVPSS framework [Yadav, 2010] to identify all sources of risks for assets. Each asset, identified in Step 2, is examined under each view of SVPSS for a security risk. Table 3 illustrates typical risk factors under each view. These risk factors can be used as a guide to enumerate specific risk factors for each asset.

Step 4: Evaluation and Prioritization of Security Risks from Various Risk Factors

We analyze and evaluate security risks from the identified risk factors by following some of the steps of the risk assessment methodology by CMS [2005]. Several works [Stoneburner et al., 2002; Australia, 2004; NIST, 2004; ISO, 27001; CMS, 2005] have presented a similar process to conduct risk analysis and evaluation. We adopt the risk analysis and evaluation steps of the risk assessment methodology by CMS [2005]. These two steps involve the following tasks:

- Estimate each risk factor's likelihood of occurrence.
- Establish the severity impact if the risk materializes.
- Determine the level of risk based on the risk factor's likelihood and its impact.
- Establish acceptable level of risk for evaluating risks.
- Compute the priority level of each risk factor.

Table 1: An Extensive List of Typical Assets Under Each of the Work System's Elements

Work System Elements	List of Assets Under Each of the Work System's Elements
Processes and Activities	Process Interface, Process Infrastructure, Process Operator, Process Manual, Process Standards, Compliance Process, Process Policy, Process Ownership, Planning and Control Mechanism Within a Process, Process Methods, Process Design, Process Execution, Process Assessment Criteria, Process Assessment Measures
Participants	Worker, Manager, Leader, Team, Manager Skills, Worker Knowledge, Team-Skills, Employee-confidentiality, Equal Employment Opportunity Compliance, Individual Accountability, Personnel Screening, Security Awareness Training, Personnel Policy, Remediation Policy, Process-training, Process–Actor Interface, Code of Practice, Performance Criteria, Performance Evaluation, Assessment Training
Information	Data Backup, Work System (i.e., Organizational) Knowledge, Personal Information, Access Rights, Evaluation of Access Rights, Privacy Law Compliance, Privacy Policy, Information-sharing Policy, Policy Review, Policy Administration, Process Inputs, Process Outputs, Process Maintenance, Process Design Standards, Process Monitoring, Assessment Policy, Assessment Method, Assessment Data
Technologies	Laptop, Desktop, Tablet PC ; Software Application, Application Manual; Access Control; Management Techniques; Monitoring Tools; Tracking Tools; User-interface; Technology-process Integration; Technology Assessment Policy; Technology Assessment Criteria
Products & Services	Product Review, Product Packaging, Service Review, Product Specification, Service Specification, Product Design Standards, Product Compliance, Service Compliance, Quality Control, Quality Monitoring, Product Inspection, Product Evaluation, Product Design Process, Service Design Process, Product Manufacturing Process, Quality Assurance Criteria, Quality Assurance Policy
Customers	Customer, Employee, Customer Goodwill, Customer Data, Employee Data, Customer Privacy Compliance, Employee Privacy Compliance, Equal Employment Opportunity Compliance, ADA Compliance, Customer Privacy Policy, Employee Privacy Policy, Remediation Policy, Employee Accountability, Security Awareness Training, Personnel Screening Policy, Duty Segregation Policy, Employee Termination Security Policy; Customer Care Process, Employee Care Process, Employee Grievance Handling Process, Quality of Service Criteria, Quality of Service Policy, Quality of Service Assessment
Environments	Workplace Location, Location Perimeter, Human Resource; Control–Environment, Workplace Culture, State Environmental Regulations, Federal Environmental Regulations, Human Resource Policy, Control–Environment Policy, Secure Workplace Policy, Human Resource Hiring Process, Human Resource Management Process, Workplace Design Process, Location Perimeter Security Criteria, Location Perimeter Security Assessment, Workplace Security Assessment
Infrastructure	Server, LAN, Router, Disk Array, Building, Shared Database, Server Applications, Software License, Database License, Software Maintenance Agreement, Software Training, Software License Policy, Software Maintenance Policy, User Training Policy, Infrastructure Security Policy, Building Security Policy, Infrastructure Design Process, Infrastructure Review Process, Server Setup Process, Infrastructure Performance Criteria, LAN Security Assessment
Strategies	Work System Operation, Work Force, Work Design, Work Schedule, Occupational Safety and Health Act (OSHA) Compliance, OSHA-related Work System Policy, Work Design Policy, Work Schedule Policy, Work Assembly Process, Work Design Process, OSHA Compliance Assessment, Work System Operation Assessment

We use a security risk register [Yadav, 2010] to document the risk evaluation outcome. A security risk register is a compact and tabular representation of risk details about each risk factor. A sample security risk register template is shown in Figure 3.

Table 2: Risks Under Six-View Perspective of System Security Framework [Yadav 2010]

Six-View Perspective	Typical Risk Factors
Threat View	Natural disasters, malicious threats, non-malicious threats
Resource View	Non-availability, compromised integrity, disclosure of confidential resources
Process View	Weak points in a process, vulnerabilities in the interface between the actors and the processes, and failures of processes
Assessment View	Inadequate and poor assessment criteria, inadequate assessment methods and procedures, lack of clarity and transparency in assessment methods, and lack of clear roles and responsibilities of assessment staffs
Management View	Poor and/or the lack of policy, accountability, administration, monitoring, remediation
Legal View	Violation of security and privacy laws, security-related legal uncertainties, and litigation

Assets	Security Views	Sources of Risk or Risk Factors	Threat Likelihood Estimate for Each Risk Factor[a]	Impact Severity (if the threat is realized)[b]	Resultant Risk Level[c]	Acceptable Risk Level Rating[d]	Risk Priority Rating[e]	Security Requirements	Security Mechanisms

Note: [a] Values are: Negligible, Very Low, Low, Medium, High, Very High, or Extreme
[b] Values are: Insignificant, Minor, Significant, Damaging, Serious, or Critical
[c] Values are: Nil, Low, Medium, High, or Very High
[d] Values are: Very Low, Low, Moderate, High, or Very High
[e] Values are: 0 = Very Low, 1 = Low, 2 = Moderate, 3 = High, or 4 = Vey High

Figure 3. Security Risk Register Template to Document Risk Factors

Figure 3 shows only the headings for each column in the security risk register. These columns will be completed in the subsequent steps. The security risk register template, as shown in Figure 3, has one main row for each identified asset. For each asset-row, there can be several risk factors under various security views. For each risk factor, a threat likelihood estimate and an impact severity is determined. Threat likelihood is an estimate of the frequency or chance of a threat happening [NIST, 2004]. Qualitative measures are used to specify the threat likelihood estimate and the impact severity level. Several works [Australia, 2004; CMS, 2005] on risk analysis use qualitative scales for defining and determining the threat likelihood and its impact. For example, a qualitative scale consisting of "Negligible," "Very Low," "Low," "Medium," "High," "Very High," and "Extreme" values can be used to specify the level of threat likelihood estimate. Table 4 defines the scales based on the CMS Information Security Risk Assessment (RA) Methodology [CMS, 2005]. An alternative interpretation of the scale values in terms of probability, shown in Table 4, gives additional information about the nature of likelihood estimation.

Table 3: Likelihood Scale Description

Scale for Likelihood Estimate	Scale Description	An alternative description in terms of probability
Negligible	Unlikely to occur	> 1/10,000
Very Low	Likely to occur two/three times every five years	> 1/1,000
Low	Likely to occur once every year or less	>1/100
Medium	Likely to occur once every six months or less	>1/10
High	Likely to occur once per month or less	>1/5
Very High	Likely to occur multiple times per month	>1/2
Extreme	Likely to occur multiple times per day	>3/4

Table 5 defines the scale for the impact severity level [CMS, 2005]. The impact severity scale is defined based on several works [ISO, 27001; Stoneburner et al., 2002; and Shrestha, 2004] on security risk assessment. The scale description and their association with the financial loss amount in Table 5 should help an analyst establish the most appropriate scale value for a severity impact.

Table 4: Impact Severity Level Scale		
Impact Severity Scale	Description	Financial Loss (in US$)
Insignificant	Will have almost no impact if the threat occurs Will result in minimal loss of functional integrity Requires little or no recovery cost	Up to 10,000
Minor	Will have some minor effect on the business function May cause minor financial loss, but will not result in negative publicity or political damage Will require only minimal effort to complete corrective actions and continue or resume operations	10,001 to 100,000
Significant	Will result in some tangible harm, albeit negligible, and perhaps realized by only a few individuals or agencies May cause political embarrassment, negative publicity, and moderate financial loss Will require a moderate expenditure of resources to repair	100,001 to 500,000
Damaging	May cause damage to the reputation of the company, and/or notable loss of confidence in the ability for the company to complete its stated business mission May result in legal liability, and will require significant expenditure of resources to complete corrective actions and restore operations	500,001 to 1,000,000
Serious	May cause considerable disruption in the business function and/or loss of customer or business partner confidence May result in compromise of large amount of government information or services, a substantial financial loss, and the failure to deliver CMS public programs and services	1,000,001 to 5,000,000
Critical	May cause an extended disruption in the business function, and may require recovery in an Alternate Site environment May result in full compromise of the company's ability to provide public programs and services, and complete the stated business mission	Above 5,000,000

A risk level or simply a risk is defined as a function of the likelihood of a given risk factor and its impact severity. A risk level is then computed using the following expression shown as (1):

$$\text{Risk level} = \text{Threat Likelihood Estimate} * \text{Impact Severity} \quad (1)$$

The level of risk can be easily determined by using the risk level matrix in Table 6. Each cell in Table 6 shows a risk level value for each combination of threat likelihood estimate and impact severity level based on Equation 1 above. For example, using Equation 1, a threat likelihood value of "Low" combined with the impact severity level of "Minor" results in a value of "Low" as shown in Table 6. Thus, the scale for a risk level can be specified in terms of "Very Low," "Low," "Moderate," "High," and "Very High" [CMS, 2005].

Table 5: Risk Levels Based on the Combinations of a Likelihood Occurrence with an Impact Severity

Likelihood of Occurrence	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Very Low	Very Low	Very Low	Low	Low	Low
Very Low	Very Low	Very Low	Low	Low	Moderate	Moderate
Low	Very Low	Low	Moderate	Moderate	High	High
Medium	Very Low	Low	Moderate	High	High	Very High
High	Low	Moderate	High	High	Very High	Very High
Very High	Low	Moderate	High	Very High	Very High	Very High
Extreme	Low	Moderate	Very High	Very High	Very High	Very High

According to Table 6, we have five levels of risk level. Table 7 assigns a numerical value for each risk level.

Table 6: A Numerical Rating for Each Risk Level	
Risk Level	Numerical Value
Very Low	0
Low	1
Moderate	2
High	3
Very High	4

Thus, a risk priority rating level can be computed based on a given acceptable risk level rating using the following expression shown in (2):

Risk Priority Rating level = Resultant Risk Level Rating – Acceptable Risk Rating Level (2)

A resultant risk level rating is a value from Table 7 based on the values of the threat likelihood and impact severity as per Table 6. An acceptable risk rating is a risk rating that is acceptable to the organization under study. The acceptable risk rating is specified by the owner of the work system under study. A numerical value between 0 and 4, as shown in Table 7, is used to specify an acceptable risk rating level. Thus, using Tables 6 and 7 and the risk-rating computation expression of (2), a risk priority rating level can be computed for each risk factor listed in the security risk register.

The above computational process to estimate the threat likelihood and the various risk levels are discussed extensively in various literatures [NIST, 2004; ISO, 27001; CMS, 2005].

Step 5. Identification of Security Requirements (Viewed as Assertions) to Mitigate Security Risks

By now, we have identified the risk priority rating for each risk factor of an asset. A risk priority rating level shows the importance of a risk factor. The higher the risk priority level of a risk factor, the higher is the need to identify the appropriate security requirements in order to mitigate the impact from that risk factor. A security requirement can be viewed as an action that a work system must take to protect itself from various risk factors. Table 8 illustrates typical security requirements under each security perspective. Table 8 can act as a guide/checklist to identify security requirements.

A comprehensive set of security requirements enables a work system to come up with a more complete set of mechanisms (controls) to manage security risks.

Table 8: Security Requirements Under Six-View Perspective of System Security Framework	
Six-View Perspective	Typical Security Requirements
Threat View	Backup data, Detect Intrusion, Thwart Flood Attack, Thwart Buffer Overflow Attack, etc.
Resource View	Maintain Confidentiality of a resource, Maintain Integrity of a resource, Maintain Availability of a resource, Maintain Reliability of a resource
Process View	Develop secure processes for dealing with threats, Develop secure processes for protecting resources, Develop secure processes for managing legal and privacy requirements, Manage secure process integrity, Conduct audit of secure processes
Assessment View	Conduct periodic testing and evaluation of the effectiveness of security policies and plans, Define assessment policy, Evaluate assessment criteria
Management View	Establish Security Policy and Procedures, Establish Accountability, Administer Security, Monitor Security, Handle remediation
Legal View	Enable Privacy, Comply with Privacy and Security Laws

Step 6. Specification of Security Mechanisms (Evidences) to Help Manage Security Risks

Mechanisms refer to standards, methods, techniques, and tools that can be implemented into a work system to deal with threats and other concerns. Table 9 shows examples of several types of mechanisms. Mechanisms are specified to support each security requirements identified in the previous step. One mechanism can obviously support more than one security requirements. System security risk management can be more effective by deploying security mechanisms in a multilayer of system defenses. Reduction in security risks can be accomplished by applying several lines of system defense in sequence [Straub, 1998]. These lines of system defense are deterrence, prevention, detection, and recovery [Straub, 1998]. Loch, Carr, and Warkentin [1992] classify the lines of defense as protection, reduction, transfer, and financing. Based on the above two schemes, we classify security mechanisms under the following types of lines of system defense:

1. Prevention
2. Mitigation
3. Transfer
4. Financing

Please refer to the appropriate sources [Straub, 1998; Loch, 1992; Mirkovic and Reiher 2004] for more details. Table 9 presents a useful distinction among security mechanisms that can be used by managers and analysts to fine-tune the selection of appropriate countermeasures. Several security mechanisms, such as intrusion detection systems and audit logs, can be classified as both preventive and mitigation mechanisms. However, they are shown under only one category based on the nature of their predominant use.

Table 9: Security Mechanisms Under Six-View Perspective of System Security Framework

Security View	Classification of Security Mechanisms	Security Mechanisms
Threat	Prevention	Threat Security Policy, Security Awareness and Training, Equipment Security, Access Control, Cryptography, Compliance with Threat Security Policy
	Mitigation	Backup Procedure, Intrusion Detection System, Reconfiguration Mechanism
	Transfer	Outsourcing, Compliance Outsourcing
	Financing (Coping)	Threat Security Insurance
Resource	Prevention	Resource Policy, Formal Standards for Establishing User Access, User ID Management, Management of Outside Users' Access, Periodic Evaluation of Access Rights, Approval of Access Rights, Resource Testing, Resource Maintenance
	Mitigation	Resource Monitoring, Resource Redundancy, Data backup, Reconfiguration Mechanism
	Transfer	Resource Outsourcing
	Financing	Resource Security Insurance
Process	Prevention	Separation of Duties, User Account Controls, User Training, Swift Termination-Replacement Action, Process design Standards, Process Policy, Backup Controls
	Mitigation	Process Audit Log, Process Monitoring
	Transfer	Business Process Outsourcing
	Financing	
Assessment	Prevention	Assessment Policy, Assessment Training, Assessment Standards, Assessment Tools, Security Audit Tools, Penetration Analysis Tools, Vulnerability Detection Tools, Security Scanner Tools
	Mitigation	Intrusion Detection System, Assessment Data Log
	Transfer	Assessment Outsourcing
	Financing	
Management	Prevention	Policies and Procedures, Personnel Screening, Security Awareness Training, Backup Procedures, Vulnerability Assessment Tools, Facility Protection, Disposal of Unclassified Hard Drive and Other Devices, Scanning Tools, Configuration Management Tools, Monitoring, Swift Termination-handling Policy
	Mitigation	Recovery Tools, Reconfiguration Tools, Intrusion Detection System
	Transfer	Facility Protection Outsourcing
	Financing	
Legal	Prevention	Access Policy, Privacy Policy, Transparency and Control of Access Privileges, Audit History Reporting, Structured Access Privileges, Centralized Authentication and Authorization, Audit Log, Cross Functional Security Committee, Secure Shredding Bins, Spam Reporting, Spam Handling Tools
	Mitigation	Audit Log, Intrusion Detection System
	Transfer	Legal Outsourcing
	Financing	Liability Insurance

Step 7. Development of the Security Assertion-Evidence Diagram

So far, the MVWSSA method has covered the ascertainment phase of the assessment process. Based on the goals and the context of a work system, the above steps help identify the risk factors, security requirements, and security mechanisms. Steps 7 and 8 relate to the measurement phase of the assessment process. Here, we specify assertions and evidences and then collect data on evidences. We turn around and view the identified security mechanisms as if they already existed in the work system. We treat these security mechanisms as evidence for measurement purposes. This evidence, in turn, supports the security requirements, henceforth called assertions. We construct an assertion–evidence diagram for each asset of the work system. An assertion–evidence diagram [Sun et al, 2006] consists of assertions, evidence, and their interrelationships. An assertion is basically a proposition that is logically supported by facts, observations, and illustrations. Evidence is a fact or information indicating whether an assertion is true or false. Assertions are generally organized in a hierarchical structure, including a main assertion and several sub-assertions. The main assertion is the highest level of assertion; the sub-assertions relate to the main assertion. Evidence represents the information that supports or negates assertions. In our method, a high level proposition about the security of an asset is the main assertion. All identified security requirements are treated as sub-assertions. The security mechanisms, as indicated earlier, are viewed as evidences. A security assertion-evidence diagram is in the form of a tree structure where each leaf node represents evidence. As an illustration, let us say that we have identified a Web server as an asset to be protected. In that case, the proposition "the Web server is protected" can be taken as the main (highest level) assertion about the security of the Web server. The identified security requirements to reduce the impact of each risk factor on the Web server are restated as propositions and viewed as sub-assertions. The needed security mechanisms are viewed as the evidence. Figure 4 shows a partial assertion–evidence diagram with the various levels of assertions and evidences. In Figure 4, an oval-shape symbol is used to represent an assertion. A rectangular-shape symbol is used to represent evidence.

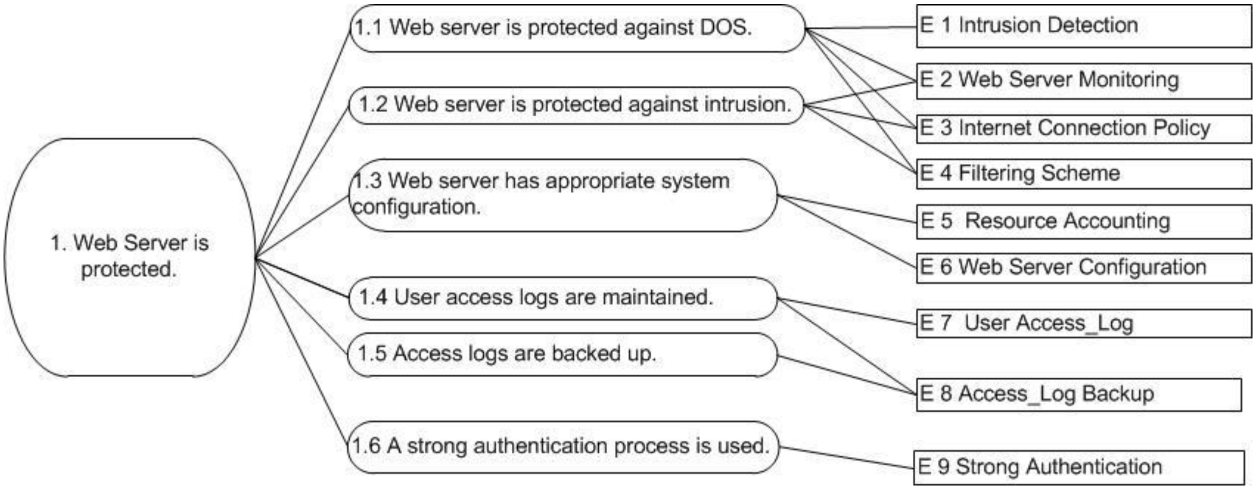

1. Web Server is protected.
1.1 Web server is protected against DOS.
1.2 Web server is protected against intrusion.
1.3 Web server has appropriate system configuration.
1.4 User access logs are maintained.
1.5 Access logs are backed up.
1.6 A strong authentication process is used.
E 1 Intrusion Detection
E 2 Web Server Monitoring
E 3 Internet Connection Policy
E 4 Filtering Scheme
E 5 Resource Accounting
E 6 Web Server Configuration
E 7 User Access_Log
E 8 Access_Log Backup
E 9 Strong Authentication

Figure 4. A Partial Assertion-Evidence Diagram—An Illustration

Step 8. Collection and Representation of Evidence Strength

In this step, users and/or resident experts specify the strength of evidence, which indicates the level of support that a piece of evidence provides in favor of and/or against the assertion to which it pertains. Strength of evidence is represented by m-values [Shafer, 1976; Sun et al., 2006]. The m-value is the basic probability assignment function in Dempster-Shafer Theory (DST) of Evidence [Shafer, 1976]. Evidence strength in the form of m-values is collected using various data collection techniques such as interview and survey. Evidence strength can also be obtained as a consensus based on inputs from multiple experts in order to avoid individual subjective judgment. The overall evidence strength of an evidence is represented as a m-value pair {n1, n2} where n1 represents the degree of belief by an assurance provider (user) that the evidence (security mechanism) is present in the work system, and n2 represents the degree of belief by the assurance provider that the evidence is not present in the work system. The difference of 1- n1- n2 represents the ignorance assigned to the ambiguity of whether the evidence is present or not. In other words, let us say that there is an evidence "e" and the assurance provider feels positive about it and provides a support level of, say, 0.7 that the evidence "e" is present in the work system. At the same time, the assurance provider feels that there is no reason to believe that the evidence is not present (~e). This means that 0.7 degree of support is assigned to "e," 0.0 degree of support to "~e," and the remaining 0.3 is ignorance assigned to the case of "not sure" {e, ~e}. Using a mathematical notation, we say m(e)=0.7, m(~e)=0.0, and m(e,~e)=0.3 where m(e) is the degree of support for "e" being true, m(~e) is the degree of support for "e" being not true, and m(e,~e) is the degree of support for not being sure.

Step 9. Assessment of the Overall Level of Security Risk to Each Asset

In this step, beliefs (belief functions) on assertions are computed by combining the strength of evidence (m-values) based on the diagram's structure. This is done by propagating m-values through the diagram based on the Dempster's rule of evidence combination [Sentz and Ferson, 2002; Sun et al., 2006]. The overall belief on each main assertion related to an asset is also computed based on the assertion–evidence diagram created in the previous step. The overall belief is computed using the Dempster's rule for combining multiple belief functions and propagating m-values from sub-assertions back to the main assertion [Sentz and Ferson, 2002; Sun et al., 2006].

The computed overall belief function of a main assertion represents the assurance provider's level of confidence in the main assertion. For example, let us say that the computed overall belief function of the assertion "the Web server is protected" is {0.85, 0.0}. This means that the assurance provider is 85 percent confident that the main assertion "the Web server is protected" is true and 0 percent confident that the main assertion is not true. There is, however, a 15 percent ambiguity that the main assertion is not adequately protected. In other words, we can say that there is a 15 percent overall security risk that the Web server is not adequately protected.

The belief function of a main assertion is then compared against the pre-established security risk tolerance level as specified by the work system for each asset. The security risk tolerance level is specified for each asset by the owner of the work system under study. This evaluation then becomes the basis for the recommendations of new/additional security mechanisms. A tabular structure shown in Table 10 can be used to document the assessment results of the overall security risk for each asset.

Table 10: A Tabular Structure to Document the Assessment Results

Assets (name and description)	Overall Belief Function of the main assertion	Belief Value for "not sure" (ignorance) in %	Pre-established Risk Tolerance Level in %	Recommended Mechanisms	
				Preventive	Mitigation
Asset #1	…	...			
Asset #2	…	…			
Asset #n	…	…			

The given risk tolerance level is then compared against the computed ignorance (not sure) risk level. If the ignorance risk level is higher than the given risk tolerance level, the suitable security mechanisms should be recommended to reduce the ignorance risk level. It may also be necessary to reexamine the adequacy of the identified security requirements before recommending the appropriate security mechanisms. A reassessment of the work system's security risk with the added security mechanisms can be easily performed by repeating Steps 8–10 of the MVWSSA method. A software tool to automate the MVWSSA steps would be highly desirable.

Step 10. Recommendation of Preventive and Mitigation Security Mechanisms

In this step, a set of preventive and/or mitigation security mechanisms are recommended based on the evaluation of the overall belief function of each asset. The suggested mechanisms can be documented in Table 10, shown above. These recommendations can be explained in the form of a simple report that can be used as a guide for revamping/fine-tuning the security mechanisms of the work system.

The above steps are illustrated through a real case in the next section.

IV. APPLICATION OF THE MVWSSA METHOD

We apply the Multi-View Work System Security Assessment (MVWSSA) method to assess the security risk of the University Digital Signage (UDS) system of a major university. The UDS system is relatively a new application, and it is currently in operation at the XYZ University. The real name of the university has been disguised in order to maintain anonymity. We approached the CIO of the university with a proposal to assess the security risk of a system within the IT Division. The CIO agreed and showed interest in assessing the security risk of the UDS system. The Assistant Vice President (AVP) for IT and ISO and a PC/Network support person participated in the assessment project on a regular basis. We refer to them as administrators in the subsequent discussions.

The UDS system is described in Appendix A as a case study. A digital signage system is a form of an electronic display system that shows television programming, menus, information, advertising, and other messages. UDS supports digital signs (such as LCD, LED, plasma displays, or projected images) similar to the ones found in public and private environments, such as retail stores, hotels, and restaurants, as well as corporate or institution buildings.

Target Work System and Its Scope

Here we establish the scope of the work system and define its boundary. The UDS system of the XYZ University is viewed as a target work system for assessing its risks. Figure 5 shows the scope of UDS as a work system. The work system serves several kinds of customers (users and consumers)—faculty, staff, students, and administrators.

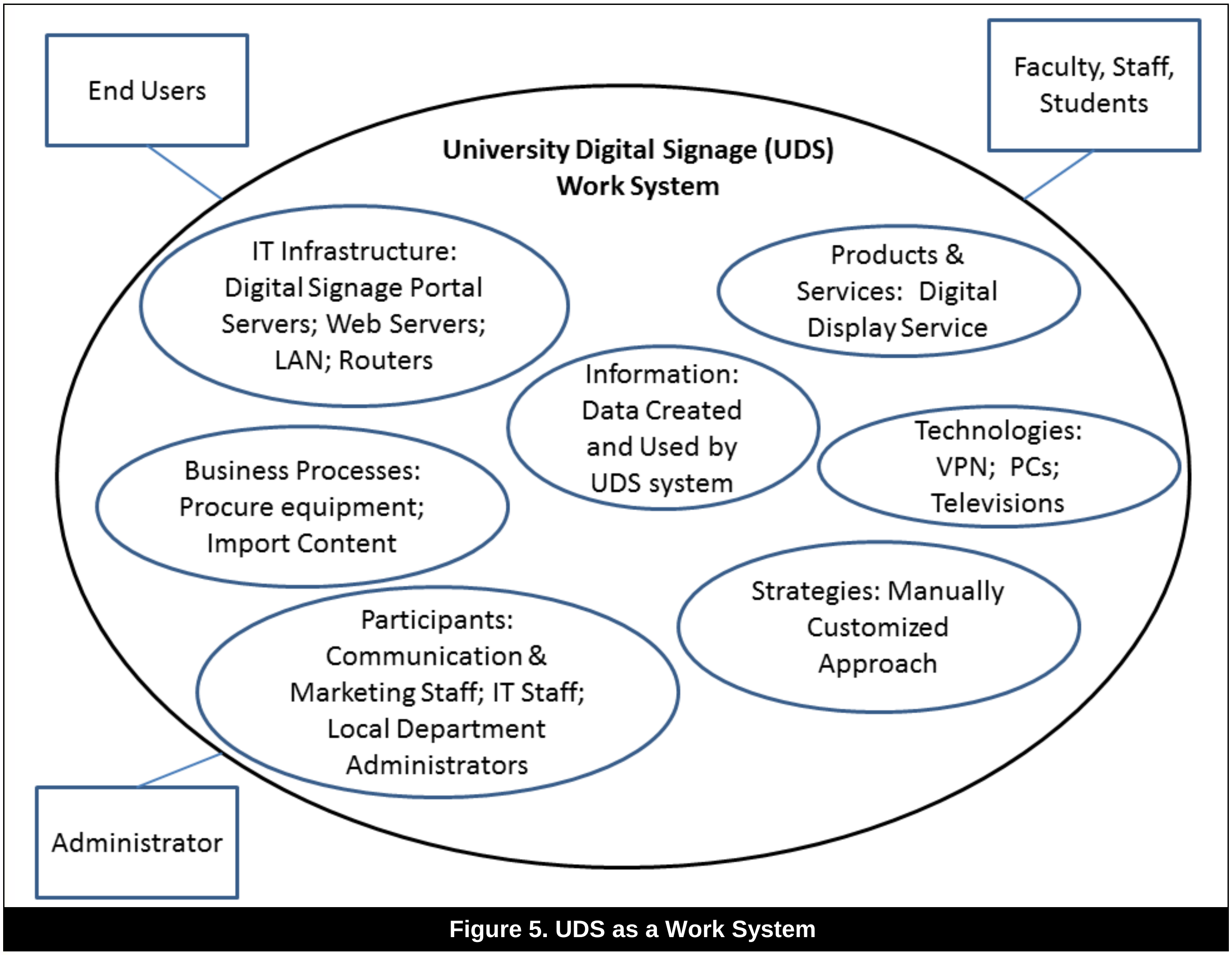

End Users
Faculty, Staff, Students
University Digital Signage (UDS) Work System
IT Infrastructure: Digital Signage Portal Servers; Web Servers; LAN; Routers
Products & Services: Digital Display Service
Information: Data Created and Used by UDS system
Technologies: VPN; PCs; Televisions
Business Processes: Procure equipment; Import Content
Strategies: Manually Customized Approach
Participants: Communication & Marketing Staff; IT Staff; Local Department Administrators
Administrator

Figure 5. UDS as a Work System

It seems that the XYZ University has very informal strategy when it comes to the operation and maintenance of the UDS work system. In addition, there are no separate written security policies to guide the security of this work system. However, the university does have a general security policy.

The security policy should address the following policy areas as per the six views of the SVPSS [Yadav, 2010]:

- Threat security policy dealing with natural disasters, viruses, hackers, etc.
- Resource security policy dealing with the availability, confidentiality, and integrity of the resources
- Process security policy providing rules and guidelines for secure processes
- Security assessment policy for developing standards and measures for evaluating security assessment activities
- Legal security policy including rules to deal with privacy and legal laws affecting the UDS data
- Security management policy guidelines for administering and monitoring Digital Signage security

Identification of Digital Signage's Assets

The MVWSSA method suggests that assets be examined under each work system's element. The UDS's assets under various elements are listed in Table 11. Each work element was viewed with multiple perspectives in identifying the assets.

Table 11: List of the UDS Work System's Assets Under Various Work Elements

Work System Elements	Typical Assets Under the Six View Perspective of UDS Work System's Elements
Processes and Activities: Procurement Process, Content Importing Process	Procurement Process–Interface, Content Importing Process–Interface, Procurement Process–Operator, Content Importing Process–Operator, Equipment Procurement standard, UDS Usage Training Policy, Installation Policy, Procurement Policy, Procurement Process Method, Content Process Importing Method, Procurement Process Assessment Criteria, Content Process Assessment Criteria
Participants: Communication and Marketing Staff; System Administrator, IT Staff, Local administrator	Communication and Marketing Staff, System Administrator, IT Staff, Administrator Skills, IT Staff Knowledge, Employee Confidentiality, Equal Employment Opportunity Compliance, System Administrator Accountability, Staff Screening, System Security Awareness Training, Personnel Policy, Code of Practice, Staff Performance Criteria, Staff Performance Evaluation, UDS Security Assessment Training
Information: Data created and used by UDS	Content, Data Backup, End-user Access Rights, Privacy Law Compliance, Digital Millennium Copyright Act Compliance, Intellectual Property Compliance, Texas Public Information Act Compliance, XYZ University Privacy Policy, Procurement Process Inputs, UDS Service Process Outputs, Procurement Process Assessment Policy, Procurement Process Assessment Data
Technologies: VPN tools, PCs, Security tools	Personal Computers, VPN Tools, Security Tools, Televisions, Nexus Client Software, Software Manual, PC-access Control, Procurement Process Management Techniques, Content Process Management Techniques, UDS Service and Web-access Monitoring Tools, Technology Assessment Policy, Technology Assessment Criteria
Products and Services: Digital Display Service	Digital Display Service Review, Digital Display Service Specification, Digital Display Service design, Digital Millennium Copyright Act Compliance, Digital Display Service Quality Control, Digital Display Service Quality Monitoring, Digital Display Service Evaluation, Digital Display Service Quality Assurance Criteria
Customers: End-users	End-users (faculty, staff, students), USDSS Operator, Privacy Law Compliance, Staff Privacy Compliance, Equal Employment Opportunity Compliance, Staff Privacy Policy, Employee Accountability, Security Awareness Training, Personnel Screening Policy, Duty Segregation Policy, Employee Termination Security Policy, Equipment Procurement Process, UDS Usage Training Process
Environments: Academic Campus Setting	Equipment Room Perimeter, IT Division-Local Department Interface, Human Resource Policy, Secure Workplace Policy, Workplace Security Assessment
Infrastructure: Digital Signage Portal Servers, Web Servers, LAN, Routers, Data Storage, Equipment Room, Tele-communications Link	Digital Signage Portal Server, Web Server, LAN, Router, Data Storage, Equipment Room, Shared Database, Software License, Database License, Software Maintenance Agreement, Software License Policy, Software Maintenance Policy, User Training Policy, Infrastructure Security Policy, Building Security Policy, Infrastructure Performance Criteria, LAN Security Assessment Criteria, LAN Security Assessment Measures
Strategies: Manually Customized Approach	UDS Operation, Work Schedule, Occupational Safety and Health Act (OSHA) Compliance, OSHA-related Work System Policy, Work Schedule Policy, OSHA Compliance Assessment, Work System Operation Assessment

Identification of Risk Factors for Digital Signage Assets Using Six-View Perspective of System Security (SVPSS)

Here we identify risk factors for the assets of the UDS work system. Table 4 above can be used as a guide to identify risk factors under different views. In consultation with the administrators, we selected three assets from Table 11—Portal Server, Nexus Client Software, and Televisions—for further analysis and to identify the risk factors. Table 12 shows these risk factors in the "Sources of Risk or the Risk Factors" column of the Security Risk Register. The security views are utilized to help discover various kinds of risk factors for each asset. We will use this security risk register to show incrementally the progression of the MVWSSA method. In order to make it fit on the page, some columns of the Security Risk Register are omitted from the figures.

Table 12: Security Risk Register Showing Risk Factors for Several UDS Assets

Security Risk Register—UDS—Risk Factors for Assets—MVWSSA Method				
Assets	Security View	Sources of Risk or Risk Factors	Threat Likelihood Estimate for Each Risk	Impact Severity (if the threat is realized)
Digital Signage Porta Server	Threat	Wrong Digital Signage Portal Server Configuration		
		Denial of Service (DOS) Attack		
	Resource	Non-availability of Digital Signage Portal Server		
	Legal	Inadequate Support for the Content Data Retention Law		
		Inadequate Authorization to Access Contents Usage		
	Management	Inadequate Digital Signage Portal Sever Policy Framework		
		Poor Strategy for Backup and Recovery of Content		
	Process	Poor Monitoring of Digital Signage Portal Server Operation		
		Weak Digital Signage Portal Server Login Interface		
	Assessment	Inadequate Digital Signage Portal Performance Metrics		
		Poor Digital Signage Portal Assessment Training		
Televisions	Threat	Theft		
		Natural Disasters		
	Resource	Non-availability of TVs		
	Legal	Lack of Compliance with the Public Asset Retention Law		
	Management	Inadequate TV Installation Policy Framework		
		Poor Strategy for Protection of TV		
	Process	Poor Monitoring of TV Operation		
		Weak TV Monitoring Interface		
	Assessment	Inadequate TV Performance Metrics		
		Poor TV Assessment Training		
Nexus Client Software	Threat	Accidental Deletions by Employees		
		Virus Attack		
	Resource	Non-availability of Nexus Client Software		
		Disclosure of Nexus Client Software Data		
	Legal	Unlawful Usage		
	Management	Inadequate Usage Policy		
	Process	Inadequate Software License Validation Process		
	Assessment	Inadequate Security and Vulnerability Analysis		
		Poor Nexus Client Software Security and Vulnerability Assessment Criteria		

Evaluation and Prioritization of UDS Security Risks from Various Risk Factors

In this step, the identified risk factors in the previous step were analyzed for system security risk. We established a risk level that was acceptable to the work system’s administrators. The administrators were asked to estimate the threat likelihood and the impact severity level for each risk factor. The administrators were given information on the concepts of threat likelihood and the impact severity level. Based on the administrators’ threat likelihood and impact severity estimates, we computed the resultant risk level for each risk factor by combining its likelihood estimate with its impact severity level as per Table 6 shown in Step 4 above. We then computed the risk priority level for each risk factor by subtracting its acceptable risk level from its resultant risk level as shown in the security risk register in Table 13. The security risk register has been split into three Tables —13, 14, and 15—in order to have better readability and to properly fit on a page.

Table 13: Security Risk Register Showing the Risk Priority Rating Level for the Portal Server's Risk Factors

Security Risk Register—UDS—Risk Priority Rating for Portal Server—MVWSSA

Assets	Security View	Sources of Risk or Risk Factors	Threat Likelihood Estimate for Each Risk Factor	Impact Severity (if the threat is realized)	Resultant Risk Level	Acceptable Risk Level Rating	Risk Priority Level
Digital Signage Portal Server	Threat	Wrong Digital Signage Portal Server	Low	Significant	Moderate (2)	Moderate (2)	0
		Denial of Service (DOS) Attack	Low	Significant	Moderate (2)	Moderate (2)	0
	Resource	Non-availability of Digital Signage Portal Server	Medium	Significant	Moderate (2)	Moderate (2)	0
	Legal	Inadequate Support for the Content Data Retention Law	Negligible	Serious	Low (1)	Very low (0)	1
		Inadequate Authorization to Access Contents Usage	Medium	Serious	High (3)	Moderate (2)	1
	Management	Inadequate Digital Signage Portal Server Policy Framework	Low	Significant	Moderate (2)	Moderate (2)	0
		Poor Strategy for Backup and Recovery of Content	Very low	Significant	low (1)	High (3)	-2
	Process	Poor Monitoring of Digital Signage Portal Server Operation	Low	Significant	Moderate (2)	Moderate (2)	0
		Weak Digital Signage Portal Server Login Interface	Low	Serious	High (3)	Moderate (2)	1
	Assessment	Inadequate Digital Signage Portal Performance Metrics	Low	Significant	Moderate (2)	Moderate (2)	0
		Poor Digital Signage Portal Assessment Training	Low	Significant	Moderate (2)	Moderate (2)	0

Table 14: Security Risk Register Showing the Risk Priority Rating Level for the Televisions' Risk Factors

Security Risk Register—UDS—Risk Priority Rating for Televisions—MVWSSA

Assets	Security View	Sources of Risk or Risk Factors	Threat Likelihood Estimate for Each Risk Factor	Impact Severity (if the threat is realized)	Resultant Risk Level	Acceptable Risk Level Rating	Risk Priority Level
Television	Threat	Theft	Medium	Serious	High (3)	Very low (0)	3
		Natural Disasters	Low	Damaging	Moderate (2)	Low (1)	1
	Resource	Non-availability of TVs	Low	Damaging	Moderate (2)	Low (1)	1
	Legal	Lack of Compliance with the Public Asset Retention Law	Low	Insignificant	Very low (0)	Very low (0)	0
	Management	Inadequate TV Installation Policy Framework	Low	Damaging	Moderate (2)	Low (1)	1
		Poor Strategy for Protection of TV	Medium	Damaging	High (3)	Low (1)	2
	Process	Poor Monitoring of TV Operation	Medium	Damaging	High (3)	Low (1)	2
		Weak TV Monitoring Interface	Negligible	Insignificant	Very low (0)	Very high (4)	-4
	Assessment	Inadequate TV Performance Metrics	Negligible	Insignificant	Very low (0)	Very high (4)	-4
		Poor TV Assessment Training	Negligible	Insignificant	Low (1)	Very high (4)	-3

Table 15: Security Risk Register Showing the Risk Priority Rating Level for the Portal Server's Risk factors

Security Risk Register—UDS—Risk Priority Rating for Nexus Client Software—MVWSSA

Assets	Security View	Sources of Risk or Risk Factors	Threat Likelihood Estimate for Each Risk Factor	Impact Severity (if the threat is realized)	Resultant Risk Level	Acceptable Risk Level Rating	Risk Priority Level
Nexus Client Software	Threat	Accidental Deletions by Employees	Medium	Minor	Low (1)	High (3)	-2
		Virus Attack	Low	Damaging	Moderate (2)	Very low (0)	2
	Resource	Non-availability of Nexus Client Software	Low	Minor	Low (1)	High (3)	-3
		Disclosure of Nexus Client Software Data	Low	Insignificant	Very low (0)	Very high (4)	-4
	Legal	Unlawful Usage	Low	Critical	High (3)	Very low (0)	3
	Management	Inadequate Usage Policy	Low	Critical	High (3)	Very low (0)	3

Table 15: Security Risk Register Showing the Risk Priority Rating Level for the Portal Server's Risk factors – Continued

Nexus Client Software	Process	Inadequate Software License Validation Process	Low	Minor	Low (1)	High (3)	-2
	Assessment	Inadequate Security and Vulnerability Analysis	Low	Serious	High (3)	Very low (0)	3
		Poor Nexus Client Software Security and Vulnerability Assessment Criteria	Medium	Serious	High (3)	Very low (0)	3

Identification of UDS Security Requirements

We note that the televisions and the Nexus Client software were considered for further analysis. Due to the lack of space, we focus only on the Nexus Client software for further discussion. The appropriate security requirements were identified using Table 8 of Step 5 as a guide. Table 16 shows the needed security requirements for every risk factor with priority level of 2 and above. A priority level of 2 was established as a cut-off point by the administrators based on their understanding of the UDS's context.

Table 16: Security Register Showing Security Requirements and Mechanisms for the Nexus Client Software Factors

Security Risk Register—UDS—Security Requirements, Mechanisms for Nexus Client Software—MVWSSA

Assets	Security View	Sources of Risk or Risk Factors	Resultant Risk Level	Acceptable Risk Level Rating	Risk Priority Level	Security Requirements	Security Mechanisms
Nexus Client Software	Threat	Accidental deletions by employees	Low (1)	High (3)	-2		
		Virus attack	Moderate (2)	Very low (0)	2	1. Protect against intrusion 2. Thwart access control discovery attack	1. Access control lists configuration 2. Intrusion detection tools 3. Anti-virus software
	Legal	Unlawful usage	High (3)	Very low (0)	3	1. Analyze the legal risks for UDS 2. Establish rules for handling unlawful usage of UDS	1. Transparency and control of access privileges 2. Centralized authentication and authorization
	Management	Inadequate usage policy	High (3)	Very low (0)	3	Review usage policy and procedures	Nexus Client software usage training
	Process	Inadequate Software License Validation process	Low (1)	High (3)	-2		

Table 16: Security Register Showing Security Requirements and Mechanisms for the Nexus Client Software Factors – Continued

Nexus Client Software	Assessment	Inadequate security and vulnerability analysis	High (3)	Very low (0)	3	1. Collect data on measures of security and vulnerability analysis 2. Evaluate the measures' effectiveness	1. Security scanner tools 2. Nexus Client software Security and Vulnerability Assessment training
		Poor Nexus Client software security and vulnerability assessment criteria	High (3)	Very low (0)	3	1. Define assessment criteria for assessing threat security 2. Define measures for each criterion for assessing threat security	1. Nexus Client software Security and Vulnerability Assessment standards 2. Nexus Client software Security and Vulnerability Assessment policy

Specification of Security Mechanisms (i.e., Evidences) for UDS

Here we identified the appropriate security mechanisms, using Table 9 as a guide, to support the security requirements identified in the previous step. The security mechanisms are also documented in Table 16.

Development of the Security Assertion-Evidence Diagram for Digital Signage

Based on the identified security requirements and mechanisms, we developed the security assertion–evidence diagram for the Nexus Client software. The assertion–evidence diagram is shown in Figure 6.

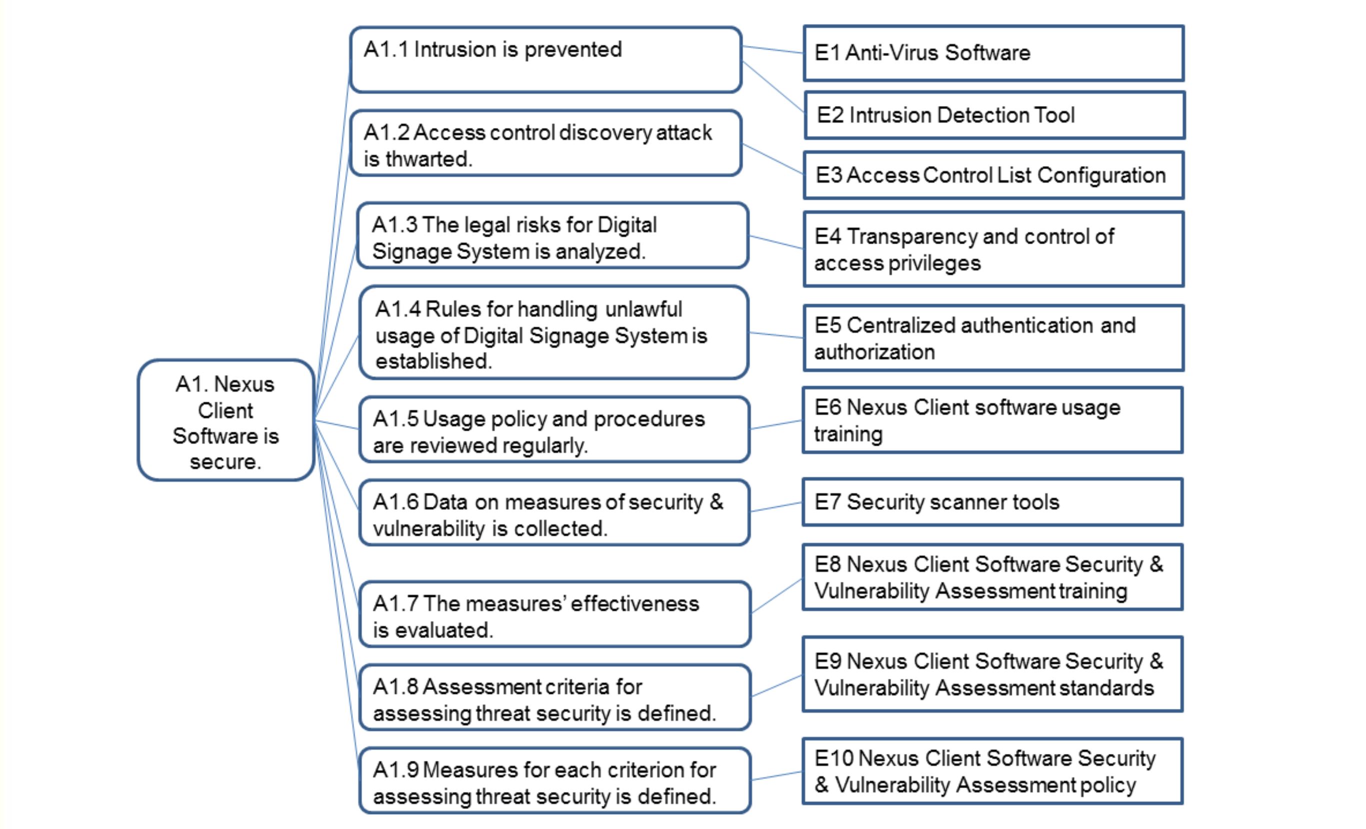

A1. Nexus Client Software is secure.
A1.1 Intrusion is prevented
A1.2 Access control discovery attack is thwarted.
A1.3 The legal risks for Digital Signage System is analyzed.
A1.4 Rules for handling unlawful usage of Digital Signage System is established.
A1.5 Usage policy and procedures are reviewed regularly.
A1.6 Data on measures of security & vulnerability is collected.
A1.7 The measures' effectiveness is evaluated.
A1.8 Assessment criteria for assessing threat security is defined.
A1.9 Measures for each criterion for assessing threat security is defined.
E1 Anti-Virus Software
E2 Intrusion Detection Tool
E3 Access Control List Configuration
E4 Transparency and control of access privileges
E5 Centralized authentication and authorization
E6 Nexus Client software usage training
E7 Security scanner tools
E8 Nexus Client Software Security & Vulnerability Assessment training
E9 Nexus Client Software Security & Vulnerability Assessment standards
E10 Nexus Client Software Security & Vulnerability Assessment policy

Figure 6. Assertion–Evidence Diagram for the Nexus Client Software Asset

Collection and Representation of Evidence Strength for Nexus Client Software

Real data on evidence strength for UDS was collected by sending a questionnaire to the administrators. A presentation on the ideas of assertion and evidence was made to the administrators prior to sending the questionnaire. The two administrators estimated the strength of evidence for each mechanism shown in rectangles in Figure 7. An average of evidence strength for each mechanism was computed and is shown in Figure 7. For example, as per the administrators' estimation, the evidence strength for the anti-virus software is 0.8.

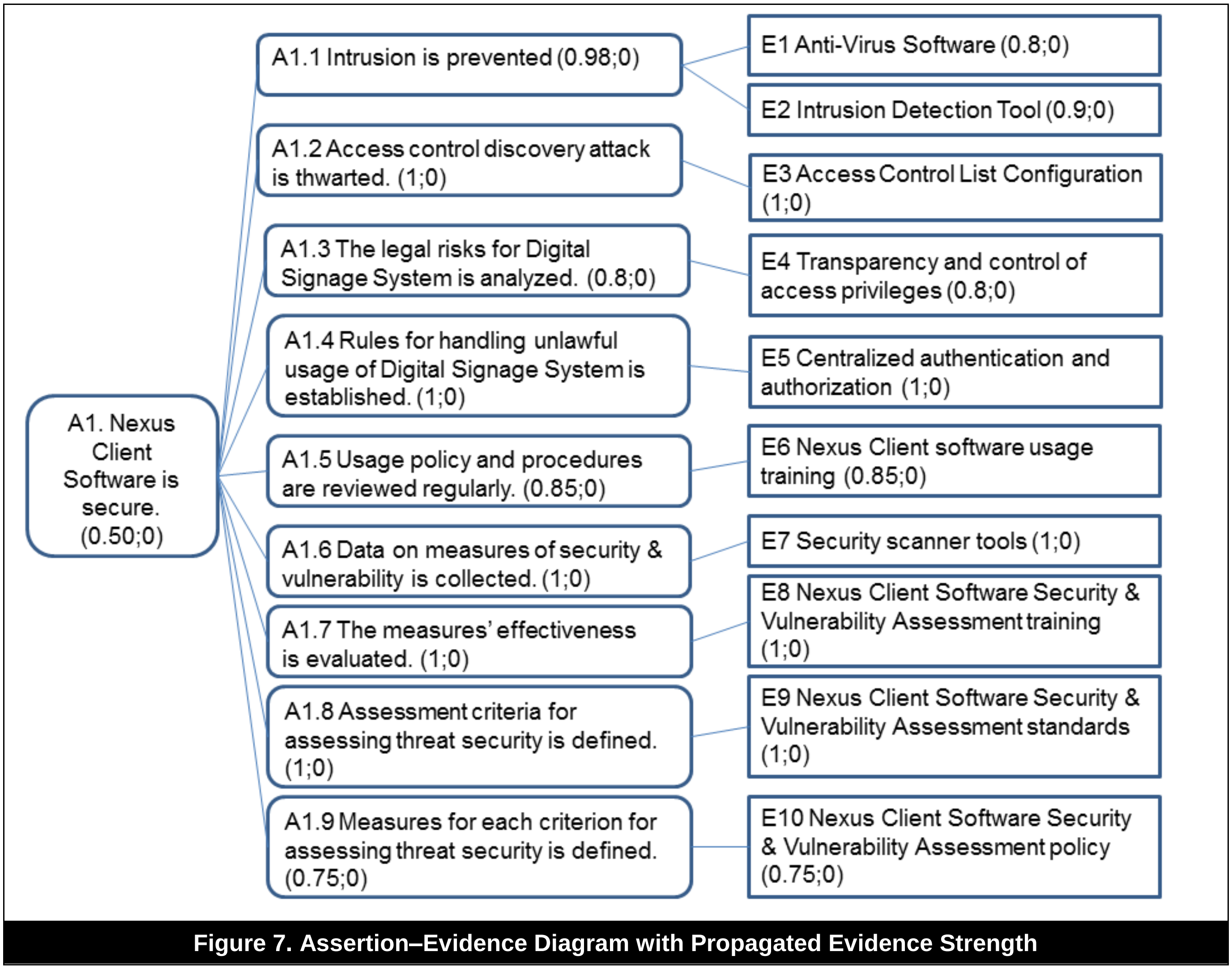

A1. Nexus Client Software is secure. (0.50;0)
A1.1 Intrusion is prevented (0.98;0)
A1.2 Access control discovery attack is thwarted. (1;0)
A1.3 The legal risks for Digital Signage System is analyzed. (0.8;0)
A1.4 Rules for handling unlawful usage of Digital Signage System is established. (1;0)
A1.5 Usage policy and procedures are reviewed regularly. (0.85;0)
A1.6 Data on measures of security & vulnerability is collected. (1;0)
A1.7 The measures' effectiveness is evaluated. (1;0)
A1.8 Assessment criteria for assessing threat security is defined. (1;0)
A1.9 Measures for each criterion for assessing threat security is defined. (0.75;0)
E1 Anti-Virus Software (0.8;0)
E2 Intrusion Detection Tool (0.9;0)
E3 Access Control List Configuration (1;0)
E4 Transparency and control of access privileges (0.8;0)
E5 Centralized authentication and authorization (1;0)
E6 Nexus Client software usage training (0.85;0)
E7 Security scanner tools (1;0)
E8 Nexus Client Software Security & Vulnerability Assessment training (1;0)
E9 Nexus Client Software Security & Vulnerability Assessment standards (1;0)
E10 Nexus Client Software Security & Vulnerability Assessment policy (0.75;0)

Figure 7. Assertion–Evidence Diagram with Propagated Evidence Strength

Assessment of the Overall Level of Security Risk to Nexus Client Software

Figure 7 also shows the overall belief function for the sub-assertions and the main assertion. These belief functions were computed using the evidence combination rules [Srivastava and Shafer, 1992; Sentz and Ferson, 2002; Sun et al., 2006]. The readers are referred to the cited work for details on combination rules for computing belief functions. As shown in Figure 7, the overall belief function of the assertion "Nexus Client software is secure" is {0.50, 0.0}. The equations and the computational process are excluded from the article due to the lack of space. Table 17 documents the assessment results. It indicates that there is a 50 percent (1 - 0.50 - 0.0) security risk that the Nexus Client software is not adequately protected. The pre-established risk tolerance level was established as 1 percent by the administrators. This indicates that the additional security requirements and/or mechanisms may be needed to reduce the security risk level further. Some of the additional mechanisms are suggested in the next step.

Table 17: Documentation of the Overall Assessment Results

Assets (name and description)	Overall Belief Function of the main assertion	Belief Value for “not sure” (ignorance) in %	Pre-established Risk Tolerance Level in %	Action Needed for Risk Reduction (Yes, No)	Recommended Mechanisms	
					Preventive	Mitigation
Nexus Client Software	{.5,0.0}	50	1	Yes		

Recommendation of Preventive and Mitigation Security Mechanisms for Digital Signage

In this step, a review of the existing security requirements and mechanisms may be performed to recommend appropriate security mechanisms. In the case of UDS, we see from Figure 7 that the UDS system’s security risk can be reduced by reviewing its usage training, security and vulnerability assessment policy, and transparency and control access privileges. Anti-virus software should be updated regularly. In addition, a periodic evaluation of access rights should be instituted. As a mitigation mechanism, a log of software risk assessment data should be maintained. The recommended mechanisms are shown in Table 18.

Table 18: Documentation of the Suggested Recommendations

Assets (name and description)	Overall Belief Function of the main assertion	Belief Value for “not sure” (ignorance) in %	Pre-established Risk Tolerance Level in %	Action needed for Risk Reduction (Yes, No)?	Recommended Mechanisms	
					Preventive	Mitigation
Nexus Client Software	{.50,0.0}	50	1	Yes	Nexus Client software usage training review, Nexus Client software security and vulnerability assessment policy review, Review of transparency and control access privileges, Anti-virus software update, Periodic evaluation of access rights	Software risk assessment data log

A detailed recommendation report can be prepared based on the information in Table 18.

The above real case application demonstrates the use of the MVWSSA method. It supports the whole security risk assessment process fully. It provides a better structure and guidelines to support all three phases—ascertainment, measurement, and evaluation—of the security risk assessment process.

V. COMPARISON WITH OTHER METHODS

Tables 1 documented the comparison of several models and methods in the extant literature. Our foregoing discussion of the proposed MVWSSA method shows that the proposed method covers more aspects of the system security risk assessment process as compared to other methods. It integrates the ideas from qualitative as well as quantitative models and methods into a complete system security assessment method taking into account the multiple security views of a work system.

In comparison to the previous methods, our method is more comprehensive, adaptable, and practical for use by system and security risk analysts. Our method not only provides steps and guidelines to help analysts determine security requirements and mechanisms but also includes steps and guidelines for measuring and evaluating the strength of existing security mechanisms of a work system. Most of the other methods do not cover the security assessment process completely. For example, Sun, Srivastava, and Mock [2006] present a very good assessment method that focuses on security risk’s evidence measurement and evaluation. However, their method provides little support for the ascertainment phase of the assessment process. Similarly, other models such as Yadav’s SVPSS framework [Yadav, 2010] and Alter and Sherer’s Model [Alter and Sherer, 2004] support the ascertainment phase but provide little support for the measurement and evaluation of the existing security mechanisms of a work system.

It is adaptable in the sense that the proposed method does not have to be used in its entirety in every situation. For example, if an analyst wants to do only the system security risk analysis and is interested only in the ascertainment phase of the process, then only Steps 1 through 6 of the method could be used. On the other hand, if an analyst wants to just evaluate the existing security mechanisms of a work system, then only Steps 7 through 10 need to be used. Obviously, the method can be used to examine and protect any set of selected assets. Our method is more useful in identifying and evaluating all kinds of risk factors. It also relates the risk factors directly with the corresponding security requirements, mechanisms and their implementation in a work system.

According to standard dictionaries, "practical" is defined as having "useful ends in view; capable of useful action." The method covers beginning-to-end activities of security risk assessment with clearly defined outputs at each step. The proposed method produces very useful information that can be readily used in practice.

VI. Conclusions and Future Work

This article has presented a comprehensive system security risk assessment method that covers all three phases of the system security risk assessment process. More specifically, the method includes:

1. A multiple-view perspective of system security
2. A set of guidelines for carrying out the steps
3. Steps to ascertain, measure, and evaluate work system security risk

The method integrates ideas from extant models and methods into a coherent set of steps for supporting the system security risk assessment process completely. It extends existing system security methods by incorporating new ideas of multifaceted security view and work system into a coherent set of steps to ascertain security requirements, to measure the evidence for the needed security requirements, and to evaluate the evidence against the needed security mechanisms.

The MVWSSA method was applied successfully to an UDS system. Treating UDS as a work system and applying multi-view security perspective, the method enabled us to identify a more complete set of assets, security requirements, and mechanisms.

The MVWSSA method takes a broader and multi-view of assets that may be vulnerable to threats and other security risks. This may lead to the identification of many assets. Identification of too many assets may be considered to be a limitation of the method. However, we feel that, in today's complex business environment, it is always better to identify all assets than miss some that may turn out to be critical later on. It is always possible to ignore the assets from further consideration if they do not seem important to the work system under study. This recommendation for identifying all assets may seem at odds with the concept of Open Information Society [Ahituv, 2001] where everything is accessible to everyone. However, we feel that an ideal open information society is a long way away and the current trend in security threats suggests that, in the meantime, businesses have to protect all their assets.

Real world implications of security risk assessment methods and frameworks are very important to consider. A method is not very practical if it cannot be used effectively. Bob Violino [CSO, 2010] discusses real-world experiences of four IT risk assessment frameworks—OCTAVE, FAIR, NIST RMF, and TARA. Complexity, lack of quantitative modeling, difficult to use, poor documentation, and lack of automation are the major drawbacks in using IT risk assessment frameworks [CSO, 2010]. We believe that system security risk assessment is inherently a complex process. However, a security risk assessment method can be made easier to use through automation, proper documentation, and illustration. For example, an automated tool can incorporate case-based reasoning approach to offer illustration and examples in addition to automating the security risk assessment method.

We plan to apply the MVWSSA method to case studies involving several work systems. A software tool to support and automate most of the steps of the method is also in the offing.

VII. LIMITATIONS

The MVWSSA method, just like many existing security risk assessment methods, is complex. One of the reasons for it being complex is that it covers all the three phases of SSR assessment process. Another reason is the lack of a software tool to support the method.

It can be argued that the proposed research, like many extant works on methods and models, is intuition-driven and not theory-driven. The proposed method does extend the pragmatic and conceptual work of other researchers. However, the conceptual ideas behind the steps of the MVWSSA method may not be fully formalized. It would be insightful to explain the theoretical underpinnings of the proposed method. Exposition and formalization of the method-relevant theoretical underpinnings could be an excellent topic for future research.

The average of evidence strength for each mechanism was computed based on the data collected from two administrators during the data collection for the UDS case study. In general, an average of two data points may not be sufficient. In this study, however, the two administrators were the only individuals with the intimate knowledge of UDS. Therefore, the data on evidence strength was collected from only two people.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor, or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Ackerman, G.A., and K.S. Moran (2010) "Bioterrorism and Threat Assessment", *Weapons of Mass Destruction Terrorism Research Program*, http://www.blixassociates.com/wp-content/uploads/2011/03/No22.pdf.

Ahituv, N. (2001) "The Open Information Society", *Communications of the ACM*, (44)6, pp. 48–52.

Alter, S. (2002) "The Work System Method for Understanding Information Systems and Information Systems Research", *Communications of the AIS*, (9)6, pp. 90–104.

Alter, S. (2006) *The Work System Method: Connecting People, Processes, and IT for Business Results*, Larkspur, CA: Work System Press.

Alter, S. (2008) "Defining Information Systems as Work Systems: Implications for the IS Field", *European Journal of Information Systems,* (17)5, pp. 448–469.

Alter, S., and S. Sherer (2004) "A General, But Readily Adaptable Model of Information System Risk", *Communications of Association for Information Systems*, (14), pp. 1–28.

Australia: Standards Australia (2004) *AS/NZS 4360:2004 Risk Management,* Sydney, Australia.

Baker, W.H., L.P. Rees, and P.S. Tippett (2007) "Necessary Measures: Metric-driven Information Security Risk Assessment and Decision Making", *Communication of ACM,* (50)10, pp. 101–107.

Barki, H., S. Rivard, and J. Talbot (2001) "An Integrative Contingency Model of Software Project Risk Management", *Journal of Management Information Systems,* (17)4, pp. 37–70.

Benaroch, M. (2002) "Managing Information Technology Investment Risk: A Real Options Perspective", *Journal of Management Information Systems,* (19)2, pp. 43–84.

Boehm, B. (1989) *Software Risk Management*, Washington, DC: IEEE Computer Society Press.

Bornman, W.G., and L. Labuschagne (2004) "A Comparative Framework for Evaluating Information Security Risk Management Methods", *Peer-reviewed Proceedings of the ISSA 2004 Enabling Tomorrow Conference.* Pretoria, South Africa, ISSA.

Caralli, R.A., J.F. Stevens, L.R. Young, and W.R. Wilson (2007) "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", *Technical Report No. CMU/SEI-2007-TR-012, ESC-TR-2007-012,* www.cert.org/archive/pdf/07tr012.pdf.

Charette, R. (1989) *Software Engineering Risk Analysis and Management,* New York: McGraw Hill.

CMS: Centers for Medicare and Medicaid Services (2005) *CMS Information Security Risk Assessment (RA) Methodology,* Department of Health and Human Services, Baltimore, Maryland, Version #2.1, May 11.

CSO (2010) "IT Risk Assessment Frameworks: Real-world Experience, CSO Security and Risk", May 3, http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience.

Deloitte Insights (2012a) "Making the Real Case for Cyber Security", *CIO Journal,* WSJ.com, May 9, http://deloitte.wsj.com/cio/2012/05/09/making-the-real-case-for-cyber-security/.

Deloitte Insights (2012b) “Is Your IT Security Approach Due for a Refresh?”, *CIO Journal,* WSJ.com, May 16, http://deloitte.wsj.com/cio/2012/05/16/is-your-it-security-approach-due-for-a-refresh/?KEYWORDS=Security+breach.

Engleman, E., and C. Strohm (2012) “Cyber Security Disaster Seen in U.S. Survey Citing Spending Gaps”, *Bloomberg,* January 31, http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html, (current April 20, 2012).

Fein, R.A., B. Vossekuil, and G.A. Holden (1995) “Threat Assessment: An Approach to Prevent Targeted Violence”, *National Institute of Justice: Research in Action*, pp. 1–7.

Feng N., M.Q. Li (2010) “An Information Systems Security Risk Assessment Model Under Uncertain Environment”,

Applied Soft Computing, (11)7, pp. 4332–4340.

Higuera, R., and Y. Haimes (1996) *Software Risk Management,* Pittsburgh, PA: Carnegie Mellon, Software Engineering Institute, Report SEI/CMU-96-TR-012.

International Organization for Standardization and International Electro Technical Commission (2005) *Information Technology—Security Techniques—Information Security Management Systems—Requirements,* http://www.27000.org/iso-27001.htm.

INTERNATIONAL SECURITY TECHNOLOGY Inc. (IST Inc.) (2002) *A Brief History of CORA*, http://www.ist-usa.com.

James, L., R. Demaree, and G. Wolf (1984) “Estimating Within-group Inter-rater Reliability with and Without Response Bias”, *Journal of Applied Psychology*, (69)1, pp. 85–98, DOI: 10.1037/0021-9010.69.1.85.

Karabacak, B., and I. Sogukpinar (2005) “ISRAM: Information Security Risk Analysis Method”, *Computers & Security*, (24), pp. 147–159.

Kontio, J., G. Getto, and D. Landes (1998) “Experiences in Improving Risk Processes Using the Concepts of the riskit Method”, SIGSOFT’98, Sixth International Symposium on the Foundations of Software Engineering.

Loch, K.D., H.H. Carr, and M.E. Warkentin (1992) “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding”, *MIS Quarterly*, pp. 173–186.

Lund, S., F. Den Braber, K. Stolen, and F. Vraalsen (2004) “A UML Profile for the Identification and Analysis of Security Risks During Structured Brainstorming”, SINTEF Technical Report STF40 A03067, http://coras.sourceforge.net/documents/uml-sa-report2.pdf.

Lyytinen, K., L. Mathiassen, and J. Ropponen (1996) “A Framework for Software Risk Management”, *Journal of Information Technology*, (11), pp. 275–285.

Mirkovic, J., and P. Reiher (2004) “A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms”, *ACM SIGCOMM Computer Communication Review*, (34)2, pp. 39–53.

Neuendorf, K.A. (2002) *The Content Analysis Guidebook,* Thousand Oaks, CA: Sage Publication.

Nidumolu, S. (1995) “The Effect of Coordination and Uncertainty on Software Project Performance: Residual Performance Risk as an Intervening Variable”, *Information Systems Research*, (6)3, pp. 191–219.

Nidumolu, S. (1996) “A Comparison of Structural Contingency and Risk-based Perspectives on Coordination in Software Development Projects”, *Journal of Management Information Systems*, (13)2, pp. 77–113.

NIST (2004). “U.S. National Institute of Standards and Technology, NIST 800-12—An Introduction to Computer Security: The NIST Handbook”, http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter7.html.

Ohia, U.O. (2011) “A Model for Effectively Assessing Student Learning Outcomes”, Maui, Hawaii, U.S., pp. 525–532.

Rainer, R.K., C.A. Snyder, and H.H. Carr (1991) “Risk Analysis for Information Technology”, *Journal of Management Information Systems*, (8)1, pp. 129–147.

Schneider, R.M. (2010) “A Comparison of Information Security Risk Analysis in the Context of e-Government to Criminological Threat Assessment Techniques”, Information Security Curriculum Development Conference, ACM, New York.

Sentz, K., and S. Ferson (2002) “Combination of Evidence in Dempster—Shafer Theory”, Sandia National Laboratories SAND 2002-0835.

Shafer, G. (1976) *A Mathematical Theory of Evidence,* Princeton, N.J: Princeton University Press.

Sherer, S., and S. Alter (2004) “Information System Risk and Risk Factors: Are They Mostly About Information Systems?”, *Communications of Association for Information Systems*, (14),pp. 29–60.

Shrestha, A. (2004) “Information Security Management System (7799) for an Internet Gateway”, SANS Institute, http://www.sans.org/reading_room/whitepapers/iso17799/information-security-management-system-7799-internet-gateway_1454.

Srivastava, R.P., and G. Shafer (1992) “Belief–Function Formulas for Audit Risk”, *The Accounting Review*, (67)2, April, pp. 249–283.

Stolen, K., F.D., Braber, T. Dimitrakos, R. Fredriksen, B.A. Gran, S.H. Houmb, J.Ø. Aagedal, et al. (2002) “Model-based Risk Assessment—The CORAS Approach”, presented at the 1st iTrust Workshop, http://heim.ifi.uio.no/~massl/publications/nik02-coras.pdf

Stoneburner, G., A. Goguen, and A. Feringa (2002) “A Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology”, NIST Special Publication 800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Straub, D.W., and R.J. Welke (1998) “Coping with Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly*, (22), pp. 441–469.

Suh, B., and I. Han (2003) “The IS Risk Analysis Based on a Business Model”, *Information & Management*, (41), pp. 49–158.

Sun, L.L., R.P. Srivastava, and T.J. Mock (2006) “An Information Systems Security Risk Assessment Model Under Dempster-Shafer Theory of Belief Functions”, *Journal of Management Information Systems*, (22)4, pp. 109–142.

Vorster, A., and L. Labuschagne (2005) “A Framework for Comparing Information Security Risk Analysis Methodologies”, *Proceedings of SAICSIT 2005*, pp. 95–103.

Whitman, M., and H.J. Mattord (2010) *Management of Information Security,* Boston: Thomson Course Technology.

Yadav, S.B. (2010) “A Six-View Perspective Framework for System Security—Issues, Risks, and Requirements”, *International Journal of Information Security and Privacy*, (4)1, January–March, pp. 60–90.

APPENDIX A: UNIVERSITY DIGITAL SIGNAGE SYSTEM

Introduction

Digital signage system is a form of electronic display that shows television programming, menus, information, advertising, and other messages. Digital signs (such as LCD, LED, plasma displays, or projected images) can be found in public and private environments, such as retail stores, hotels, and restaurants, as well as corporate or institution buildings. In this article, a public university with the business requirement for digital signage system is considered. In the following subsections, a brief description of the organization and its exiting digital signage system is provided.

XYZ Public University Digital Signage System

XYZ University has a large population of students, faculty, and staff. It is mentioned in the IT Division's strategic plan that IT Division should make the needed information easily available to students, faculty, and staff. To fulfill this objective, for the last four years, XYZ University IT Division, along with representatives from interested areas and departments, have been evaluating and testing various digital signage solutions for information displays in campus buildings and facilities. In the last year, the assessment team selected a software product that best suits the campus needs—Nexus. In April 2010, IT Division upgraded the university events calendar program and scrolling monitor systems to the Nexus software. The new approach allows the display of richer, more robust content, including Web pages, videos, and lives news data. Departments are also able to implement digital signage in their own areas, customizing the content and display for their purposes. However, during an emergency, a centrally managed digital signage will be used to display emergency notifications and alerts from the President's office. Many XYZ University areas have expressed interest in using digital signage in collaboration with the XYZ University's IT Division, including the Advising Center, Athletics, College of Architecture, College of Human Sciences, College of Mass Communications, Communications and Marketing, College of Business, Student Union, and University Student Housing. Before the UDS system was put into service, IT Division collaborated with two local departments to pilot the Nexus-powered digital signage in their respective areas in addition to the IT Division locations.

The UDS system is based on client-server model. The central digital signage portal server connects database information (from a database server) to the end-user or client program through the XYZ University's intranet. The Digital Signage Content Portal provides a user interface for importing content and installing software. The local workstations consist of Dell OptiPlex personal computers, 55-inch or 44-inch TV, and operating and application software. The pre-installed software includes Microsoft Office 2010, Adobe Reader X, Adobe Flash Player, and Nexus Client. The Nexus Client software is responsible for the interaction between local PC and the Digital Signage Content Portal. The local clients can install other software depending on the displayed content format.

Core Business Processes of XYZ Public University Digital Signage System

UDS's primary business processes are described below:

A. Procurement Process

After the UDS system's usage is approved, IT Division sends the quote of equipment that is necessary for the installation of UDS. The users order all the equipment.

B. Import Process

The end users import the content they want to display on the UDS system through the Digital Signage Content Portal.

Scope of Security Assessment

The UDS system is selected as the target work system for the security assessment. All the work elements of the UDS system are within the scope of this security assessment.

Table A1: Work Elements of UDS

Work Elements	Description
Customers	Students, Faculties, Colleges, Departments which have installed Digital Signage System (DSS)
Products & Services	Events Display, Emergency Message, Advertisements
Business Process	Software Installation Process, Procurement Process, Training Process, Content Importing Process
Participants	IT Division Staff, Maintenance staff, Server Administrator, Communication and Marketing Manager
Information	Content, Data Backup
Technologies	Content Portal, LDC, User Interface, RSS Reader
Infrastructure	Network infrastructure, Database server, Web server
Environment	Academic setting
Strategies	Manually customized approach

Current State of UDS System Security

The technical design and the security architecture of the UDS system under consideration seem to be reasonably well-designed and documented. However, the XYZ University's IT Division does not have a formal (written) security policy for this specific work system. There is an overall IT Security Policy for information technology, which is too general for a specific work system. There are only informal plans and procedures for the operation of the UDS system.

The current IT Security Policy that can be applied to UDS includes Computer Security and Privacy Policy, Digital Millennium Copyright Act, Intellectual Property, Laws and XYZ University Policies, Personal Information Privacy, Texas Public Information Act, and XYZ University Privacy Policy. Group policy and active directory are used to control the security risk for the UDS.

ABOUT THE AUTHORS

Surya B. Yadav is the Sowell Professor of Telecom Technology in Rawls College of Business, Texas Tech University, Lubbock, Texas. He received his Bachelor of Science degree in electrical engineering from Banaras University in 1972, the M.Tech. degree from IIT Kanpur, India, in 1974, and the Ph.D. degree in business information systems from Georgia State University, Atlanta, in 1981. He has published in several journals including *Communications of the ACM, IEEE Transactions on Software Engineering, IEEE Transactions on Systems, Man and Cybernetics, Journal of Management Information Systems, Journal of Intelligent Information Systems,* and *Decision Support Systems.* His research areas include intelligent information retrieval systems, text mining, and system security.

Tianxi Dong is currently an MIS Ph.D. student in the Rawls College of Business at Texas Tech University. Dong earned her MS in Management Science from Shanghai University of Finance and Economics. Her current research interests include business intelligence, data mining, text mining, and information system security. She has published in *Journal of the American Society for Information Science and Technology* and *Journal of Service Science and Management.*

Communications of the Association for Information Systems

ISSN: 1529-3181