An Information Systems Security Risk Assessment Model Under the Dempster–Shafer Theory of Belief Functions

LILI SUN, RAJENDRA P. SRIVASTAVA, AND THEODORE J. MOCK

LILI SUN is an Assistant Professor at the Department of Accounting and Information Systems at Rutgers Business School. She received her B.S. in Accounting and Finance from Peking University, China, and Ph.D. (honors) in Accounting and Information Systems from the University of Kansas.

RAJENDRA P. SRIVASTAVA is Ernst & Young Distinguished Professor of Accounting and Director of the Ernst & Young Center for Auditing Research and Advanced Technology at the School of Business, University of Kansas. He holds a Ph.D. in Accounting from the University of Oklahoma, Norman (1982), and a Ph.D. in Physics from Oregon State University, Corvallis (1972). Professor Srivastava's publications have appeared in *Accounting Review, Journal of Accounting Research, Auditing: A Journal of Practice and Theory, Journal of Management Information Systems,* and many other accounting and artificial intelligence (AI) journals. He received the 1996 Award for Notable Contribution to AI and Expert Systems Research in Accounting from the AI/Expert Systems Section of the American Accounting Association. He is currently Associate Editor of *Journal of Emerging Technologies in Accounting,* AI/ET Section Journal of the American Accounting Association, and has been a member of the editorial and review boards of several journals, including *Accounting Review* (1989–1993), *Auditing: A Journal of Practice and Theory* (July 1993–2005), *Indian Accounting Review, International Journal of Auditing,* and *International Journal of Accounting and Information Systems.* Professor Srivastava served as the chairman of the AI/Emerging Technology Section of American Accounting Association during 1994–95.

THEODORE J. (TED) MOCK is the Arthur Andersen Alumni Professor of Accounting at the University of Southern California (USC) and a Professor of Auditing Research at Maastricht University in the Netherlands. Professor Mock's training includes degrees in mathematics and finance from Ohio State University and a Ph.D. from the University of California, Berkeley. His research interests lie primarily in the areas of audit and assurance. During 1977–78, he was the first audit research fellow at KPMG in New York City. His American Institute of Certified Public Accountants (AICPA) research monograph with J. Turner on internal control evaluation was awarded the American Accounting Association Wildman Award, and he was a coauthor of the AICPA monograph on collaborative audit research that received the 1998 Joint AICPA/AAA Collaboration Award. In 2003, he received the Outstanding Auditing Educator award of the AAA Auditing Section. In addition to USC, he has held

Journal of Management Information Systems / Spring 2006, Vol. 22, No. 4, pp. 109–142.
© 2006 M.E. Sharpe, Inc.
0742–1222 / 2006 $9.50 + 0.00.

academic appointments at the University of California–Los Angeles, Ohio State University, the Norwegian School of Economics and Business, Bond, Australian National, Griffith, Edith Cowan and Southern Cross Universities in Australia, University of Otago in New Zealand, Maastricht University in the Netherlands, City University of Hong Kong, Nanyang Technological University, and National University of Singapore. Dr. Mock has served many positions within the American Accounting Association including editor of *Auditing: A Journal of Practice & Theory,* Director of Research, and President of the Auditing Section.

ABSTRACT: This study develops an alternative methodology for the risk analysis of information systems security (ISS), an evidential reasoning approach under the Dempster–Shafer theory of belief functions. The approach has the following important dimensions. First, the evidential reasoning approach provides a rigorous, structured manner to incorporate relevant ISS risk factors, related countermeasures, and their interrelationships when estimating ISS risk. Second, the methodology employs the belief function definition of risk—that is, ISS risk is the plausibility of ISS failures. The proposed approach has other appealing features, such as facilitating cost–benefit analyses to help promote efficient ISS risk management. The paper elaborates the theoretical concepts and provides operational guidance for implementing the method. The method is illustrated using a hypothetical example from the perspective of management and a real-world example from the perspective of external assurance providers. Sensitivity analyses are performed to evaluate the impact of important parameters on the model's results.

KEY WORDS AND PHRASES: belief function theory, cost–benefit analysis, evidential reasoning, information systems security, risk analysis, sensitivity analysis.

NO SYSTEM CAN BE MADE ABSOLUTELY SECURE [57], and one can rarely open a newspaper without reading about yet another computer security breach [6, 32, 64]. For example, in May 2005, eight former employees of Bank of America, Wachovia, and other major banks were arrested for illegally stealing and selling account information of an estimated 500,000 customers [64]. As information systems (IS) have become more prevalent in business, the consequences of information system security (ISS) violations have become more and more costly. For example, the 639 organizations responding to the Computer Security Institute (CSI)/FBI 2005 Computer Crime and Security Survey reported an estimated annual loss of $31 million caused by only one type of security issues—theft of proprietary information—and a total estimated annual loss of $130 million caused by all computer security incidents [18]. Recent literature [8, 9] has also documented a significant economic cost for publicly announced information security breaches. In addition to the damaging costs of security breaches, the pressure to comply with regulatory requirements, such as the Sarbanes–Oxley Act in the United States, also drives the need toward more emphasis on information security issues.

In order to prevent security breaches, businesses use controls (countermeasures) to safeguard their assets from various types of threats by identifying IS assets that are vulnerable to threats. But, even in the presence of controls, the assets often are not fully protected from threats because of inherent control weaknesses. Thus, risk analysis is a critical step for the management of ISS [57]. Many ISS risk analysis methodologies have been developed by both academic researchers and practitioners, including quantitative methods such as expected value (EV) analysis and stochastic dominance approach; qualitative methods such as scenario analysis, questionnaire, and fuzzy metrics; and popular practical tool kits such as IRAM (Information Risk Analysis Methodologies), developed by Information Security Forum, and CRAMM (CCTA Risk Analysis and Management Method), developed by Central Computer and Telecommunications Agency (CCTA).

In our view, the existing ISS risk analysis methodologies have a number of important weaknesses and constraints. First, regarding how to estimate the probability of a threat to an IS asset and the related ISS risk, existing methods only provide general suggestions as to how to deal with the many interrelated relevant factors involved in ISS risk analysis and with the need to estimate the requisite probabilities [59]. Second, most existing methods use the probability of a negative outcome to model risk. This definition of risk ignores an important component of ISS risk—the level of residual uncertainty or ambiguity that remains after available evidence is considered.

By proposing an alternative approach to ISS risk analysis, this paper contributes to the ISS risk analysis literature in the following ways:

1. It uses the Dempster–Shafer theory of belief functions to model uncertainties involved in the assessment process of the presence or absence of threats and presence or absence of control measures. The belief function framework has been used effectively in many domains as diverse as auditing and medical diagnostics [53].
2. It provides a more comprehensive definition of information security risk by using the notion of the plausibility (risk) of a negative outcome. This notion encompasses the most commonly accepted definitions of risk as described by the Cutter Consortium survey [12, see also 1]. As explained later, the plausibility of a negative outcome covers the potential for the realization of unwanted, negative consequences of an event or situation, or an uncertain condition involving a negative or positive effect.
3. It provides a structured approach to incorporating the impact of risk factors (i.e., threats) and the impact of the corresponding countermeasures (i.e., controls) on information security risk. In particular, it facilitates incorporating the impact on the ISS risk of control measures that pertain to multiple threats. This is not easy to incorporate in the existing approaches.
4. It facilitates the assessment of risk by decomposing the overall information security risk into its subcomponents and assessing the risks associated with the subcomponents by individually assessing the impact of threats and controls to specific subcomponents of the overall risk. This decomposition of risk

assessment is appealing because human abilities to estimate the overall outcome of a future event are poor, especially given a complicated situation consisting of multiple interrelated factors [1, 59].

5. It provides a flexible ISS risk assessment model that can be modified according to the problem domain and uses a well-established calculus of belief functions to aggregate all the risks to determine the overall ISS risk.
6. Finally, it provides a way to assess the cost/benefit of maintaining controls to counterbalance the threats.

Background Research

ISS ISSUES HAVE BEEN GIVEN SERIOUS CONSIDERATION by both academics and practitioners for quite some time [4, 15, 21, 24, 31, 57, 58, 66]. Because of space limitations, we do not present a complete review of the IS risk analysis literature. Instead, we discuss the major limitations of the existing approaches and how our approach mitigates some of these limitations. For comprehensive reviews of this literature, see Alter and Sherer [1] and Rainer et al. [37]. In addition to providing comprehensive reviews and highlighting the limitations of the prior literature, both of these studies provide their own approaches for IS risk analysis, which we discuss later in this section.

Before we discuss the existing approaches and their weaknesses, we discuss the complexities that exist in practice regarding IS risk analysis. Basically, an IS is composed of multiple assets, including hardware, software, data, people, and infrastructure. Threat agents (e.g., hackers, competitors) seek to abuse these assets through exploiting vulnerabilities. Asset owners (organizations) place value on IS assets and adopt countermeasures to reduce vulnerabilities. Countermeasures include deterrence, prevention, detection, and recovery [16, 57]. However, "residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets" [29, p. 14]. Managers will seek to minimize this risk given other constraints, such as the limited resources that can be employed to safeguard the assets.

In practice, ISS risk management is quite complex. Consider the following example, which illustrates some of these complexities. Suppose a risk analyst wants to evaluate whether the information of an organization conducting its business through the Internet is secure. The analyst can easily determine that the information is exposed to risk during transmission over the Internet, during storage in the company's system, and during storage in customers' personal computers. Furthermore, the information stored in the company's system is vulnerable to threats initiated by unauthorized outsiders (hackers), other customers, and internal employees. Thus, we see that each asset may be vulnerable to multiple types of threats and that multiple control procedures or countermeasures may be implemented to protect the information from such a threat. For example, to reduce the risk of accessing information by unauthorized employees, the organization may implement several countermeasures such

as physical control over the system, limit access to the physical facility through special ID cards, and limit access to the system through special passwords.

In addition, there are situations where one countermeasure may not only protect information from just one type of threat but also from multiple types of threats. For example, firewalls can protect information from being stolen or from being contaminated by hackers and customers. Thus, it is clear that, given the level of complexity of ISS risk management, simple linear models as proposed in most of the existing approaches will not be able to capture such complexities.

The existing approaches for IS risk analysis can be grouped into three major categories: quantitative, qualitative, and a combination of quantitative and qualitative approaches. The quantitative approaches are generally called "expected value analyses" in the sense that they consider IS risk exposure as a function of the probability of a threat and the expected loss due to the vulnerability of the organization to this threat (e.g., see [37]). Examples of EV analysis approaches include annualized loss expectancy (ALE) [34, 35], and the Livermore risk analysis methodology (LRAM) [19].

The stochastic dominance (SD) approach [36] focuses on answering the specific question of what contingency plan should be used to prevent losses if a disaster occurs. To achieve this goal, SD compares the costs associated with various backup and recovery options during the entire disaster recovery process in all areas of the organization. Instead of emphasizing the estimation of risks for different types of disasters, the SD approach analyzes how long it will take to recover from a disaster and how much the organization will suffer during the recovery period.

All of the above approaches measure risk either as the probability of a negative outcome or a product of the probability of a negative outcome due to a threat and the probability that the corresponding control will fail to eliminate the threat [19, 34, 35]. This definition of risk does not capture the conceptualization of risk by the majority of IS professionals as found in a survey by the Cutter Consortium [12]. They found that 49 percent of the respondents conceptualized the risk as the potential for negative consequences of an event or situation and 22 percent as an uncertain condition or event that involves a negative or positive effect on achieving some objective. Of course, the first part is the traditional definition of risk, but, because of the ambiguity as to whether the outcome is negative or positive, the second part cannot be modeled using probability framework. As we show later, the use of plausibility function in the Dempster–Shafer theory to define risk incorporates both dimensions and thus represents a more comprehensive definition.

Rainer et al. [37] propose a risk analysis process that uses a combination of qualitative and quantitative methodologies. The process is composed of eight steps. Steps 1 through 4 describe how to identify information technology (IT) assets. In step 5, the values of the IT assets identified are assigned. Step 6 enumerates the possible threats to IT assets. Step 7 determines the vulnerability of IT assets to potential threats. In Step 8, the IT risk exposure for the organization is determined. The strength of the Rainer et al. approach is that it advocates the combined usage of qualitative and quantitative methods. While their approach is quite comprehensive, to accomplish step 8

and capture the complexity of ISS risk assessment, they would need to use an approach such as discussed in this paper.

Recently, Alter and Sherer [1] criticize existing ISS risk assessment approaches for lacking clarity in their definition of risk, practicality of use, completeness, and adaptability. They propose a general model that they argue satisfies all of the above criteria. Their model uses a flow chart to describe the interrelationships among systems being analyzed, sources of uncertainty, risk management, range of outcomes, and the probabilities of negative outcomes, goals and expectations, financial loss, and effects on other systems and projects. This approach also has limitations similar to prior approaches. For example, while they criticize the definition of risk in the literature prior to their study, they do not provide a workable definition of risk in terms of probability. In fact, one cannot use the probability framework to define the risk as conceptualized by the majority of IS professionals as reported by the Cutter Consortium [12]. In addition, the Alter and Sherer approach will have difficulty capturing the complexities of the ISS risk environment dealing with the existence of multiple controls pertaining to a single threat and a single threat impacting multiple vulnerabilities.

In addition to the academic research discussed above, there are several IS risk analysis approaches developed by practitioners such as SPRINT and SARA by the Information Security Forum (ISF; www.securityforum.org/html) and CRAMM (www.cramm.com). Basically, these methods have used the approaches discussed by academics, which, in general, assess IS risk by identifying asset vulnerabilities to threats and assessing the effects of corresponding countermeasures. Since these methods are proprietary, little is known about them. However, since these are based on the prior academic works, they are likely to have weaknesses similar to the academic approaches discussed earlier.

Summary of Limitations with Existing Approaches

First, the existing methods use the probability of a negative outcome to represent risk. This representation of risk covers only one subcomponent of ISS risk (i.e., the probability of a negative outcome) and leaves out another important subcomponent (i.e., the level of uncertainty concerning whether the outcome will be positive or negative). This study defines ISS risk as the plausibility of a negative outcome under the Dempster–Shafer theory of belief functions [39]. As elaborated in Appendix A, the plausibility of a negative outcome encompasses both risk subcomponents listed above. As noted above, the notion of risk using plausibility is a more conservative measure of risk than the probability measure of a negative outcome.

Second, regarding how to estimate the probability of a threat's occurrence and the overall ISS risk, existing methods only provide general suggestions, such as obtaining these estimates through discussions among relevant parties or through understanding the process of threat propagation. Unfortunately, such discussions are quite limited for guiding users to properly estimate ISS risk. As noted by Post and Diltz, "From the viewpoint of the analyst, the greatest difficulty with EV analysis lies in

estimating the probability of losing a component of the system" [36, p. 364]. Further, existing methods do not provide a systematic way to incorporate the judgments about the effects of various countermeasures given the complex interrelationships as described earlier. LRAM is somewhat of an exception in that it decomposes the risk of an IS asset being abused into two parts, the expected frequency of threat occurrence and the risk of control failure. However, it also fails to provide guidance on how to assess the failure of multiple controls pertaining to a single threat or how to assess the failure and the impact of a single control on multiple threats. The proposed approach provides a structure to the ISS risk assessment process by decomposing risk into its subcomponents and identifying relevant controls and their interrelationships.

Third, the existing methods either focus on the graphical relationships among ISS risk factors using flow charts or diagrams (e.g., Alter and Sherer's general model [1]), or emphasize the quantitative computation of risk probabilities (e.g., EV analysis [19, 34, 35]), but not both. The proposed approach consists of both the quantitative computation of risks and the graphical representation of relevant constructs through an evidential diagram, which can fully capture the complexities of multiple controls dealing with one threat and one control dealing with multiple threats. In addition, our approach is adaptable—that is, one can draw an evidential diagram that is appropriate in the situation depending on the assets, vulnerabilities, and the corresponding countermeasures involved. Of course, there are limitations in our approach, which are elaborated in the conclusion.

Theory of Belief Functions

THE EVIDENTIAL REASONING APPROACH UNDER the Dempster–Shafer theory of belief functions has been widely used in a broad range of disciplines, including audit and assurance services [43, 49, 50, 51, 52, 53, 54], artificial intelligence and expert systems [17, 61], data mining [33, 60], financial portfolio management [45], image processing in radiology [10], remote sensing in agriculture [11] and in the ocean [28], and forecasting demand for mobile satellites [27].

There are three basic functions that are important to understand in the use of belief functions in a decision-making process—*m*-values, belief functions, and plausibility functions. Dempster's rule [39] is the fundamental rule for combining items of evidence. Appendix A provides additional details on these basic concepts.[1]

Basically, an evidential reasoning approach to risk assessment is a process where several variables (assertions), when combined together, inform the analyst about a variable of interest, such as ISS risk. As mentioned in the introduction, there are several advantages of this approach. In addition to using Dempster–Shafer's theory of belief functions for representing uncertainties, the present approach allows the decision maker to develop an evidential diagram to assess the ISS risk that contains various variables such as the IS assets, the related threats, and the corresponding countermeasures. Next, the decision maker can input his or her judgments about the presence or absence of threats and the impact of countermeasures on the corresponding threats in terms of belief functions. This process enables the decision maker to

aggregate the evidence pertaining to various intermediate variables and then infer about the variable of interest, which is the ISS risk in the present case.

Definition of ISS Risk

We use the notion of risk represented by the plausibility of a negative outcome, which has been used by Srivastava and Shafer [54] to define audit risk in financial audits and by Démotier et al. [13] to define the quality risk in water treatment. Under the Dempster–Shafer theory of belief functions, ISS risk is defined to be the *plausibility* of information not being secure (see Appendix A for the mathematical definition of *plausibility function*).

This definition of risk is a somewhat conservative measure of risk as it is based on the worst-case scenario where any ambiguity (uncertainty) in the situation is added to any direct evidence of information security risk. To illustrate the definition, consider a situation where we have some belief, say, 0.30 on a 0–1 scale, that an IS asset is secure, a 0.20 level of belief that it is not secure, and a 0.5 level of ignorance indicating whether it is secure or not is unknown, based on what we know about the presence of threats and the corresponding countermeasures. This information tells us that the plausibility that the information is not secure is 0.7—that is, Pl (IS is not secure) = 0.7—which is the ISS risk. In other words, we have 70 percent risk that the IS is not secure based on all available information. If we obtain additional information such as control measures that mitigate relevant threats, then one would assess the impact of these control measures on the threats and combine this information with the earlier assessed beliefs. Dempster's rule may be used to obtain the overall plausibility that the IS is not secure to obtain a measure of overall ISS risk.

Evidential Reasoning Model for ISS Risk Assessment

The process of developing an evidential reasoning model consists of four phases: specification of the model structure (i.e., the evidential diagram), assessment and representation of evidence strength, determination of the overall level of ISS risk and each individual IS asset's risk, and cost–benefit analysis of ISS risk. We illustrate the process by considering the following hypothetical situation. Suppose a manager is interested in evaluating the ISS risk involved in one important IS asset—hardware. The corresponding evidential diagram is given in Figure 1, which is further elaborated in the following discussions.

Phase 1: Specify the Model Structure

An evidential diagram consists of assertions, evidence, and their interrelationships. Assertions include the main assertion and subassertions. The main assertion is the highest-level assertion; the subassertions are lower-level assertions. For the evaluation of the ISS risk involved in hardware, the main assertion is identified as "1. Hardware is secure." If hardware is secure, it must be protected from various threats,

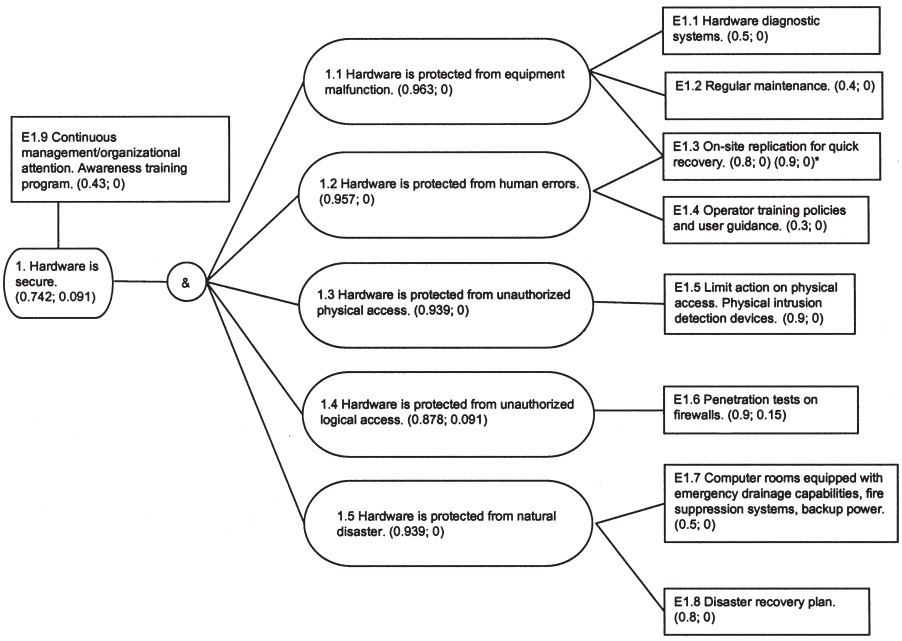


Figure 1. Hypothetical Evidential Diagram for Hardware Security Risk
Notes: The rectangular boxes represent evidence. Numbers in parentheses represent *m*-values or belief inputs provided by the ISS risk assessor. The first *m*-value represents the level of support the evidence provides to the assertion it pertains to, and the second *m*-value represents the level of support for the negation of the assertion it pertains to. The rounded boxes represent assertions. Detailed definitions for evidence are presented in Table 1.
* (0.8; 0) represents the level of support for subassertion 1; (0.9; 0) represents the level of support for subassertion 2.

including equipment malfunction, human errors, unauthorized physical access, unauthorized logical access, and natural disaster. Hardware being protected from each of these threats is expressed as subassertions 1.1 to 1.5.

In Figure 1, the rounded boxes represent assertion nodes. Note that the evidential diagram presented here is for illustrative purposes and that it is not complete in terms of assertions related to assets, threats, and countermeasures. One can always add new assertions related to any new additional threat or add a new asset and the corresponding threats and countermeasures as appropriate in the specific situation.

Relationships between assertions (e.g., between the main assertion and subassertions, and between higher-level subassertions and lower-level subassertions) need to be defined using logical relationships such as "and" and "or." We use the "and" relationship between the main assertion and the subassertions, which implies that the main assertion (higher-level subassertion) is true if and only if each subassertion (lower-level subassertion) is true.

Evidence represents the information that supports or negates assertions. Evidence nodes are represented by rectangular boxes in the evidential diagrams. Examples of

evidence include controls implemented by the organization to protect assets and procedures performed by the risk analyst to evaluate the controls. Evidence nodes are connected to the corresponding assertion(s) that they directly pertain to. For instance, in Figure 1, the evidence "E1.9 Continuous management/organizational attention. Awareness training program" directly pertains to assertion "1. Hardware is secure" and thus it is connected to that assertion. Evidence "E1.6 Penetration tests on firewalls" pertains to the subassertion "1.4 Hardware is protected from unauthorized logical access" and thus is connected to this subassertion.

In certain situations, one item of evidence can be connected to more than one assertion. For example, in Figure 1, evidence "E1.3 On-site replication for quick recovery" pertains to two subassertions, "1.1. Hardware is protected from equipment malfunction" and "1.2 Hardware is protected from human errors." Table 1 provides a detailed description of evidence in Figure 1.

The ISS risk assessor can use existing qualitative methodologies, such as scenarios [20], and questionnaires to develop the evidential diagram. Although costly, methods such as Delphi techniques[2] can be used to refine the completeness and accuracy of an evidential diagram.

Phase 2: Assess and Represent Strength of Evidence

In this step, users assess strength of evidence, which indicates the level of support that a piece of evidence provides in favor of or against the assertion it pertains to. Strength of evidence is represented by *m*-values. To avoid being heavily affected by individual subjective judgment, evidence strength can be elicited from multiple experts. Group meetings or Delphi techniques can be used to help achieve consensus among experts.

Phase 3: Determine the Overall Level of ISS Risk Related to an IS Asset and ISS Risk from Individual Threats

In this step, beliefs on assertions are computed by combining the strength of all the items of evidence (*m*-values), based upon the model's structure. This is done by propagating *m*-values through the network.[3] The present study uses Auditor's Assistant software [44] to conduct the computation.

Figure 1 shows that, given the assumed assessments of evidential strength, the overall belief supporting the assertion that "hardware is secure" is 0.742, the overall belief negating the assertion is 0.091, with 0.167 remaining as ambiguity. This suggests that the risk involved in hardware is 0.258—that is, the plausibility that hardware is not secure is 0.258.

By following the above steps, the decision maker will obtain a quantitative measure of ISS risk. However, this may not be the ultimate goal of the analysis. For example, managers may want to compute and compare the expected loss from threats for each IS asset, based on the assessed ISS risk, with and without countermeasures in

Table 1. Description of Evidence in Figure 1

Evidence number	Detailed description
E1.1	The company employs hardware or software products on an ongoing basis to detect or discover existing or impending problems.
E1.2	The company develops and adheres to a schedule of programmed preventive maintenance on various systems to avoid problems as well as completing maintenance tasks needed to correct problems that might occur.
E1.3	The company uses redundant hardware systems to allow quick recovery in the event of failure.
E1.4	The company develops thorough procedural documentation for both routine and special case computing tasks. It ensures that all operators are thoroughly trained and certified.
E1.5	The company allows access only to those with a verified need for entry and monitors security of all critical systems employing appropriate intrusion detection equipment and methods.
E1.6	The company arranges for either in-house or, perhaps preferably, third-party experts to attempt penetration into the company's network/computers.
E1.7	The company has considered all appropriate environmental factors in both primary and backup modes: cooling, power, fire suppression, and so on.
E1.8	The company has incorporated responses to disasters into a comprehensive disaster recovery plan, staffed appropriately to implement the plan, trained the staff on plan actions, and tested the acceptability of the plan.
E1.9	The company maintains a sharp focus on changing threats on a continuing basis using both management attention and well-conceived, ongoing training programs.

order to determine whether countermeasures are cost-effective. Next, we discuss how to conduct cost–benefit analysis under the evidential reasoning approach.

Cost–Benefit Analysis Under the Evidential Reasoning Approach

GIVEN THE LIMITED ORGANIZATIONAL RESOURCES available for security measures, any IS can only be secured at a level consistent with cost–benefit considerations rather than at a 100 percent secure level. In general, any security measure or combinations of measures should not cost more than the expected cost of tolerating the problem addressed by the measure(s) [37]. Therefore, cost–benefit analysis is critical for ISS risk management.

Here, we present a cost–benefit analysis of having control measures to reduce the information security risk under the Dempster–Shafer theory of belief functions. There are several approaches to decision making using an expected value approach under Dempster–Shafer theory [22, 23, 30, 47, 48, 55, 56, 62]. They all suggest a way to resolve the ambiguity and then perform the EV analysis. We use Strat's approach [55, 56, see also 51] because it provides the worst- and the best-case scenarios, which, in turn, provides the decision maker a choice between the two extremes.

Let us assume that m^{+}_{Ci}, m^{-}_{Ci}, and $(1 - m^{+}_{Ci} - m^{-}_{Ci})$, respectively, represent the overall belief that a given asset is protected, not protected, and ambiguity in the assertion that the asset is either protected or not protected from threat i in the presence of control measures pertaining to the threat. As suggested by Strat [55, 56], in order to perform the EV analysis under Dempster-Shafer theory, we introduce a parameter ρ ($1 \geq \rho \geq 0$), an indicator of a decision maker's risk attitude, where $\rho = 1$ indicates that the decision maker is extremely risk seeking and $\rho = 0$ indicates that he or she is extremely risk averse. The parameter ρ can take different values for different assertions (assets) because the risk attitude of a decision maker may vary along with his or her prioritization of IS assets. Parameter ρ allows the decision maker to resolve the ambiguity by allocating part of the ambiguity, that is, $\rho(1 - m^{+}_{Ci} - m^{-}_{Ci})$, in favor of the assertion that it is true and the remaining ambiguity, $(1 - \rho)(1 - m^{+}_{Ci} - m^{-}_{Ci})$, to the negation of the assertion that it is not true. Thus, the revised overall m-values can be written as

$$m'^{+}_{Ci} = m^{+}_{Ci} + \rho\left(1 - m^{+}_{Ci} - m^{-}_{Ci}\right)$$

and

$$m'^{-}_{Ci} = m^{-}_{Ci} + (1 - \rho)\left(1 - m^{+}_{Ci} - m^{-}_{Ci}\right).$$

The revised m-values add to one. The value of ρ determines how ambiguity is resolved. A value of $\rho = 0$ indicates the worst-case scenario, where the ambiguity, $(1 - m^{+}_{Ci} - m^{-}_{Ci})$, is assigned to the negation of the assertion. A value of $\rho = 1$ represents the best-case scenario, where all the ambiguity is assigned to the support of the assertion.

The expected loss due to n types of threats in the presence of a set of countermeasures for the corresponding threats can be expressed as (e.g., see [51])

$$\text{Expected loss } \textit{with} \text{ countermeasures} = \sum_{i=1}^{n} m'^{-}_{Ci} A_i, \tag{1}$$

where A_i is the potential loss of the IS asset due to ith threat.

The expected loss due to n types of threats in absence of a set of countermeasures for the corresponding threats can be expressed as

$$\text{Expected loss } \textit{without} \text{ countermeasures} = \sum_{i=1}^{n} m'^{-}_{NCi} A_i, \tag{2}$$

where A_i is as defined above, and m'^{-}_{NCi} represents the overall belief that *i*th threat occurs to the asset in absence of countermeasures (or no countermeasures as indicated by the subscript *NCi*) and is given by

$$m'^{-}_{NCi} = m^{-}_{NCi} + (1-\rho)\left(1 - m^{+}_{NCi} - m^{-}_{NCi}\right).$$

In the worst-case scenario ($\rho = 0$), Equations (1) and (2) reduce to

$$\begin{aligned}\text{Expected loss } \textit{with} \text{ countermeasures (worst case)} &= \sum_{i=1}^{n} m'^{-}_{Ci} A_i = \sum_{i=1}^{n} \left(1 - m^{+}_{Ci}\right) A_i \\ &= \sum_{i=1}^{n} \textit{ISS-Risk}_{Ci} A_i \end{aligned} \tag{3}$$

$$\begin{aligned}\text{Expected loss } \textit{without} \text{ countermeasures (worst case)} &= \sum_{i=1}^{n} m'^{-}_{NCi} A_i = \sum_{i=1}^{n} \left(1 - m^{+}_{NCi}\right) A_i \\ &= \sum_{i=1}^{n} \textit{ISS-Risk}_{NCi} A_i, \end{aligned} \tag{4}$$

where $\textit{ISS-Risk}_{Ci}$ and $\textit{ISS-Risk}_{NCi}$, respectively, represent the ISS risk when countermeasures are present and not present. As mentioned earlier, these risks are defined in terms of plausibility that the IS asset is not protected from the *i*th threat.

To evaluate the benefits of implementing countermeasures, the IS analyst can conduct a comparison of the expected organizational costs with and without the countermeasures. In the presence of a set of countermeasures, two types of cost exist. One is the cost for implementing the countermeasures. The other is the amount of potential loss of the asset due to the residual risk of threat occurrence even in the presence of the countermeasures. This amount is the expected value of the loss in dollar terms in the presence of countermeasure as defined in Equation (1) or in Equation (3) for the worst-case scenario. Without countermeasures, the cost is simply the expected amount of asset loss due to the risk of threat occurrence, which is defined in Equation (2) or in Equation (4) for the worst-case scenario.

If ISS risk management is efficient, the total costs with countermeasures should be lower than the costs without countermeasures, which is expressed as

$$\sum_{i=1}^{n} m'^{-}_{Ci} A_i + \sum_{i=1}^{n} K_i < \sum_{i=1}^{n} m'^{-}_{NCi} A_i, \tag{5}$$

where K_i represents the total costs of implementing a set of countermeasures for the *i*th threat.

The left side of the expression in Equation (5) represents the total expected organizational costs in the presence of countermeasures, and the right side of the expression represents the total expected organizational costs in the absence of countermeasures.

The next section describes how the above *m*-values, m'^{-}_{Ci} and m'^{-}_{NCi}, can be assessed through the use of an evidential diagram.

To further demonstrate the cost–benefit analysis presented above, let us continue using the hypothetical example used earlier. As an illustration, suppose the manager has estimated the following costs for implementing countermeasures and loss of hardware if threats occur:

IS asset	Total cost of controls	Total loss from threat occurrence
Hardware	$250,000	$400,000

Assume that the manager also believes that, in the absence of countermeasures, hardware is secured only at a 0.2 level of belief, on a 0–1 scale.

Based on Equation (5), the total expected organizational costs in the presence of countermeasures for hardware is as follows (see Figure 1 for *m*-values):

$$\text{Expected costs } \textit{with} \text{ countermeasures} = \left[0.091 + (1-\rho) \times 0.167\right] \times \$400,000 + \$250,000.$$

The expected costs in the absence of countermeasures for hardware is as follows:

$$\text{Expected costs } \textit{without} \text{ countermeasures} = (1-\rho) \times 0.8 \times \$400,000.$$

As discussed earlier, the estimation of ISS risk and organizational costs varies along with the risk preference parameter ρ. Next, we analyze two extreme situations, $\rho = 1$ and $\rho = 0$.

The best-case scenario ($\rho = 1$). Under this scenario, all the ambiguity is assigned to the support of the assertions. Therefore, the expected organizational costs for all three assets in the absence of countermeasures would be 0, less than costs in the presence of countermeasures. Under this scenario, the manager will choose not to implement any countermeasure.

The worst-case scenario ($\rho = 0$). Under this scenario, all the ambiguity is assigned to the negation of the assertions. Therefore, the estimated organizational costs for hardware in the presence of countermeasures and in the absence of countermeasures are as follows:

$$\text{Expected costs } \textit{with} \text{ countermeasures} = \left[0.091 + 0.167\right] \times \$400,000 + \$250,000 = \$353,200$$

$$\text{Expected costs } \textit{without} \text{ countermeasures} = 0.8 \times \$400,000 = \$320,000.$$

The above results suggest that, under the worst-case scenario, the security management of hardware is inefficient because, for hardware, the estimated costs in the presence of controls are $33,200 higher than those in the absence of controls. This suggests that the manager should examine the existing controls and take actions that will either

lead to a higher level of effectiveness or lower costs for current controls or reduce/eliminate the ineffective controls.

Sensitivity Analysis on the Evidential Reasoning Model

IN BOTH THE MANAGEMENT INFORMATION SYSTEMS (MIS) and other research fields, sensitivity analysis has often been adopted as a tool to evaluate a new approach. There is substantial awareness of the usefulness of sensitivity analysis to help understand the effect of various parameters and model specifications on a model's performance [7, 25]. Therefore, in this section, we employ sensitivity analysis to evaluate the effect of several important aspects of the proposed approach. The aspects studied include the assumed logical relationships among assertions, the location of evidence, and the strength of evidence.

To obtain sensitivity analysis results grounded in an actual ISS risk assessment situation, we perform the analyses based upon the proposed ISS risk assessment model applied to an actual WebTrust assurance engagement [2, 3].[4] The engagement was performed by an external assurance provider for a client we call ABC Company.[5]

ABC is a global company with a relatively long business history and several years of e-business history. A "big four" auditing and assurance firm provided assurance concerning ABC's disclosure of its electronic commerce business practices on its Web site and the effectiveness of ISS controls over transaction integrity and information security for three basic business functions during the year 2000.

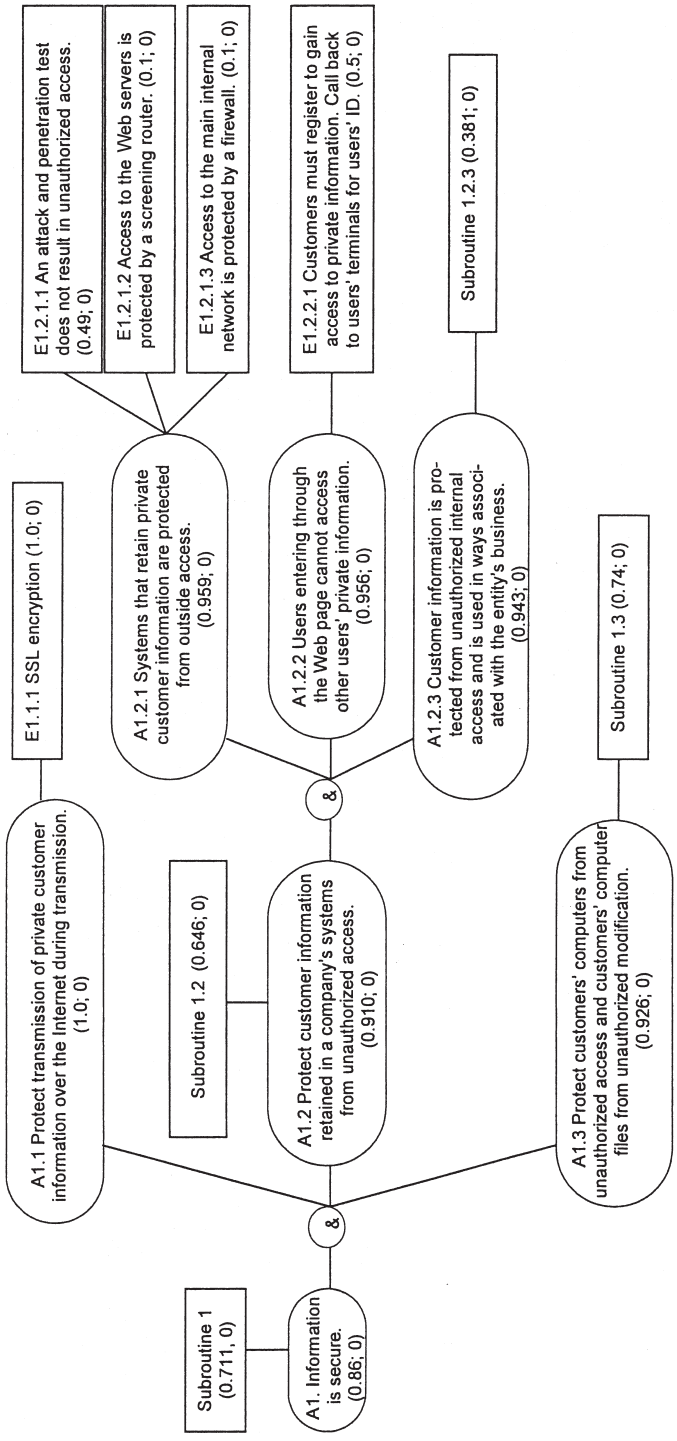
Based on the assurance results, the system was judged to be secure based on applicable American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (AICPA/CICA) WebTrust criteria in effect during the examination period. Therefore, a WebTrust seal and assurance report was issued (see Appendix B). The assurance firm provided us with access to the information needed to develop a real example of ISS risk assessment. The specific security risks examined focus on information security related to customer data and various risks that these data are not adequately protected from various threats.

Development of Evidential Diagram

Based upon the process suggested previously, an evidential diagram (see Figure 2) for the "information protection" assertion in ABC Company's assurance engagement was developed. The actual assurance engagement documented three assertion categories—business practices and information privacy disclosures, transaction integrity, and customer information protection. Customer information protection is the focus of the sensitivity analysis as it represents assurance directly related to ABC's ISS risk.

The structure of the example was defined by a combined effort of the authors and the audit manager based upon a 40-page fieldwork master file that documented the engagement. The file documented audit scope, assertions being investigated, and corresponding items of evidence gathered to evaluate the various assertions.

Part A


A1. Information is secure. (0.86; 0)
Subroutine 1 (0.711, 0)
&
A1.1 Protect transmission of private customer information over the Internet during transmission. (1.0; 0)
E1.1.1 SSL encryption (1.0; 0)
Subroutine 1.2 (0.646; 0)
A1.2 Protect customer information retained in a company's systems from unauthorized access. (0.910; 0)
&
A1.2.1 Systems that retain private customer information are protected from outside access. (0.959; 0)
E1.2.1.1 An attack and penetration test does not result in unauthorized access. (0.49; 0)
E1.2.1.2 Access to the Web servers is protected by a screening router. (0.1; 0)
E1.2.1.3 Access to the main internal network is protected by a firewall. (0.1; 0)
A1.2.2 Users entering through the Web page cannot access other users' private information. (0.956; 0)
E1.2.2.1 Customers must register to gain access to private information. Call back to users' terminals for users' ID. (0.5; 0)
A1.2.3 Customer information is protected from unauthorized internal access and is used in ways associated with the entity's business. (0.943; 0)
Subroutine 1.2.3 (0.381; 0)
A1.3 Protect customers' computers from unauthorized access and customers' computer files from unauthorized modification. (0.926; 0)
Subroutine 1.3 (0.74; 0)

05 srivastava.pmd

Part B

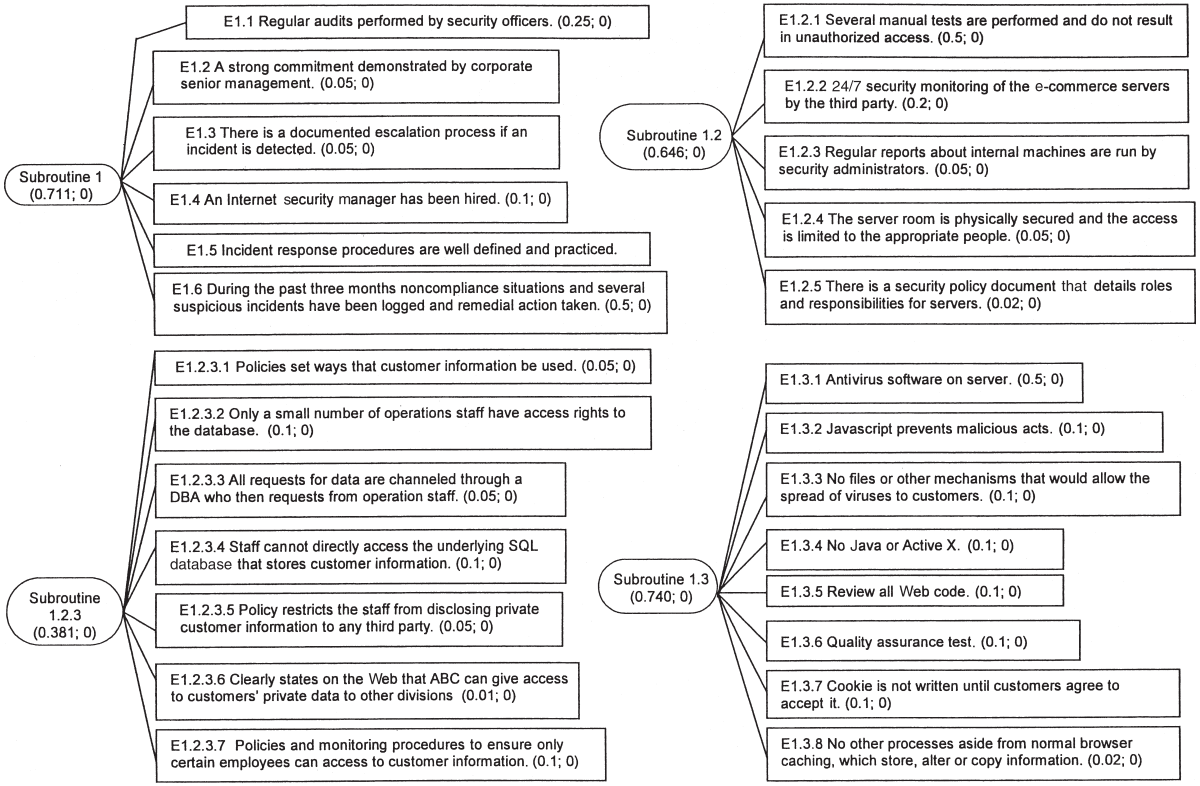


Figure 2. The Evidential Diagram for the Overall Assertion "Customer Information Is Secure" with an "and" Relationship Among Assertions in the WebTrust Assurance Engagement of ABC Company.

125

3/10/2006, 2:51 PM

As a starting point for sensitivity analysis, belief inputs (*m*-values) on strength of evidence were elicited from the audit manager.[6] The audit manager was a first-time user of the evidential reasoning approach under belief function theory. Therefore, two authors provided the audit manager with a half an hour of training that explained the principles needed to express beliefs under a belief function approach. After being exposed to the training, the audit manager still had some questions about the approach. Further discussions were made to clarify them.

The following fuzzy metric was also provided to facilitate his input of the strength of evidence: very low strength = [0 – 0.1); low strength = [0.1 – 0.3); median strength = [0.3 – 0.7); high strength = [0.7 – 0.9); very high strength = [0.9 – 1.0].[7] The entire process including the training, the troubleshooting discussion, and the completion of belief inputs by the audit manager lasted about three hours. Auditor's Assistant software [44] was used to aggregate *m*-values from all the items of evidence and to compute the ISS risk, which is the plausibility that customer data were not being adequately protected.[8]

Discussion of the Derived Evidential Diagram

The derived evidential diagram is presented in Figure 2. Part A of Figure 2 shows the overall model, which, as discussed earlier, consists of assertions concerning customer information security and evidence collected during the engagement to test the validity of these assertions. Due to space limitations, some items of evidence are grouped together and presented in Part B of Figure 2.

The model consists of one main assertion, three second-level assertions (subassertions), and three third-level assertions (sub-subassertions). The main assertion (A1), "information is secure," represents the overall security of the evaluated IS asset: customer information. Three subassertions, A1.1, A1.2, and A1.3, assert that information is protected from three vulnerabilities categorized by location: during transmission, during storage in the firm's systems, and during storage in customers' computers. Subassertion A1.2 deals with the security level of information retained in the firm's systems. This information is vulnerable to three major types of potential abusers: unauthorized outsiders, other customers, and internal employees. Therefore, under subassertion A1.2, three sub-subassertions, A1.2.1, A1.2.2, and A1.2.3, are identified to represent information protection from these three types of abusers.

Note that all 31 items of evidence in this model were assessed by the assurance provider to be positive. One possible explanation is that the assurance provider did not obtain any negative evidence during the engagement. An alternative explanation is that the audit team's strategy was a purely "positive evidence" strategy. In such an approach, the objective is to obtain sufficient positive evidence such that the belief that the "information is secure" assertion is true exceeds some threshold—say, 0.90. Thus, negative evidence would not need to be documented in the master file. In the sensitivity analyses performed later, we do investigate effects of negative evidence.

Based upon our evidential model with the "and"[9] relationship and strength of evidence assessments provided by the audit manager, the overall belief that the "infor-

mation is secure" is calculated to be "0.86, 0.0." This means that the assurance provider is 86 percent confident that the overall assertion "information is secure" is true and has zero belief that the assertion is not true since no negative evidence was obtained with respect to this assertion. However, there is 14 percent ambiguity or ISS risk remaining. The 14 percent ambiguity indicates a 14 percent overall risk that customer information is not adequately protected.

The evidential diagram model is a logical, structured, and comprehensive representation of all the assertions, corresponding items of evidence, and their relationships documented in the original audit documents. The original audit documents are largely unconnected audit facts, but the evidential diagram model provides systematic information that can be used by auditors and systems analysts in general to assess ISS risk and reliability.

Sensitivity Analysis Results

To evaluate the effect of several important aspects of the proposed approach, we next perform sensitivity analysis on the assumed logical relationships among assertions, the location of evidence, and the strength of evidence.

Impact of Relationship Among Assertions on the Overall ISS Risk Assessments

The model derived from ABC engagement and presented in Figure 2 is based on the "and" relationship among assertions. One possible shortcoming of the "and" relationship is that it can significantly weaken the overall belief of an assertion when it is used to aggregate beliefs from related subassertions [26, 54].[10] The more subassertions there are, the more significantly this "dilution effect" may become. In order to address the above problem with the "and" relationship, we next consider an alternative, "weighted average," relationship. The main reason to choose the "weighted average" relationship among many alternatives is that ISS risk analysis often involves users' prioritization of risks [51, 57]. The "weighted average" relationship can better represent the relative importance of the risk related to subassertions.

Similar to Shenoy and Shenoy [45], we use the "discounting" method to express the "weighted average" relationship in the belief functions framework. Each subassertion's m-values are discounted by some weight $1 - w_i$, where w_i represents the relative importance of subassertion *a.i.* A one-to-one relationship is established between an assertion a and its subassertion $a.i$:

$$m\left(\left\{(a, a.i), (\sim a, \sim a.i)\right\}\right) = w_i$$

$$m\left(\left\{(a, a.i), (\sim a, a.i), (a, \sim a.i), (\sim a, \sim a.i)\right\}\right) = 1 - w_i.$$

Table 2 defines the "weighted average" relationship between the assertion (subassertion) and each of its subassertions (sub-subassertions). Weights used to define

05 srivastava.pmd

128

Table 2. Definitions of the "Weighted Average" Relationships Between the Assertion, Subassertions, and Sub-Subassertions

	The "weighted average" relationship between the overall assertion 1 and each of its three subassertions 1.1, 1.2, and 1.3		The "weighted average" relationship between subassertion 1.2 and each of its three sub-subassertions 1.2.1, 1.2.2, and 1.2.3
R1–1.1	$m(\{(a_1, a_{1.1}), (\sim a_1, \sim a_{1.1})\}) = 0.4$ $m(\{(a_1, a_{1.1}), (\sim a_1, a_{1.1}), (a_1, \sim a_{1.1}), (\sim a_1, \sim a_{1.1})\}) = 0.6$	R1.2–1.2.1	$m(\{(a_{1.2}, a_{1.2.1}), (\sim a_{1.2}, \sim a_{1.2.1})\}) = 0.3$ $m(\{(a_{1.2}, a_{1.2.1}), (\sim a_{1.2}, a_{1.2.1}), (a_{1.2}, \sim a_{1.2.1}), (\sim a_{1.2}, \sim a_{1.2.1})\}) = 0.7$
R1–1.2	$m(\{(a_1, a_{1.2}), (\sim a_1, \sim a_{1.2})\}) = 0.4$ $m(\{(a_1, a_{1.2}), (\sim a_1, a_{1.2}), (a_1, \sim a_{1.2}), (\sim a_1, \sim a_{1.2})\}) = 0.6$	R1.2–1.2.2	$m(\{(a_{1.2}, a_{1.2.2}), (\sim a_{1.2}, \sim a_{1.2.2})\}) = 0.6$ $m(\{(a_{1.2}, a_{1.2.2}), (\sim a_{1.2}, a_{1.2.2}), (a_{1.2}, \sim a_{1.2.2}), (\sim a_{1.2}, \sim a_{1.2.2})\}) = 0.4$
R1–1.3	$m(\{(a_1, a_{1.3}), (\sim a_1, \sim a_{1.3})\}) = 0.2$ $m(\{(a_1, a_{1.3}), (\sim a_1, a_{1.3}), (a_1, \sim a_{1.3}), (\sim a_1, \sim a_{1.3})\}) = 0.8$	R1.2–1.2.3	$m(\{(a_{1.2}, a_{1.2.3}), (\sim a_{1.2}, \sim a_{1.2.3})\}) = 0.1$ $m(\{(a_{1.2}, a_{1.2.3}), (\sim a_{1.2}, a_{1.2.3}), (a_{1.2}, \sim a_{1.2.3}), (\sim a_{1.2}, \sim a_{1.2.3})\}) = 0.9$

3/10/2006, 2:51 PM

the "weighted average" relationship in Table 2 were provided by the audit manager based upon his expertise. The weights assigned to the three subassertions A1.1, A1.2, and A1.3 are, respectively, 0.4, 0.4, and 0.2. The weights assigned to the three subsubassertions A1.2.1, A1.2.2, and A1.2.3 are, respectively, 0.3, 0.6, and 0.1. Unequal weights assigned by the assurance provider further support the usefulness of a "weighted average" relationship in this context.

Using the same belief inputs as used in Figure 2, we create the model with the "weighted average" relationship among assertions that is shown in Figure 3. The overall belief on the assertion "information is secure" under the model with a "weighted average" relationship among assertions is 90 percent and the risk that "information is not protected" is 10 percent (see Figure 3). This assurance level is more consistent with a high level of assurance implied in the unqualified assurance report.[11] Recall that the model with the "and" relationship among assertions yielded an overall belief of 86 percent (see Figure 2).[12] The implied 14 percent assurance risk suggests extra audit work is needed to reach a higher level of assurance that interested parties may require. This may possibly lead to an inefficient assurance engagement.

The Impact of Evidence Location in the Hierarchy of Evidence

In this section, we perform sensitivity analyses to explore the impact of the location of evidence on the risk assessments using the model with the "and" relationship and the "weighted average" relationship among assertions. Location in the hierarchy of evidence indicates to which level of assertion (subassertion) a piece of evidence directly pertains. We choose one item of evidence respectively from each of the three levels of assertions in the model. Next, we observe how the overall belief on the main assertion "information is secure" changes as the strength of the chosen evidence varies from negative evidence (–0.9) to positive evidence of (+0.9).

Figure 4 presents the sensitivity analyses results.[13] The chart on the left represents results under the model with the "and" relationship; the chart on the right represents results under the model with the "weighted average" relationship. The slopes of lines represent the rate of change of the overall belief with respect to the strength of evidence. Under both models, we find similar results as follow.

Evidence at the overall assertion level yields the highest impact on the overall belief concerning the assertion "information is secure," evidence at the subassertion level yields the second-highest impact on the overall belief, and evidence at the subsubassertion level yields the lowest impact. This finding seems to be reflected in current financial statement audit practice [5], where evidence at the overall level is considered to be relatively more important compared to audit evidence specific to individual accounts or transaction streams.

The Impact of Strength of Evidence

Here, we examine how the strength of evidence affects the beliefs on assertions. Again, we focus on the overall risk concerning "information is secure." In our sensi-

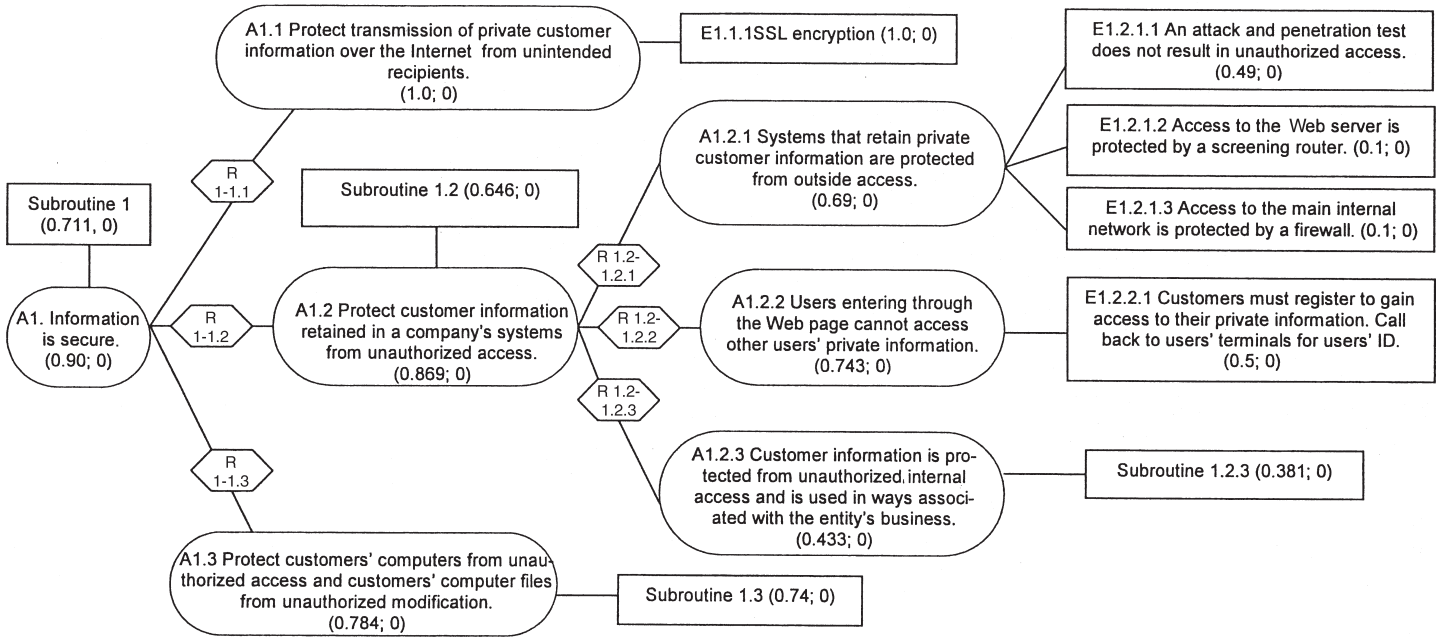


Figure 3. Evidential Diagram for the Overall Assertion "Customer Information Is Secure" with the "Weighted Average" Relationship Among Assertions in the WebTrust Assurance Engagement of ABC Company

Notes: The figures in the polygons represent the "weighted average" relationship between the assertion (subassertion) and each of its subassertions (sub-subassertions). See Table 2 for the definitions of these relationships. Subroutines are defined as those in Figure 2, Part B.

05 srivastava.pmd
130
3/10/2006, 2:51 PM

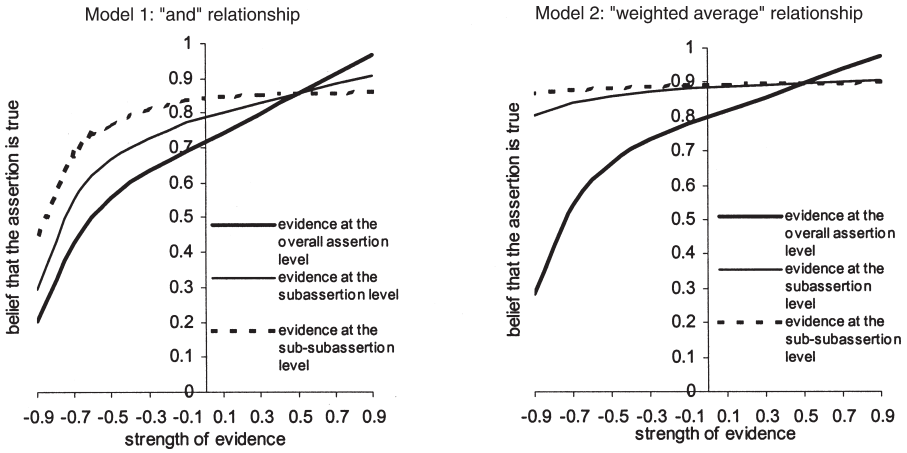


Figure 4. Impact of the Location of Evidence on the Belief of the Overall Assertion "Information Is Secure" Under Two Relationship Models

tivity analysis, we change the strength of all the evidence in our two models by +30 percent, +20 percent, +10 percent, –10 percent, –20 percent, and –30 percent. When the strengths of all items of evidence are increased by 10 percent, 20 percent, and 30 percent, under the model with the "and" ("weighted average") relationship, the corresponding increases in the overall belief are 4.4 percent, 8.06 percent, and 10.7 percent (2.00 percent, 3.72 percent, and 5.20 percent). When the strengths of all items of evidence are decreased by 10 percent, 20 percent, and 30 percent, under the model with the "and" ("weighted average") relationship, the corresponding decreases in the overall belief are 7.36 percent, 15.7 percent, and 24.8 percent (3.24 percent, 7.24 percent, and 12.18 percent). Figure 5 presents the results of this sensitivity analysis.

All items of evidence are positive in the above sensitivity analysis because the work papers provided from ABC did not contain negative evidence. We can observe, for positive evidence, a change of 10–20 percent in the input beliefs for positive items of evidence typically lead to a change of 4–8 percent in the overall belief. That is, for positive evidence, a small variation in the input beliefs often does not impact significantly the overall belief. This implies that the model is robust to small amounts of measurement error in assessing strength of positive evidence.

However, for negative evidence that indicates that the customer data may not be secure, variations in the input beliefs have a larger impact upon the overall belief. This is reflected in Figure 4. Regardless of the location of the evidence, the same magnitude of change in strength of negative evidence has a larger impact upon the overall belief than that of positive evidence. This implies that model users need to be more precise in assessing strength of negative evidence than that of positive evidence. The results in Figure 5 also indicate that the sensitivity level of the overall belief to changes in the strength of evidence is affected by the relationship among assertions. Generally speaking, the model with the "and" relationship is more sensitive to changes in the strength of evidence than the model with the "weighted average" relationship.

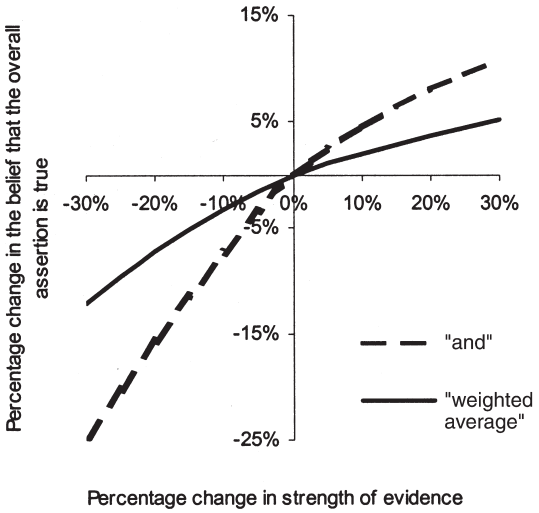


Figure 5. Impact of the Changes in the Strength of all Items of Evidence on the Belief of the Overall Assertion "Information Is Secure" Under Two Relationship Models

Conclusions

THIS STUDY DEVELOPS AN EVIDENTIAL REASONING approach for the risk analysis of ISS under the Dempster–Shafer theory of belief functions. This approach incorporates a number of possible advantages. First, the evidential reasoning approach extends existing methods by providing a rigorous, structured, and tractable approach to ISS risk assessment. The structure facilitates the explicit incorporation of the complexity of risks that derive from multiple IS assets, from multiple vulnerabilities to threats, and from multiple controls pertaining to a single threat, including situations where each control may provide different levels of assurance in protecting an asset from various threats. Second, the approach is based on belief function theory, which defines ISS risk in terms of the plausibility that an information resource is not adequately protected. The plausibility representation of risk is more comprehensive in the sense that it encompasses both knowledge about possible negative outcomes of security breakdowns and also any uncertainty or ignorance related to security assessments. Further, this approach is flexible as it allows the systems analyst to assess ISS risk either as a point estimate (plausibility) or as a range from the worst possible scenario to the best depending on the ambiguity remaining after evidence has been collected.

The paper also provides discussion on how to conduct a cost–benefit analysis under the evidential reasoning approach. To help better utilize the limited organizational resources available for ISS risk management, the illustrated cost–benefit analysis facilitates the evaluation of the effectiveness of ISS management from a cost–benefit perspective.

To evaluate the effects of important structural aspects of the proposed approach, we also performed sensitivity analysis using an evidential diagram developed based

upon information protection aspects of a real-world WebTrust assurance engagement. Study of this case provided some initial evidence on the feasibility of applying the evidential network approach previously discussed and provided some interesting empirical results that call for additional research. For example, the risk assessment documentation obtained from the assurance provider only compiled positive evidence of various controls that help mitigate ISS risks. Also, the calculated ISS risk related to the assertion that important information was adequately protected was shown to be at a relatively high 14 percent level.

Further sensitivity analyses were conducted on the logical relationship among the variables using "and" versus "weighted average" relationships, on the location of evidence in the evidential network, and on the strength of evidence (for both positive and negative evidence). These analyses provided both illustration of the kinds of analysis our approach facilitates and some results specific to the real-world case that we studied.

In conclusion, this study has provided conceptual discussions and empirically based sensitivity analyses that should help guide both practice and future research in formalizing an evidential reasoning approach to the analysis of ISS risk. Of course, the research has its limitations, some of which imply the need for additional research.

First, since this paper is the first study that introduces a formal evidential reasoning approach to ISS risk analysis and given confidentiality constraints on data related to our WebTrust illustration, we are not able to provide much empirical evidence of the advantages of this approach over others. Thus, field research is needed to empirically compare our approach with other methods. Second, the specification of model structure for the real example was done jointly by the authors and an audit manager. One question that arises is the extent to which users can independently complete such a task in practice. Since the development of the model structure is grounded upon users' understanding on the interrelationships among multiple factors involved in risk analysis, we expect that users with sufficient domain knowledge in the ISS risk analysis area, with relevant training and supporting documentation, can accomplish such a task. But much needs to be done to confirm such a conjecture.

Third, users of our approach need a basic understanding of belief functions and the assessments that need to be made. Fortunately, our experience in training the audit manager who provided input for the sensitivity analysis showed that an appropriate level of knowledge can be provided in a relatively short period of time, in this case, about a half an hour of training. Further, empirical research in the auditing domain suggests that decision makers are comfortable with using belief functions to represent their uncertainty judgments. Fourth, although the proposed approach offers advantages over existing methods, because it breaks down the risks and their plausibility to a finer level of detail, it still requires domain experts' belief inputs at the individual evidence level. Future research should be conducted to explore how to better elicit practitioner's assessments of the strength of the evidence. As discussed in the paper, one approach is to elicit evidence strength from multiple experts. Group meetings or Delphi techniques can be used to help achieve consensus among experts and perhaps attain needed reliability of assessments. Finally, clearly, the modeling approach should

be tested in other practice situations in addition to the WebTrust engagement discussed in this paper.

Acknowledgments: The authors thank the audit firm for making their audit work papers available for the study. They appreciate the help provided by the audit manager and for suggestions provided by Mike Ettredge, Greg Freix, Prakash Shenoy, and participants at the Accounting and Information Systems workshops at the University of Kansas and the Sixth Annual INFORMS Conference on Information Systems and Technology. In addition, the authors thank Jay F. Nunamaker Jr. and Robert O. Briggs, Guest Editors of the Special Issue, and the three anonymous reviewers for their constructive comments and valuable suggestions for revising the paper.

NOTES

1. Refer to Srivastava and Mock [52] and Yager et al. [63] for more elaboration and applications of belief function theory.

2. The Delphi technique begins with an initial open solicitation step followed by multiple rounds of feedback, and may be used to identify issues and obtain consensus among participants [37].

3. Shenoy and Shafer [46] have discussed this process in detail. The process of propagating *m*-values in a network becomes computationally quite complex. However, there are several software packages available [38, 44, 65] that facilitate the process.

4. Since this engagement was a WebTrust service engagement, no cost data was gathered by the auditor, and thus we were not able to use such real data for our cost–benefit analysis.

5. To meet management's need in evaluating ISS, various professional bodies are providing assurance services in this domain. For example, starting in the year 2000, accounting professionals have been providing WebTrust assurance on clients' IS (American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants) [2, 3]. Section 404 of the Sarbanes–Oxley Act of 2002 also requires external auditors to assess risks related to their clients' internal controls over financial reporting.

6. Note that the authors are not involved in the determinations of belief inputs. All *m*-values used in the study are the audit manager's independent judgments.

7. We use standard mathematical notation to represent intervals where the number next to a square bracket is not included in the interval, whereas the number next to a rounded bracket is included in the interval.

8. The information regarding the expected asset losses is not available in this study. Therefore, the step that determines the ISS risk in the form of dollar value is omitted.

9. The "and" relationship is used here because it is commonly used in prior literature. One alternative relationship, the "weighted average" relationship, is investigated in the following sensitivity analysis.

10. Krishnamoorthy [26] discusses the issues related to the "and" relationship and shows that when many subassertions are related by an "and" relationship, this may lead to counterintuitive results.

11. Although there is no quantitative standard for a high level of assurance, the conventional level for financial statement assurance is often thought to be 0.90 or 0.95.

12. In our model, there are only three subassertions and three sub-subassertions. As the number of subassertions (sub-subassertions) increases, the advantage of the "weighted average" relationship over the "and" relationship will become more obvious.

13. The analyses and results presented in this paper are based on the weights provided by the audit manager. We also performed sensitivity analyses by assuming equal weights, where each subassertion under one assertion is considered to be equally important. The sensitivity analyses results based upon the assumption of equal weights show no significant difference from those based upon the manager's weights.

REFERENCES

1. Alter, S., and Sherer, S. A general, but readily adaptable model of information system risk. *Communications of the AIS, 14,* article 1 (2004), 1–28.

2. American Institute of Certified Public Accountants. *AICPA/CICA WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce, version 1.0.* New York: AICPA, 1999.

3. American Institute of Certified Public Accountants. *AICPA/CICA WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce, version 3.0.* New York: AICPA, 2001.

4. Ball, L., and Harris, R. SMIS member: A membership analysis. *MIS Quarterly, 6,* 1 (1982), 19–38.

5. Bell, T.; Marrs, F.; Solomon, I.; and Thomas, H. *Auditing Organizations Through a Strategic-Systems Lens—The KPMG Business Measurement Process.* Montvale, NJ: KPMG Peat Marwick, 1997.

6. Bellovin, S.M. Computer security—An end state? *Communications of the ACM, 44,* 3 (2001), 131–132.

7. Byers, R.E., and Lederer, P.J. Retail bank services strategy: A model of traditional, electronic, and mixed distribution choices. *Journal of Management Information Systems, 18,* 2 (Fall 2001), 133–156.

8. Campbell, K.; Gordon, L.A.; Loeb, M.P.; and Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11,* 3 (March 2004), 431–448.

9. Cavusoglu, H.; Mishra, B.; and Raghunathan, S. The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9,* 1 (Fall 2004), 69–104.

10. Chen, S.Y.; Lin, W.C.; and Chen, C.T. Spatial reasoning based on multivariate belief functions. In J. Calder (ed.), *Proceedings of the 1992 IEEE Computer Society Conference on Computer Vision and Pattern Recognition.* Los Alamitos, CA: IEEE Computer Society Press, 1992, pp. 624–626.

11. Cohen, Y., and Shoshany, M. Analysis of convergent evidence in an evidential reasoning knowledge-based classification. In O. Altan (ed.), *Proceedings of the Twentieth International Society for Photogrammetry and Remote Sensing.* Amsterdam: Elsevier, 2004, pp. 916–920.

12. Cutter Consortium. Exactly what is risk management? Cutter Consortium Press Release, Arlington, MA, June 6, 2002 (available at www.cutter.com/press/020606.html).

13. Démotier, S.; Schön, W.; and Denoeux, T. Risk assessment based on weak information using belief functions: A case study in water treatment. *IEEE Transactions on Systems, Man and Cybernetics—Part C: Applications and Reviews, C99* (2004), 1–15.

14. Dempster, A.P. A generalization of Bayesian inference. *Journal of the Royal Statistical Society, Series B, 30* (1968), 205–247.

15. Dickson, G.W.; Leitheiser, R.L.; Wetherbe, J.C.; and Nechis, M. Key information systems issues for the 1980s. *MIS Quarterly, 8,* 3 (1984), 135–159.

16. Gopal, R.D., and Sanders, G.L. Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13,* 4 (Spring 1997), 29–47.

17. Gordon, J., and Shortliffe, E.H. The Dempster–Shafer theory of evidence. In B.G. Buchanan and E.H. Shortliffe (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project.* Reading, MA: Addison-Wesley, 1984, pp. 272–292.

18. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; and Richardson, R. CSI/FBI computer crime and security survey. Computer Security Institute, San Francisco, 2005.

19. Guarro, S.B. Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers and Security, 6,* 6 (1987), 493–504.

20. Hammond, R. Improving productivity through risk management. In R.F. Umbaugh (ed.), *Handbook of MIS Management,* 2d ed. Boston: Auerbach, 1988, pp. 655–665.

21. Hartog, C., and Herbert, M. 1985 opinion survey of MIS managers: Key issues. *MIS Quarterly, 10,* 4 (1986), 351–361.

22. Jaffray, J.-Y. Linear utility theory for belief functions. *Operations Research Letters, 8,* 2 (1989), 107–112.

23. Jaffray, J.-Y. Dynamic decision making with belief functions. In R.R. Yager, M. Fedrizzi, and J. Kacprzyk (eds.), *Advances in the Dempster–Shafer Theory of Evidence.* New York: Wiley, 1994, pp. 331–352.

24. Juul, N.C., and Jørgensen, N. The security hole in WAP: An analysis of the network and business rationales underlying a failure. *International Journal of Electronic Commerce, 7,* 4 (Summer 2003), 73–92.

25. Kleijnen, J.P.C. An overview of the design and analysis of simulation experiments for sensitivity analysis. *European Journal of Operational Research, 164,* 2 (July 2005), 287–300.

26. Krishnamoorthy, G. Discussion of aggregation of evidence in auditing: A likelihood perspective. *Auditing: A Journal of Practice and Theory, 12,* supplement (1993), 161–164.

27. McBurney, P., and Parsons, S. Using belief functions to forecast demand for mobile satellite services. In R.P. Srivastava and T. Mock (eds.), *Belief Functions in Business Decisions.* Heidelberg and New York: Physica-Verlag, 2002, pp. 281–315.

28. Moon, W.M. Integration of geophysical and geological data using evidential belief function. *IEEE Transactions on Geoscience and Remote Sensing, 28,* 4 (July 1990), 711–720.

29. National Institute of Standards and Technology (NIST) and National Security Agency (NSA). *Common Criteria for Information Technology Security Evaluation, version 2.1.* Fort Meade, MD, August 1999.

30. Nguyen, H.T., and Walker, E.A. On decision making using belief functions. In R.R. Yager, M. Fedrizzi, and J. Kacprzyk (eds.), *Advances in the Dempster–Shafer Theory of Evidence.* New York: John Wiley and Sons, 1994, pp. 311–330.

31. Niederman, F.; Brancheau, J.C.; and Wetherbe, J.C. Information systems management issues for the 1990s. *MIS Quarterly, 15,* 4 (1991), 475–502.

32. Pacelle, M., and Sidel, R. Security is breached at card processor. *Wall Street Journal* (June 20, 2005), A2.

33. Palacharla, P., and Nelson, P.C. Evidential reasoning in uncertainty for data fusion. In B. Bouchon-Meunier, R.R. Yager, and L.A. Zadeh (eds.), *Advances in Intelligent Computing: Fifth International Conference on Processing and Management of Uncertainty in Knowledge-Based Systems.* Berlin: Springer-Verlag, 1994, pp. 715–720.

34. Perschke, G.A.; Karabin, S.J.; and Brock, T.L. Four steps to information security. *Journal of Accountancy, 161,* 4 (1986), 104–113.

35. Pickard, R. Computer crime. *Information Center, 5,* 9 (September 1989), 18–27.

36. Post, G.V., and Diltz, J.D. A stochastic dominance approach to risk analysis of computer systems. *MIS Quarterly, 10,* 4 (1986), 363–375.

37. Rainer, R.K.; Snyder, C.A.; and Carr, H.H. Risk analysis for information technology. *Journal of Management Information Systems, 8,* 1 (Summer 1991), 129–147.

38. Saffiotti, A., and Umkehrer, E. Pulcinella: A general tool for propagating uncertainty in valuation networks. In B.D. D'Ambrosio, P. Smets, and P.P. Bonissone (eds.), *Proceedings of the Seventh National Conference on Artificial Intelligence.* San Francisco: Morgan Kaufmann, 1991, pp. 323–331.

39. Shafer, G. *A Mathematical Theory of Evidence.* Princeton: Princeton University Press, 1976.

40. Shafer, G. The combination of evidence. *International Journal of Intelligent Systems, 1* (1986), 155–179.

41. Shafer, G. Perspectives on the theory and practice of belief functions. *International Journal of Approximate Reasoning, 4,* 5–6 (1990), 323–362.

42. Shafer, G. The Dempster–Shafer theory. In S.C. Shapiro (ed.), *Encyclopedia of Artificial Intelligence,* 2d ed. New York: John Wiley and Sons, 1992, pp. 330–331.

43. Shafer, G., and Srivastava, R.P. The Bayesian and belief-function formalisms: A general perspective for auditing. *Auditing: A Journal of Practice and Theory, 9* (Supplement 1990), 110–148.

44. Shafer, G.; Shenoy, P.P.; and Srivastava, R.P. Auditor's Assistant: A knowledge engineering tool for audit decisions. In R.P. Srivastava and J.E. Rebele (eds.), *Proceedings of the 1988 Touche Ross/University of Kansas Symposium on Auditing Problems.* Lawrence: University of Kansas, 1988, pp. 61–79.

45. Shenoy, C., and Shenoy, P.P. Modeling financial portfolios using belief functions. In R.P. Srivastava and T. Mock (eds.), *Belief Functions in Business Decisions.* Heidelberg and New York: Physica-Verlag, 2002, pp. 316–332.

46. Shenoy, P.P., and Shafer, G. Axioms for probability and belief-function propagation. In R.D. Shachter, T.S. Levitt, J.F. Lemmer, and L.N. Kanal (eds.), *Uncertainty in Artificial Intelligence,* vol. 4. Amsterdam: North-Holland, 1990, pp. 169–198.

47. Smets, P. The combination of evidence in the transferable belief model. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 12,* 5 (May 1990), 447–458.

48. Smets, P. Constructing the pignistic probability function in a context of uncertainty. In M. Henrion, R.D. Shachter, L.N. Kanal, and J.F. Lemmer (eds.), *Uncertainty in Artificial Intelligence,* vol. 5. Amsterdam: Elsevier Science, North-Holland, 1990, pp. 29–40.

49. Srivastava, R.P. Decision making under ambiguity: A belief-function perspective. *Archives of Control Sciences, 6,* 1–2 (1997), 5–27.

50. Srivastava, R.P., and Liu, L. Applications of belief functions in business decisions: A review. *Information Systems Frontiers, 5,* 4 (December 2003), 359–378.

51. Srivastava, R.P., and Mock, T. Evidential reasoning for WebTrust assurance services. *Journal of Management Information Systems, 16,* 3 (Winter 1999–2000), 11–32.

52. Srivastava, R.P., and Mock, T. *Belief Functions in Business Decisions.* Heidelberg and New York: Physica-Verlag, 2002.

53. Srivastava, R.P., and Mock, T. Why we should consider belief functions in auditing research and practice. *Auditor's Report, 28,* 2 (2005), 58–65.

54. Srivastava, R.P., and Shafer, G. Belief-function formulas for audit risk. *Accounting Review, 67,* 2 (April 1992), 249–283.

55. Strat, T.M. Decision analysis using belief functions. *International Journal of Approximate Reasoning, 4,* 5–6 (1990), 391–417.

56. Strat, T.M. Decision analysis using belief functions. In R.R. Yager, M. Fedrizzi, and J. Kacprzyk (eds.), *Advances in the Dempster–Shafer Theory of Evidence.* New York: John Wiley and Sons, 1994, pp. 275–309.

57. Straub, D.W., and Welke, R.J. Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly, 22,* 4 (1998), 441–469.

58. Suh, B., and Han, I. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7,* 3 (Spring 2003), 135–161.

59. Tversky, A., and Kahnenman, A. Judgment under uncertainty: Heuristics and biases. *Science, 185* (1974), 1124–1131.

60. Wilkins, E., and Lavington, S.H. Belief functions and the possible worlds paradigm. *Journal of Logic and Computation, 12,* 3 (June 2002), 475–495.

61. Xu, H.; Hsia Y.-T.; and Smets, P. A belief-function based decision support system. In D. Heckerman and A. Mamdani (eds.), *Proceedings of the Ninth Uncertainty in Artificial Intelligence.* San Mateo, CA: Morgan Kaufmann, 1993, pp. 535–542.

62. Yager, R.R. Decision making under Dempster–Shafer uncertainties. Technical Report MII-915, Iona College, New Rochelle, NY, 1990.

63. Yager, R.R.; Fedrizzi, M.; and Kacprzyk, J. *Advances in the Dempster–Shafer Theory of Evidence.* New York: John Wiley and Sons, 1994.

64. Yuan, L. Companies face system attacks from inside, too. *Wall Street Journal* (June 1, 2005), B1.

65. Zarley, D.; Hsia, Y.-T.; and Shafer, G. Evidential reasoning using DELIEF. In R.G. Smith and T.M. Mitchell (eds.), *Proceedings of the Seventh National Conference of Artificial Intelligence.* Menlo Park, CA: AAAI Press, 1988, pp. 205–209.

66. Zviran, M., and Haga, W.J. Password security: An empirical study. *Journal of Management Information Systems, 15,* 4 (Spring 1999), 161–185.

Appendix A. Basics of Dempster–Shafer Theory

THE DEMPSTER–SHAFER THEORY OF BELIEF FUNCTIONS is a generalization of Bayesian theory of subjective probability [40, 41, 42]. In fact, the belief function reasoning is not new; it can be found in the work of George Hooper, Jakob Bernoulli, and Johann-Heinrich Lambert as early as the late seventeenth and early eighteenth centuries [39]. The current form of belief function theory is based on the work of Dempster during the 1960s [14] and Shafer during the 1970s [39]. Under Bayesian theory, the answer to the question of interest is represented in terms of probability. That is, under Bayesian theory, we associate objective or subjective probabilities to the possible answers to the question of interest. Under Dempster–Shafer theory, the degree of belief that can be associated with the possible answers to a question of interest may depend on the probability associated with the answers to a related question.

For example, suppose we want to know whether the IT manager has been following a given control procedure in the IS area. In response to this query, suppose the IT manager answers, "yes, we do follow the control procedure." The question is, based on this answer, what degree of belief can we associate with the IT manager's statement that "yes, we do follow the control procedure"? Well, this would depend on the subjective probability of how reliable the IT manager is. The manager's statement "yes, we follow the control procedure" is true if he or she is reliable but not necessarily true if he or she is unreliable. Suppose the subjective probability that the manager is reliable is 0.9, and he or she is unreliable is 0.1. Based on this subjective probability, we can associate 0.9 degree of belief that the management is following the control procedure and zero degree of belief (not 0.1 degree of belief) that they are not following the procedure. This zero degree of belief does not mean that we are sure that the IT manager is not following the control procedure, as a zero probability would; it simply means the IT manager's testimony gives no reason to believe that they are not following the control procedure. This 0.9 degree of belief that the management is following the control procedure along with the zero degree of belief that they are not following the procedure and 0.1 degree of belief that they may or may not be following the procedure constitutes a belief function.

In the following paragraphs, we provide the mathematical definitions of three important functions—*m*-values, beliefs, and plausibilities—under Dempster–Shafer theory that are relevant to the formulations developed in this paper.

m-Values

Suppose we have a decision problem with n possible elements or states of nature forming a mutually exclusive and collectively exhaustive set represented by $\{a_1, a_2, a_3, \ldots, a_n\}$. Call this entire set a frame represented by the symbol Θ. In the belief function formalism, uncertainty is not only assigned to the single elements of the frame but also to all other proper subsets of the frame and to the entire frame Θ. These uncertainties are called *m*-values, the basic belief assignment function [39]. Similar to probabilities, all these *m*-values add to one:

$$\sum_{A \subseteq \Theta} m(A) = 1,$$

where A represents all the subsets of the frame Θ, and $m(\phi) = 0$, that is, the m-value for the empty set is 0.

Basically, the m-value pertaining to a statement measures the degree of belief directly assigned to the statement based on the evidence. To illustrate the concept of m-values, let us consider again the earlier example of whether the management is following the control procedure or not. Based on the IT manager's response that they follow the control procedure and the subjective probabilities of 0.9 and 0.1 that the manager is reliable and unreliable, respectively, we can assign the following m-values: m(yes, they follow the procedure) = 0.9, which means that the testimony of the IT manager gives direct evidence that they follow the procedure if we believe in the manager's testimony; m(no, they do not follow the procedure) = 0, which implies that the manager's testimony provides no reason to believe that they do not follow the procedure; and $m(\{\text{yes, no}\}) = 0.1$, which represents ignorance. This 0.1 degree of belief pertains to both whether the management is following the procedure or not following the procedure. A zero degree of belief simply represents lack of evidence, unlike zero probability, which represents impossibility.

Belief Function

Basically, belief in a statement represents the total belief that the statement is true. Mathematically, the belief function for a subset of elements, say, A of a frame Θ, is defined as the sum of all the m-values for the individual elements in the subset, A, and the m-values for any subsets contained in the subset, A. In terms of symbols:

$$Bel(A) = \sum_{A \supseteq B} m(B),$$

where B is any subset of A. For example, belief in the subset $\{a_1, a_2\}$ is $Bel(\{a_1, a_2\}) = m(a_1) + m(a_2) + m(\{a_1, a_2\})$.

Again, using the above example of management following the control procedure, we get the following beliefs: Bel(yes, they follow the procedure) = 0.9, Bel(no, they do not follow the procedure) = 0, and $Bel(\{\text{yes, no}\}) = 1$. A belief of 1.0 in a statement means that the statement is for sure true, similar to a probability of 1. However, belief of zero in a statement means lack of evidence in support of the statement, unlike representing impossibility in probability.

Plausibility Function

Intuitively, the plausibility in a statement is the degree to which the statement is plausible in light of the evidence—the degree to which we do not disbelieve the statement. Mathematically, the plausibility function for a subset of elements A, of a frame

Θ, is defined to be the maximum possible belief that could be assigned to A if all future evidence were in support of A.

In terms of symbols, plausibility is defined as

$$Pl(A) = \sum_{A \cap B \neq \varnothing} m(B).$$

The plausibility function can also be defined in terms of belief function as

$$Pl(A) = 1 - Bel(\sim A).$$

Assuming A is an assertion that ISS is secured, the plausibility of $\sim A$, $Pl(\sim A)$, represents *maximum* possible risk that ISS is not secured.

Again using the earlier example, plausibility that the management is not following the control procedure is 0.1 since the belief that they are following the procedure is 0.9, that is,

$$Pl(\text{no, they do not follow}) = 1 - Bel(\text{yes, they follow}) = 1 - 0.9 = 0.1.$$

The plausibility that they follow the procedure is 1.0, that is,

$$Pl(\text{yes, they follow}) = 1 - Bel(\text{no, they do not follow}) = 1.0 - 0 = 1.0.$$

The risk that the management is not following the control procedure is 0.1 based on the plausibility of "no, they do not follow" the control procedure even though the belief that "no, they do not follow" the procedure is 0.

Dempster's Rule of Combination

Dempster's rule [39] is the fundamental rule, similar to Bayes theorem in probability theory, for combining two or more items of evidence in the belief function framework. For simplicity, let us illustrate Dempster's rule for only two items of evidence. In general, if m_1 and m_2 are the m-values representing two independent items of evidence pertaining to a frame, Θ, then the combined m-values (basic belief assignment function) for a subset A of frame Θ using Dempster's rule is given by

$$m(A) = K^{-1} \sum \left\{ m_1(B_1) m_2(B_2) \middle| B_1 \cap B_2 = A, A \neq \varnothing \right\},$$

where $K = 1 - \Sigma\{m_1(B_1)m_2(B_2)|B_1 \cap B_2 = \varnothing\}$, which represents the renormalization constant. The second term in K represents the conflict.

In order to illustrate Dempster's rule, let us consider a hypothetical example where we have two independent items of evidence pertaining to a binary variable A with values a that the variable is true and $\sim a$ that it is not true. Suppose that we obtain the following beliefs in terms of m-values from the two items of evidence:

$$\text{Evidence 1}: \; m_1(a) = 0.9, m_1(\sim a) = 0, m_1(\{a, \sim a\}) = 0.1$$

$$\text{Evidence 2}: \; m_2(a) = 0.8, m_2(\sim a) = 0.1, m_2(\{a, \sim a\}) = 0.1.$$

In applying Dempster's rule in this case, we first cross multiply the two sets of *m*-values and collect all the resulting *m*-values and assign them to the common element of the cross product. Next, we renormalize these *m*-values by dividing by renormalization constant. The cross multiplication and renormalization yield the following *m*-values and *K*:

$$K = 1 - \left[m_1(a)m_2(\sim a) + m_1(\sim a)m_2(a)\right] = 1 - \left[(0.9)(0.1) + (0.0)(0.8)\right]$$
$$= 1 - 0.09 = 0.91,$$

$$m(a) = \left[m_1(a)m_2(a) + m_1(a)m_2(\{a, \sim a\}) + m_1(\{a, \sim a\})m_2(a)\right] / K$$
$$= \left[(0.9)(0.8) + (0.9)(0.1) + (0.1)(0.8)\right] / 0.91 = 0.89 / 0.91 = 0.978,$$

$$m(\sim a) = \left[m_1(\sim a)m_2(\sim a) + m_1(\sim a)m_2(\{a, \sim a\}) + m_1(\{a, \sim a\})m_2(\sim a)\right] / K$$
$$= \left[(0.0)(0.1) + (0.0)(0.1) + (0.1)(0.1)\right] / 0.91 = 0.01 / 0.91 = 0.011,$$

$$m(\{a, \sim a\}) = \left[m_1(\{a, \sim a\})m_2(\{a, \sim a\})\right] / K =$$
$$\left[(0.1)(0.1)\right] / 0.91 = 0.01 / 0.91 = 0.011.$$

The total belief and plausibility that *a* and ~*a* are true are:

$$Bel(a) = 0.978 \text{ and } Bel(\sim a) = 0.011$$

$$Pl(a) = 1 - Bel(\sim a) = 0.989$$

$$Pl(\sim a) = 1 - Bel(a) = 0.022.$$

Appendix B. Auditor's Report of Web Assurance Service for ABC

Auditor's Report

To the Management of ABC Company:

We have audited management's assertion that ABC, during the period November 1, 2000, through January 31, 2001—

- disclosed its business and privacy practices for electronic commerce,
- complied with such business and privacy practices, and
- maintained effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately, and in conformity

with its disclosed business practices, and personally identifiable information obtained as a result of electronic commerce was protected in conformity with its disclosed privacy practices

in accordance with the American Institute of Certified Public Accountants (AICPA)/ Canadian Institute of Chartered Accountants (CICA) WebTrust Business Practices and Transaction Integrity Criteria and the AICPA/CICA WebTrust Privacy Criteria. These practices, disclosures, compliance, and controls are the responsibility of ABC's management. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the AICPA and the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC's disclosed business and privacy practices for electronic commerce transactions and the related controls over privacy and the processing of such transactions, (2) testing compliance with its disclosed business and privacy practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC management's assertion referred to above is fairly stated in all material respects in accordance with the AICPA/CICA WebTrust Business Practices and Transaction Integrity Criteria and Privacy Criteria.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) the degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust Seal for Consumer Protection on ABC's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

ABC Assurance Providers, LLP
January 31, 2001