A HOLISTIC RISK ANALYSIS METHOD FOR IDENTIFYING INFORMATION SECURITY RISKS

Janine L. Spears
The Pennsylvania State University, Smeal College of Business, University Park, PA 16802

Abstract: Risk analysis is used during the planning of information security to identify security requirements, and is also often used to determine the economic feasibility of security safeguards. The traditional method of conducting a risk analysis is technology-driven and has several shortcomings. First, its focus on technology is at the detriment of considering people and processes as significant sources of security risk. Second, an analysis driven by technical assets can be overly time-consuming and costly. Third, the traditional risk analysis method employs calculations based largely on guesswork to estimate probability and financial loss of a security breach. Finally, an IT-centric approach to security risk analysis does not involve business users to the extent necessary to identify a comprehensive set of risks, or to promote security-awareness throughout an organization. This paper proposes an alternative, holistic method to conducting risk analysis. A holistic risk analysis, as defined in this paper, is one that attempts to identify a comprehensive set of risks by focusing equally on technology, information, people, and processes. The method is driven by critical business processes, which provides focus and relevance to the analysis. Key aspects of the method include a business-driven analysis, user participation in the analysis, architecture and data flow diagrams as a means to identify relevant IT assets, risk scenarios to capture procedural and security details, and qualitative estimation. The mixture of people and tools involved in the analysis is expected to result in a more comprehensive set of identified risks and a significant increase in security awareness throughout the organization.

Keywords: risk analysis, information security, risk management, business process, data flow diagram, risk scenario.

1. INTRODUCTION

Managing information security is essentially managing a form of risk. The management of risk generally involves conducting a risk analysis to identify and evaluate risks, and then employing risk management techniques to mitigate or reduce risks where deemed appropriate. Likewise, the standard approach to managing information security involves conducting a risk analysis to identify risks to confidentiality, integrity, and availability of information systems, which is followed by risk management where safeguards are employed to mitigate those risks.

Traditional risk analysis methods applied to information systems focus foremost on technology with limited attention to people and processes. However, an information system is comprised of technology, people, processes, and data. Therefore, an effective security risk analysis must examine each of these aspects. As such, traditional risk analysis methods are seen as inadequate (e.g., Halliday et al., 1996; e.g., Gerber and von Solms, 2005). This paper examines the traditional risk analysis method, along with its strengths and limitations, and then proposes an alternative holistic method that addresses these limitations.

The paper is organized as follows. The next section defines risk and describes the purpose of a risk analysis. §3 describes the traditional risk analysis method, along with its strengths and limitations. Next, a holistic risk analysis method is proposed in §4, followed by an example and the method's benefits. §5 describes evaluation criteria for a risk analysis and how it applies to the proposed method. §6 suggests future areas of research, followed by a conclusion in §7.

2. RISK ANALYSIS

Risk is defined as (a) the possibility of loss or injury, and (b) the liability for loss or injury if it occurs (Merriam-Webster Inc., 1996). *Risk analysis*, in the context of information security, "is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause" (Pfleeger and Pfleeger, 2003). *Risk management* involves using the output from risk analysis to determine the selection and implementation of controls (safeguards) to reduce risk (Gerber and von Solms, 2005).

Risk analysis has traditionally been used in business for analyzing financial instruments and insurance products (e.g., Baskerville, 1991; Barrese and Scordis, 2003; Gerber and von Solms, 2005). In both cases, risk

analysis is driven by quantitative analysis of asset value to determine the feasibility of investing in the financial instrument or insurance product. Likewise in information security, (Alberts and Dorofee, 2001) risk analysis is often used to determine the feasibility of investing in security safeguards that reduce risks to information security (Baskerville, 1991). The other key reason for conducting risk analysis, which is the focus of this paper, is to identify security requirements (ISO/IEC 17799).

3. TRADITIONAL RISK ANALYSIS OF INFORMATION SECURITY

The traditional method for conducting information security risk analysis is technology-driven (e.g., Halliday et al., 1996; Humphreys et al., 1998 p. 49; Gerber and von Solms, 2005) because it focuses primarily on known threats to types of computing assets employed by an organization. This is due in large part to the historical origin of widely-used computer security guidelines (NIST, Common Criteria, RAND Corp, ISO 17799, SSE-CMM) that were initially developed for securing governmental and military computing infrastructures. Given that these leading security guidelines were not initially developed for information systems within a business environment, methods for identifying risks related to people (internal and external to the organization) and business processes are lacking.

For the purposes of this paper, the word *traditional* is used to denote risk analysis practices generally cited in the literature as being the conventional or common approach (e.g., Halliday et al., 1996; Kolokotronis et al., 2002; Suh and Han, 2003; Tan, 2003). Steps in a traditional risk analysis are summarized in Figure 1.

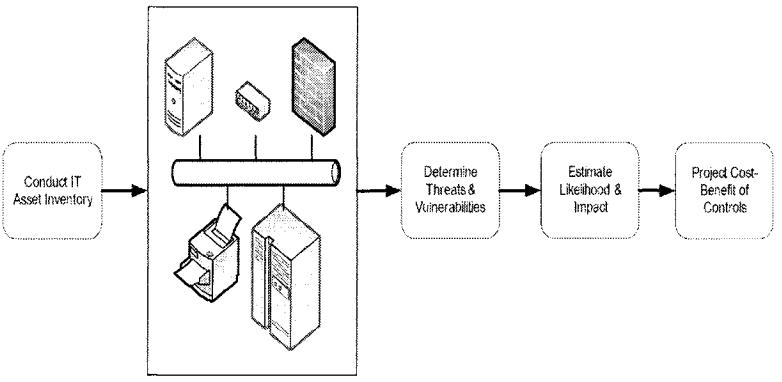

Figure 1. Traditional risk analysis for information security

The first step when conducting a risk analysis is to identify the IT assets to be protected. IT assets generally include hardware, software, data, people, documentation, and applicable facilities (Suh and Han, 2003). Note that although *people* is typically included as a type of IT asset, traditional risk analysis places minimal emphasis on people and is typically concerned solely with user identification and authentication. However, risk may be incurred by the procedures that people use to handle information. Next, for each identified asset, threats (undesired events that may occur) and vulnerabilities (existing weaknesses) related to confidentiality, integrity, and availability are identified. This is typically determined by using standard checklists (NIST, 2005) and the expertise of the security analyst. Risk is then quantified as the likelihood (i.e., probability) that a security event will occur (i.e., that a vulnerability will be exploited) multiplied by the expected monetary loss of such an event (risk = probability * expected loss). This output is used to compute a cost-benefit analysis of implementing security safeguards that will reduce risk to an acceptable level (e.g., Pfleeger and Pfleeger, 2003; Tan, 2003; Gerber and von Solms, 2005).

3.1 Strengths of Traditional Risk Analysis

The traditional risk analysis method for information security has several advantages. First, the method is widely known as the de facto standard taught in textbooks and endorsed by industry-accepted security guidelines (e.g., NIST, 2002; Pfleeger and Pfleeger, 2003).

Second, given that traditional risk analysis has focused primarily on technology, this aspect of security has been richly developed. For example, extensive lists of known threats and vulnerabilities to various technical assets are publicly available. These lists provide valuable guidance when conducting a risk analysis.

Third, automated software packages are available that perform the detailed calculations and manage the risk analysis data. These software packages are based on the traditional method of risk analysis.

Fourth, quantitative measures used in the traditional method can be used to support a cost-benefit analysis of investments in security safeguards. This is, of course, provided the calculations are reasonably accurate.

Finally, the traditional method of conducting a risk analysis for information security is closely related to risk analysis techniques employed in the financial and insurance sectors. This point, along with the mathematical foundation of the method, may add credibility.

3.2 Limitations of Traditional Risk Analysis

The traditional risk analysis method for information security has several key limitations. First, this technology-driven method places very limited emphasis on the people and process aspects of information systems. This is a major oversight, given that people and processes are widely considered to be the leading causes of security breaches (e.g., Siponen, 2000; Dhillon, 2001; Wade, 2004). In addition, there is no common approach to identifying which IT assets are to be included in the analysis. An IT professional developing a list of technical assets may not be aware of important user-developed spreadsheets and applications that contain significant security risks. Specific confidential information that warrants safeguarding may also be omitted.

Second, estimates of expected losses are based on the value of assets, and are widely inaccurate for a variety of reasons. Determining the value of intangible assets, such as information, is considered difficult, if not impossible, to estimate (Gerber and von Solms, 2005). Yet, information is one of the most important assets of an organization and is the focal point of information security. Estimates for the value of tangible assets may be inaccurate because in many cases only replacement costs are considered, which does not include the financial loss due to disruption of operations (Suh and Han, 2003). In cases where cost of disruption of operations is included in the asset value, the estimate is highly subjective. Finally, expected financial losses based on asset value typically do not include the social impact of a potential breach, such as loss of customer confidence (Bennett and Kailay, 1992).

Third, probability estimates of the likelihood of an identified vulnerability being exploited are commonly considered to be wild guesswork. One reason for this is that likelihood is determined by past history of security breaches, and this is largely underreported (e.g., Strang, 2001; Yazar, 2002; Keeney et al., 2005). Another reason that estimates of likelihood of occurrence are inaccurate is because making a more accurate estimate requires a high level of expertise by the estimator (e.g., Gerber and von Solms, 2005), which an organization may not possess. See Baskerville (1991) for additional discussion on weak quantitative estimates inherent in traditional risk analysis, which continue to exist.

A fourth limitation of the traditional method to risk analysis is the time and cost involved in conducting such an analysis. The bottom-up nature of the traditional method (i.e., driven from a micro, technology assets perspective) tends to be time-consuming, especially in medium to large

organizations (Halliday et al., 1996). Significant amounts of time may be spent analyzing assets of low importance to critical business processes.

A fifth limitation to a technology-focused analysis is that it is often solely conducted by IT professionals. This is problematic because business users are not involved, which only contributes to a lack of security awareness across an organization. Equally important, risks inherent in business processes that may be identifiable by a business user may go undetected by an IT professional.

In summary, the traditional method of conducting risk analysis for information security employs calculations based largely on guesswork to estimate probability and financial loss of a security breach. Secondly, its focus on technology is at the detriment of considering people and processes as significant sources of security risk. Finally, an IT-centric approach to security risk analysis does not involve business users to the extent necessary to identify a comprehensive set of risks, or to promote security-awareness throughout an organization.

4. A PROPOSED HOLISTIC RISK ANALYSIS METHOD

A holistic risk analysis, as defined in this paper, is one that attempts to identify a comprehensive set of risks by focusing equally on technology, information, people, and processes. The method is also holistic in nature by receiving input from a variety of participants within the organization, coupled with input from (security) industry-accepted guidelines. *The focus of this holistic method is on the identification of information security risks within critical business processes.* Key aspects of the method include user participation in the analysis, business-driven analyses, system diagrams as a means to extract relevant IT assets, and qualitative analysis.

Identifying risks that impact business processes provides a top-down analysis that defines the focus, scope, and relevance of the analysis. The proposed method, by its very nature, requires the involvement of a variety of senior management, business users and IT professionals. Once IT assets are identified and analyzed by participants, the method makes use of publicly available security checklists and guidelines (e.g., CERT, NIST) in order to capture known threats and vulnerabilities. Qualitative measures are used to estimate the impact of identified risks. These features counter the limitations of the traditional method of risk analysis identified in §3.

4.1 The Holistic Risk Analysis Method Described

In a holistic risk analysis, senior management identifies core business functions within the organization. Core business functions may be major departments within a firm, such as finance, marketing, human resources, procurement, etc. Senior management of each identified business function identifies critical business processes within their respective business function. Critical business processes are those that are vital to the financial stability and operation of an organization, of which there may be one or more. Examples include: process sales orders, procure raw materials, generate financial statements, process payroll, etc. Information security risks are identified by analyzing the associated technology, people, information, and processes that have the greatest impact on the operation of these business processes. The proposed holistic risk analysis method contains the following steps (see Figure 2):

1. Identify core business functions within the organization and their critical business processes
2. For each business process, identify the critical information system
3. Obtain an updated architecture diagram of the critical information system that includes its supporting infrastructure, and develop a list of IT assets
4. Obtain updated data flow diagrams (DFD) to identify user groups, sub-processes, external (including subordinate) systems, and information flows through the system
5. Identify confidential information from the DFDs
6. Update the list of IT assets based on information obtained from the DFDs
7. Determine the relative necessity (or importance) of each IT asset to the business process
8. Develop a risk scenario for each technical asset of high importance, each type of confidential information, and each user group with access to confidential information
9. Identify threats and vulnerabilities for each IT asset being analyzed
10. Estimate the impact of a security breach to the asset

An initial list of relevant technical assets is developed from architecture diagrams. This list of IT assets is later appended with assets identified in DFDs. Technological assets involved in handling confidential data are ranked as high in importance, even in cases where a technological asset is determined to be of low or medium necessity to the business process. For example, imagine a home healthcare products firm that occasionally transmits customer medical information by email to varying insurance companies. A paper copy is also mailed to the insurance company, so the email is not considered critical to the process of communicating medical

information. However, this data is confidential. Therefore, the email template and the security features employed are ranked as high importance due to the confidential nature of the data being transmitted.

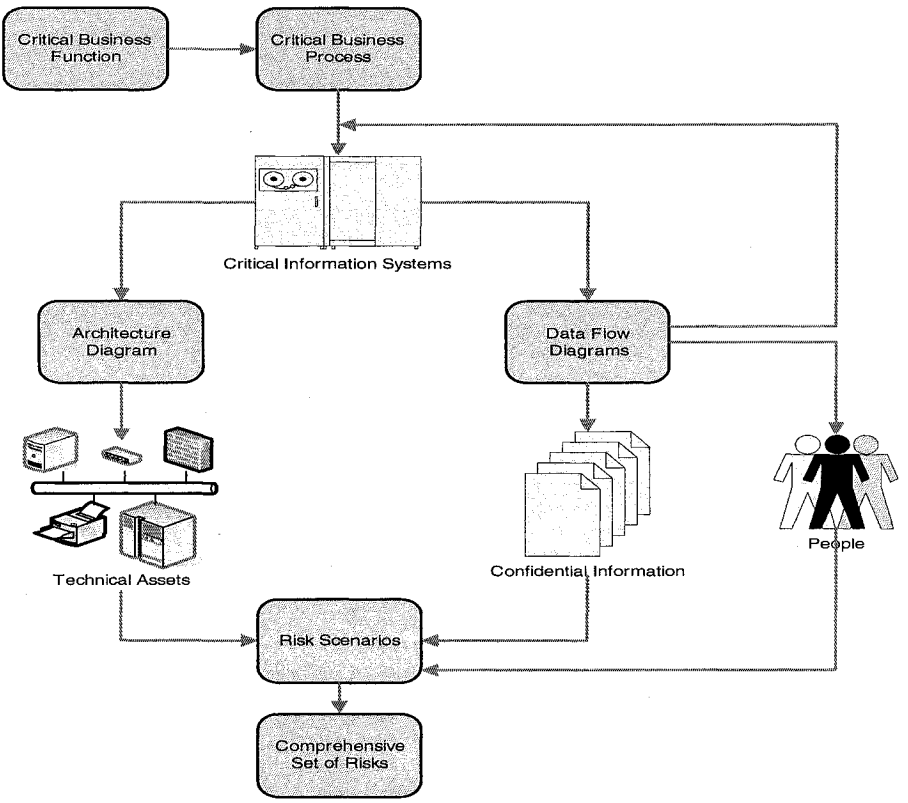

Figure 2. Holistic risk analysis for information security

Data flow diagrams are chosen because they illustrate how information flows to, from, and within a system. This is important information in a security risk analysis given that information is the essential asset to be protected. DFDs reveal information, people, and external (or subordinate) information systems. An initial (context) DFD is iteratively decomposed to lower levels of detail until all major processes within a system have been identified, along with the information flows to and from those processes.

Risk scenarios are narrative descriptions of situations that could result in a security event, either intentional or unintentional, within a targeted system (Freeman et al., 1997). In the holistic method, a risk scenario is created for each technological asset of high importance to the critical business process,

each type of confidential information, and each user group with access to confidential information. As shown in Figure 3, a risk scenario includes the asset; a list of existing security safeguards; threats and vulnerabilities; influences (e.g., conditions, events) that increase the likelihood that a vulnerability will be exploited; a history of known security breaches associated with the asset. The categories of *existing safeguards* and *influences on the likelihood of a breach* in the risk scenarios were borrowed from de Ru and Eloff (1996). The format varies slightly, depending upon the type of asset. Risk scenarios for technical assets and information types indicate who/what/where/how the asset is created, modified, deleted, and archived. Scenarios for user groups identify the contact manager, when/how security policies were communicated to the user group, types of confidential information accessed, and the purpose of that access.

As indicated in Figure 3, threats and vulnerabilities associated with an asset are contained in its risk scenario. Threats and vulnerabilities are identified from three sources: a) security industry-accepted guidelines and checklists, such as ISO17799, CERT, and NIST, b) expertise of participating IT staff, and c) information from the risk scenario that further stimulates thinking of participants who are knowledgeable of local practices.

Participants involved in developing a risk scenario for a given asset estimate the potential impact of a breach in the asset's confidentiality, integrity, and availability. Impact is estimated using a nominal scale and is determined for each vulnerability identified.

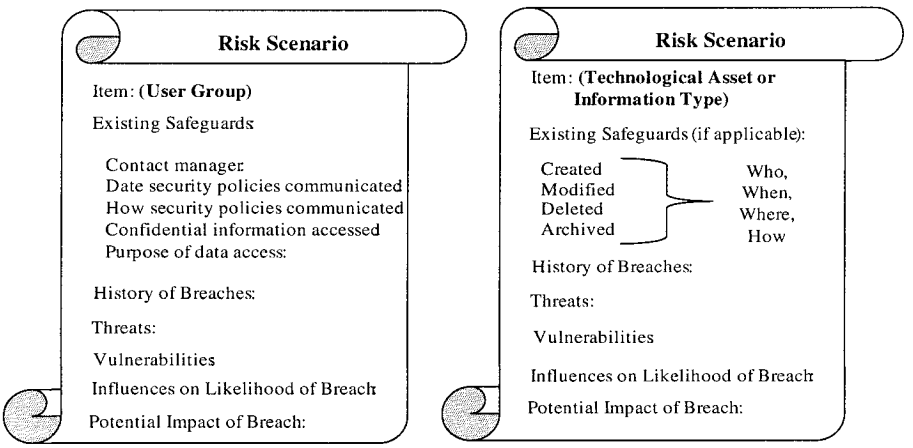

Figure 3. Risk scenarios

4.2 Example of a Holistic Risk Analysis

Finance is identified as a core business function. Senior management in the Finance department identify the *generation of financial statements* as a critical business process that is essential to the financial stability of the firm. An internally developed *financial reporting system* is used to generate the financial reports, and is identified as a critical information system for this business process. An existing architecture diagram depicts the network infrastructure supporting the financial reporting system. This diagram is updated to reflect any infrastructural changes. (If no architecture diagram previously existed, one would be created.) Using the architecture diagram, an IT professional from the network/infrastructure group develops a list of IT assets. This list contains servers, gateways, operating systems, etc.

A systems analyst and business user liaison work together to update existing data flow diagrams (DFDs) previously created during the analysis and design of the financial reporting system. (If no DFDs previously existed, they would be created.) DFDs indicate information flows to, from, and within a system. DFDs also indicate external entities (e.g., people, systems) that exchange data with the system and its sub-processes.

This example illustrates how a DFD and user input can reveal IT assets that may otherwise be overlooked in an analysis conducted solely by IT technical staff. As shown in Figure 4, a DFD indicates that press releases are sent to external press agencies. This information flow was not captured in the architecture diagram, or known by the IT technical staff, because the information is sent manually by fax. The DFD also indicates that Excel spreadsheets provide critical, confidential input to the financial reporting system. This detail is also unknown to IT technical staff because the spreadsheets are user-developed.

The high-level DFD in Figure 4 would be decomposed, such that sub-processes within the reporting system are identified, along with their information flows. Examples of sub-processes within the reporting system include *obtain current performance data*, *compute performance variances*, *compute historical comparisons*, etc. By analyzing sub-processes, information flows within a system are revealed at a greater level of detail, which in turn may identify areas of potential threat or vulnerability with regard to how information is handled. Upon completing an analysis of the DFD in this example, the list of IT assets is updated with the following assets:

- fax technologies used to send the press releases,
- the Excel spreadsheets,

- information types (e.g., actual and projected earnings, performance ratios, etc.),
- user groups (finance department, corporate executives, and press agencies),
- and other relevant assets identified in subordinate DFDs

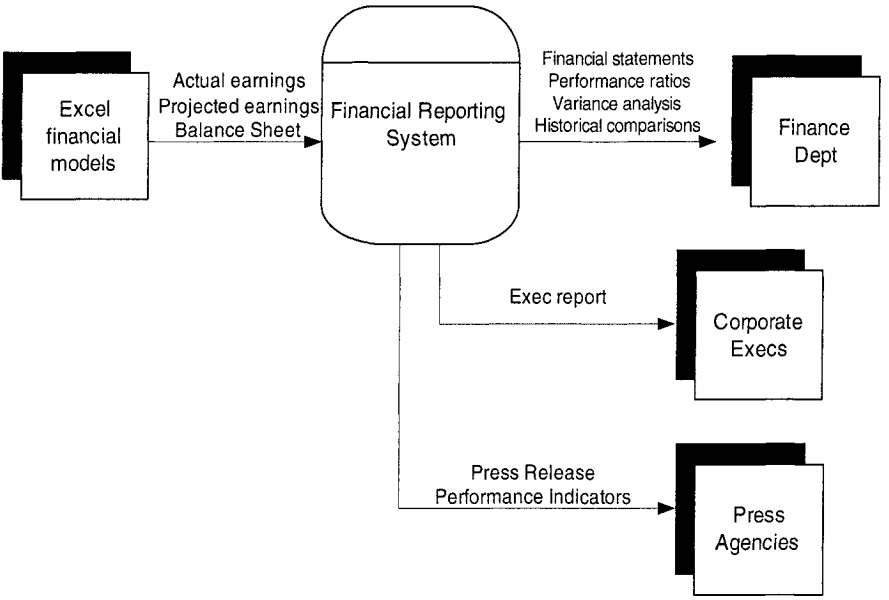

Figure 4. Contextual data flow diagram. (Squares indicate user groups and external systems. Arrows indicate information flows. A rounded rectangle represents a process.)

The teams that updated the architecture and data flow diagrams collaborate to rank the importance of the technological assets, user groups, and information to the business process of generating financial reports. The Excel spreadsheets that provide critical input to the financial reporting system are ranked of high importance, and a holistic risk analysis is subsequently conducted for this subordinate information system.

A risk scenario is created for each technological asset ranked as highly important, each type of confidential information, and each user group with access to confidential information. In this example, scenarios are developed for two types of information (actual and projected earnings), two user groups (finance department and corporate executives), and relevant technical assets identified in the architecture diagram. Data sent to press agencies are no longer confidential, so a risk scenario is not created for this user group. Note

that the Excel spreadsheets are treated as a subordinate system due to their detailed financial models, and a separate risk analysis is conducted.

Information contained in a risk scenario for *actual earnings* indicates the data is created from weekly files imported from Excel by a financial analyst. The only existing safeguard is control of user access to the financial reporting system that is authorized by a senior finance manager. A confidentiality breach had occurred the previous quarter when actual earnings were leaked to stock analysts and the press prior to the press release. On a scale of high, medium, low, the impact of such a breach is ranked high given its potential impact on stock market reaction. Other threats and vulnerabilities are identified using publicly available security checklists, the expertise of IT staff, and business users involved in creating the risk scenario. Scenario participants estimate the impact of each vulnerability should it be exploited.

4.3 Benefits of the Holistic Risk Analysis

A holistic risk analysis has several benefits over a traditional risk analysis. First, the risk analysis is driven by critical business processes – that is, those processes that are deemed essential to the financial stability and operation of the organization. In doing so, the risk analysis has a clear focus with relevant boundaries, and has a greater chance of obtaining participation from business management. Participation from business management is likely to result in a more comprehensive (holistic) set of identified risks than would be the case from a risk analysis conducted primarily by IT professionals. For example, risks to confidential information are more likely to be identified with input from business users. This is because business users are better suited to identify confidential data, which may be internal or external to the larger information system known to IT staff (e.g., could be contained in spreadsheets, etc.). Business users are also better suited to identify the procedures used in handling the data, as well identify the user groups (both internal and external to the firm) that have access to such data (either manually or electronically).

Second, the proposed model uses structured diagrams developed during the design of critical information systems. Using structured diagrams for security risk analysis further leverages the resources invested in developing such diagrams during the analysis and design of information systems. In addition, developing data flow (DFD) and architecture diagrams are techniques commonly employed within organizations and do not require security expertise. Using DFDs will likely result in additional IT staff being involved in security initiatives. For example, business and systems analysts

responsible for developing DFDs are not typically involved in the traditional risk analysis method. DFDs are used because they identify information flows in a system, and the related processes, people, and external (or sub) systems.

Third, risk scenarios capture the security history of an asset, as well as procedural information that may expose asset vulnerabilities that were not previously considered. For example, vulnerability checklists identify known technical vulnerabilities for an asset type. However, an organization's local operating environment contains additional vulnerabilities that must be uncovered. Many of these vulnerabilities are due to the existence or absence of procedures. The information contained in the risk scenarios stimulates thinking and are a third source of input for identifying threats and vulnerabilities (the other two sources being checklists and IT expertise).

Fourth, a qualitative estimate of the impact of a security breach has several advantages over calculating quantitative estimates. Qualitative measures simplify the risk estimation, are more useful when the asset value is irrelevant or unknown, and are less time-consuming (Bennett and Kailay, 1992; Suh and Han, 2003).

Finally, the proposed holistic risk analysis method requires the involvement of a multitude of roles, such as senior management, business users, systems analysts, database administrators, networking/infrastructure professionals, and security staff. Involving such a mixture of people in the process used to identify security risks will likely result in a significant increase in security awareness throughout the organization. This is a major benefit given that employees are said to typically not know their responsibilities in dealing with information security (Wade, 2004) and are responsible for an estimated 61% - 81% of violations to existing security safeguards (Bennett and Kailay, 1992; Dhillon, 2001).

5. EVALUATING THE HOLISTIC RISK ANALYSIS METHOD

Criteria for evaluating "an effective risk assessment," identified in Freeman, Darr, and Neely (1997), may be applied to a holistic risk analysis. As indicated in Table 1, an effective holistic risk analysis is *timely*, *cost-effective*, *complete*, *consistent*, and *understandable*.

Table 1. Evaluation criteria for an effective risk analysis (Freeman et al. 1997).

Evaluation Criteria	Description	Applied to the Holistic Method
Timely	The process provides the best available data in a timely manner.	A top-down risk analysis that is driven by critical business processes will have a clear focus with relevant boundaries, which is expected to result in a more timely analysis. Secondly, a qualitative analysis is expected to be less time-consuming because time is not spent gathering data for specific monetary or probabilistic values.
Cost-effective	The effort to accomplish the risk analysis is commensurate with the value of the results.	This holistic method leverages investments in existing architecture and data flow diagrams from system design. Secondly, this method is expected to uncover a greater number of procedural risks than the traditional method. It is anticipated that many of theses risks may lead to valuable, yet inexpensive, procedural safeguards.
Complete	The process is comprehensive with respect to some underlying structure, to reduce the likelihood of being "blind-sided" by an unanticipated security event.	A comprehensive analysis is conducted by involving both business users and various IT professionals. Secondly, the method places an equal focus on technology, information, people and processes.
Consistent	The rationale and methods for evaluating and reporting threats, vulnerabilities, and risks within the	Subsystems are identified via architecture diagrams, data flow diagrams, and system users and designers. Subsystems then follow the same analysis as the initial information system under analysis.

Evaluation Criteria	Description	Applied to the Holistic Method
	system are consistently applied and interpreted within and among all subsystems.	
Understandable	The rationale for the process and supporting techniques used to conduct the risk analysis have as *structured* a basis as possible and are understandable to customers without jargon. (This description replaces the word *technical* as specified by Freeman, Darr, and Neely with *structured* so that it applies to the entire holistic method.)	The holistic method involves business users and various IT professionals much in the same manner as that of the system design process. Similarly, the holistic method is performed in a structured manner with each participant, to include senior management, understanding the process and techniques as related to his/her role.

6. FUTURE RESEARCH

As previously mentioned, the traditional risk analysis method is often used to determine the economic feasibility of implementing security safeguards. Given that the traditional risk analysis method focuses on technological assets, attempts to manage information security have been skewed towards implementing increasingly complex technological safeguards (Dhillon, 2001). The holistic method requires participation from a greater variety of roles within the business and IT communities, and as such, a more comprehensive set of risks is expected to be identified than would be the case with the traditional method. A more comprehensive set of

risks would likely result in a higher number of low-cost, important, procedural safeguards. A future study would be useful to test these propositions.

The output of a risk analysis serves as input to risk management. This paper proposes a holistic method for conducting risk analysis that involves a variety of participants and parallels system analysis and design practices. Additional research is needed to develop a risk management method that effectively parallels the remainder of the SDLC (system development lifecycle) with the end goal of reducing security risks. Establishing a theoretical foundation for why information security practices can benefit from applying information systems development practices is also an important task for future research.

According to Cerullo and Cerullo (2004), there is a current trend to integrate business continuity planning with IT security planning. Business continuity planning involves identifying critical business functions and major risks that could result in their interruption. Future research could study how the holistic risk analysis method proposed in this paper could be used to facilitate business continuity planning and vice versa.

7. CONCLUSION

This paper examined the role of a risk analysis in information security planning and critiqued the traditional method for conducting risk analysis. An alternative holistic method for conducting risk analysis was proposed. The holistic method has several benefits. First, the risk analysis is driven by critical business processes, which provides focus and relevance to the analysis. Second, structured data flow and architecture diagrams developed during analysis and design of information systems are used during the security risk analysis, which further leverages the resources invested in developing such diagrams. Third, information contained in the risk scenarios stimulates thinking and are a third source of input for identifying threats and vulnerabilities (the other two sources being checklists and IT expertise). Finally, the proposed holistic risk analysis method requires participation from a variety of roles, such as senior management, business users, systems analysts, database administrators, networking/infrastructure professionals, and security staff. Involving such a mixture of people in the process used to identify security risks will likely result in a more comprehensive set of identified risks, and will likely result in a significant increase in security awareness throughout the organization.

REFERENCES

Barrese, J. and Scordis, N., 2003, "Corporate risk management." Review of Business 24(3):26.

Baskerville, R., 1991, "Risk analysis as a source of professional knowledge." Computers & Security 10(8):749-764.

Bennett, S. P. and Kailay, M. P., 1992. An application of qualitative risk analysis to computer security for the commercial sector. Computer Security Applications Conference, Eighth Annual, San Antonio, TX, IEEE.

CERT, 2001, Alberts, C. and Dorofee, A., (January 30, 2001), "An introduction to the OCTAVE method." from http://www.cert.org/octave/methodintro.html.

CERT, 2005, Keeney, M., Kowalski, E., Cappelli, D., Moore, A, Shimeall, T. and Rogers, S., (May 11, 2005),. Insider threat study: computer system sabotage in critical infrastructure sectors, http://www.cert.org.

Cerullo, V. and Cerullo, M. J., 2004, "Business continuity planning: a comprehensive approach." Information Systems Management 21(3):70-78.

de Ru, W. G. and Eloff, J. H. P., 1996, "Risk analysis modelling with the use of fuzzy logic." Computers & Security 15(3):239-248.

Dhillon, G., 2001, "Violation of safeguards by trusted personnel and understanding related information security concerns." Computers & Security 20(2):165-172.

Freeman, J. W., Darr, T. C. and Neely, R. B., 1997, Risk assessment for large heterogeneous systems. Computer Security Applications Conference, 1997, San Diego, CA, IEEE.

Gerber, M. and von Solms, R., 2005, "Management of risk in the information age." Computers & Security 24:16-30.

Halliday, S., Badenhorst, K. and von Solms, R., 1996, "A business approach to effective information technology risk analysis and management." Information Management & Computer Security 4(1):19.

Humphreys, E. J., Moses, R. H. and Plate, H. E., 1998, Guide to Risk Assessment and Risk Management. London, British Standards Institute.

ISO/IEC 17799, 2000, Information technology -- Code of practice for information security management.

Kolokotronis, N., Margaritis, C. and Papadopoulou, P., 2002, "An integrated approach for securing electronic transactions over the Web." Benchmarking 9(2):166-181.

Merriam-Webster Inc., 1996, Merriam-Webster's Dictionary of Law, Philippines, Merriam-Webster, Inc.

NIST, 2002, Risk Management Guide for Information Technology Systems. Washington, DC, National Institute of Standards and Technology: U.S. Department of Commerce, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

NIST, April 19, 2005, Practices & Checklists / Implementation Guides, National Institute of Standards and Technology: U.S. Department of Commerce, http://csrc.nist.gov/pcig/cig.html.

Pfleeger, C. P. and Pfleeger, S. L., 2003, Security in Computing. Upper Saddle River, NJ, Prentice Hall, pp. 462-475.

Siponen, M. T., 2000, "Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice." Information Management & Computer Security 8(5):197-210.

Strang, R., 2001, "Recognizing and meeting Title III concerns in computer investigations." Computer Crimes and Intellectual Property 49(2):8-13.

Suh, B. and Han, I., 2003, "The IS risk analysis based on a business model." Information & Management 41(2): pp. 149-158.

Tan, D., 2003, Quanitative Risk Analysis Step-by-Step, SANS Institute, http://www.sans.org.

Wade, J., 2004, The weak link in IT security. Risk Management. 51:32-37.

Yazar, Z., 2002, A qualitative risk analysis and management tool - CRAMM, SANS Institute, http://www.sans.org.