Performing a Security Risk Assessment

Ron Schmittling, CISA, CIA, CPA/CITP, is a manager in the Risk Services practice at Brown Smith Wallace LLC, where he leads the IT security and privacy practice. Schmittling's more than 16 years of experience also include more than five years in senior-level technical leadership roles at a major financial services firm, as well as positions in IT audit, internal audit and consulting for several international organizations.

Anthony Munns, CISA, CIRM, CITP, FBCS, NCC-UK, coleads Brown Smith Wallace's risk services practice. Prior to joining the firm, he led Arthur Andersen's St. Louis (Missouri, USA)-based risk consulting practice and led the Great Plains (USA) regional business systems audit practice. His specialty is bringing major company practices to small and medium-sized companies. In his more than 20-year career, Munns has managed and audited the implementation and support of enterprise systems and processes including SAP, PeopleSoft, Lawson, JD Edwards and custom client/server systems.

Enterprise risk management (ERM)[1] is a fundamental approach for the management of an organization. Based on the landmark work of the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[2] in the 1990s, its seminal *Enterprise Risk Management—Integrated Framework*,[3] has become a primary tool for organizational risk management. Regulators in the US have recognized the value of an enterprise risk approach, and see it as a requirement for the well-controlled organization. Two primary examples of this are compliance with the US Sarbanes-Oxley Act[4] and the US Health Insurance Portability and Accountability Act (HIPAA),[5] both of which require a periodic risk assessment.

Although regulations do not instruct organizations on how to control or secure their systems, they do require that those systems be secure in some way and that the organization prove to independent auditors that their security and control infrastructure is in place and operating effectively. The enterprise risk assessment methodology has become an established approach to identifying and managing systemic risk for an organization. And, more and more, this approach is being applied in such diverse fields as environmental Superfund,[6] health[7] and corporate ratings.[8]

> "Perform security risk assessments that employ the enterprise risk assessment approach and include all stakeholders."

Classically, IT security risk has been seen as the responsibility of the IT or network staff, as those individuals have the best understanding of the components of the control infrastructure. Moreover, security risk assessments have typically been performed within the IT department with little or no input from others.

This approach has limitations. As systems have become more complex, integrated and connected to third parties, the security and controls budget quickly reaches its limitations. Therefore, to ensure best use of the available resources, IT should understand the relative significance of different sets of systems, applications, data, storage and communication mechanisms. To meet such requirements, organizations should perform security risk assessments that employ the enterprise risk assessment approach and include all stakeholders to ensure that all aspects of the IT organization are addressed, including hardware and software, employee awareness training, and business processes.

IT enterprise security risk assessments are performed to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker's perspective. This process is required to obtain organizational management's commitment to allocate resources and implement the appropriate security solutions.

A comprehensive enterprise security risk assessment also helps determine the value of the various types of data generated and stored across the organization. Without valuing the various types of data in the organization, it is nearly impossible to prioritize and allocate technology resources where they are needed the most. To accurately assess risk, management must identify the data that are most valuable to the organization, the storage mechanisms of said data and their associated vulnerabilities.

REASONS/RATIONALE FOR PERFORMING A SECURITY RISK ASSESSMENT

Organizations have many reasons for taking a proactive and repetitive approach to addressing information security concerns. Legal and regulatory requirements aimed at protecting sensitive or personal data, as well as general public security requirements, create an

expectation for companies of all sizes to devote the utmost attention and priority to information security risks. An IT security risk assessment takes on many names and can vary greatly in terms of method, rigor and scope, but the core goal remains the same: identify and quantify the risks to the organization's information assets. This information is used to determine how best to mitigate those risks and effectively preserve the organization's mission.

Some areas of rationale for performing an enterprise security risk assessment include:

- **Cost justification**—Added security usually involves additional expense. Since this does not generate easily identifiable income, justifying the expense is often difficult. An effective IT security risk assessment process should educate key business managers on the most critical risks associated with the use of technology, and automatically and directly provide justification for security investments.
- **Productivity**—Enterprise security risk assessments should improve the productivity of IT operations, security and audit. By taking steps to formalize a review, create a review structure, collect security knowledge within the system's knowledge base and implement self-analysis features, the risk assessment can boost productivity.
- **Breaking barriers**—To be most effective, security must be addressed by organizational management as well as the IT staff. Organizational management is responsible for making decisions that relate to the appropriate level of security for the organization. The IT staff, on the other hand, is responsible for making decisions that relate to the implementation of the specific security requirements for systems, applications, data and controls.
- **Self-analysis**—The enterprise security risk assessment system must always be simple enough to use, without the need for any security knowledge or IT expertise. This will allow management to take ownership of security for the organization's systems, applications and data. It also enables security to become a more significant part of an organization's culture.
- **Communication**—By acquiring information from multiple parts of an organization, an enterprise security risk assessment boosts communication and expedites decision making.

ENTERPRISE SECURITY RISK ASSESSMENT METHODOLOGY

The enterprise risk assessment and enterprise risk management processes comprise the heart of the information security framework. These are the processes that establish the rules and guidelines of the security policy while transforming the objectives of an information security framework into specific plans for the implementation of key controls and mechanisms that minimize threats and vulnerabilities. Each part of the technology infrastructure should be assessed for its risk profile. From that assessment, a determination should be made to effectively and efficiently allocate the organization's time and money toward achieving the most appropriate and best employed overall security policies. The process of performing such a risk assessment can be quite complex and should take into account secondary and other effects of action (or inaction) when deciding how to address security for the various IT resources.

Depending on the size and complexity of an organization's IT environment, it may become clear that what is needed is not so much a thorough and itemized assessment of precise values and risks, but a more general prioritization. Determination of how security resources are allocated should incorporate key business managers' risk appetites, as they have a greater understanding of the organization's security risk universe and are better equipped to make that decision.

Each organization is different, so the decision as to what kind of risk assessment should be performed depends largely on the specific organization. If it is determined that all the organization needs at this time is general prioritization, a simplified approach to an enterprise security risk assessment can be taken and, even if it already has been determined that a more in-depth assessment must be completed, the simplified approach can be a helpful first step in generating an overview to guide decision making in pursuit of that more in-depth assessment.

> "Determination of how security resources are allocated should incorporate key business managers' risk appetites."

If one is unsure what kind of assessment the organization requires, a simplified assessment can help make that determination. If one finds that it is impossible to produce accurate results in the process of completing a simplified assessment—perhaps because this process does not take into account a detailed enough set of assessment factors—this alone can be helpful in determining the type of assessment the organization needs.

The assessment approach or methodology analyzes the relationships among assets, threats, vulnerabilities and other elements. There are numerous methodologies, but in general they can be classified into two main types: quantitative and qualitative analysis. The methodology chosen should be able to produce a quantitative statement about the impact of the risk and the effect of the security issues, together with some qualitative statements describing the significance and the appropriate security measures for minimizing these risks.

Security risk assessment should be a continuous activity. A comprehensive enterprise security risk assessment should be conducted at least once every two years to explore the risks associated with the organization's information systems. An enterprise security risk assessment can only give a snapshot of the risks of the information systems at a particular point in time. For mission-critical information systems, it is highly recommended to conduct a security risk assessment more frequently, if not continuously.

> "An enterprise security risk assessment can only give a snapshot of the risks of the information systems at a particular point in time."

PROCESS

The objective of a risk assessment is to understand the existing system and environment, and identify risks through analysis of the information/data collected. By default, all relevant information should be considered, irrespective of storage format. Several types of information that are often collected include:

- Security requirements and objectives
- System or network architecture and infrastructure, such as a network diagram showing how assets are configured and interconnected
- Information available to the public or accessible from the organization's web site
- Physical assets, such as hardware, including those in the data center, network, and communication components and peripherals (e.g., desktop, laptop, PDAs)
- Operating systems, such as PC and server operating systems, and network management systems
- Data repositories, such as database management systems and files
- A listing of all applications
- Network details, such as supported protocols and network services offered
- Security systems in use, such as access control mechanisms, change control, antivirus, spam control and network monitoring
- Security components deployed, such as firewalls and intrusion detection systems
- Processes, such as a business process, computer operation process, network operation process and application operation process
- Identification and authentication mechanisms
- Government laws and regulations pertaining to minimum security control requirements
- Documented or informal policies, procedures and guidelines

The project scope and objectives can influence the style of analysis and types of deliverables of the enterprise security risk assessment. The scope of an enterprise security risk assessment may cover the connection of the internal network with the Internet, the security protection for a computer center, a specific department's use of the IT infrastructure or the IT security of the entire organization. Thus, the corresponding objectives should identify all relevant security requirements, such as protection when connecting to the Internet, identifying high-risk areas in a computer room or assessing the overall information security level of a department. The security requirements should be based on business needs, which are typically driven by senior management, to identify the desired level of security protection. A key component of any risk assessment should be the relevant regulatory requirements, such as Sarbanes-Oxley, HIPAA, the US Gramm-Leach-Bliley Act and the European Data Protection Directive.

The following are common tasks that should be performed in an enterprise security risk assessment (Please note that these are listed for reference only. The actual tasks performed will depend on each organization's assessment scope and user requirements.):

- Identify business needs and changes to requirements that may affect overall IT and security direction.
- Review adequacy of existing security policies, standards, guidelines and procedures.
- Analyze assets, threats and vulnerabilities, including their impacts and likelihood.

- Assess physical protection applied to computing equipment and other network components.
- Conduct technical and procedural review and analysis of the network architecture, protocols and components to ensure that they are implemented according to the security policies.
- Review and check the configuration, implementation and usage of remote access systems, servers, firewalls and external network connections, including the client Internet connection.
- Review logical access and other authentication mechanisms.
- Review current level of security awareness and commitment of staff within the organization.
- Review agreements involving services or products from vendors and contractors.
- Develop practical technical recommendations to address the vulnerabilities identified, and reduce the level of security risk.

Mapping threats to assets and vulnerabilities can help identify their possible combinations. Each threat can be associated with a specific vulnerability, or even multiple vulnerabilities. Unless a threat can exploit a vulnerability, it is not a risk to an asset.

> "This interrelationship of assets, threats and vulnerabilities is critical to the analysis of security risks."

The range of all possible combinations should be reduced prior to performing a risk analysis. Some combinations may not make sense or are not feasible. This interrelationship of assets, threats and vulnerabilities is critical to the analysis of security risks, but factors such as project scope, budget and constraints may also affect the levels and magnitude of mappings.

Once the assets, threats and vulnerabilities are identified, it is possible to determine the impact and likelihood of security risks.

Impact Assessment

An impact assessment (also known as impact analysis or consequence assessment) estimates the degree of overall harm or loss that could occur as a result of the exploitation of a security vulnerability. Quantifiable elements of impact are those on revenues, profits, cost, service levels, regulations and reputation. It is necessary to consider the level of risk that can be tolerated and how, what and when assets could be affected by such risks. The more severe the consequences of a threat, the higher the risk. For example, if the prices in a bid document are compromised, the cost to the organization would be the product of lost profit from that contract and the lost load on production systems with the percentage likelihood of winning the contract.

Likelihood Assessment

A likelihood assessment estimates the probability of a threat occurring. In this type of assessment, it is necessary to determine the circumstances that will affect the likelihood of the risk occurring. Normally, the likelihood of a threat increases with the number of authorized users. The likelihood can be expressed in terms of the frequency of occurrence, such as once in a day, once in a month or once in a year. The greater the likelihood of a threat occurring, the higher the risk. It can be difficult to reasonably quantify likelihood for many parameters; therefore, relative likelihood can be employed as a ranking. An illustration of this would be the relative likelihood in a geographical area of an earthquake, a hurricane or a tornado, ranked in descending order of likelihood.

A systems example is the high likelihood of an attempt to exploit a new vulnerability to an installed operating system as soon as the vulnerability is published. If the system affected is classified as critical, the impact is also high. As a result, the risk of this threat is high.

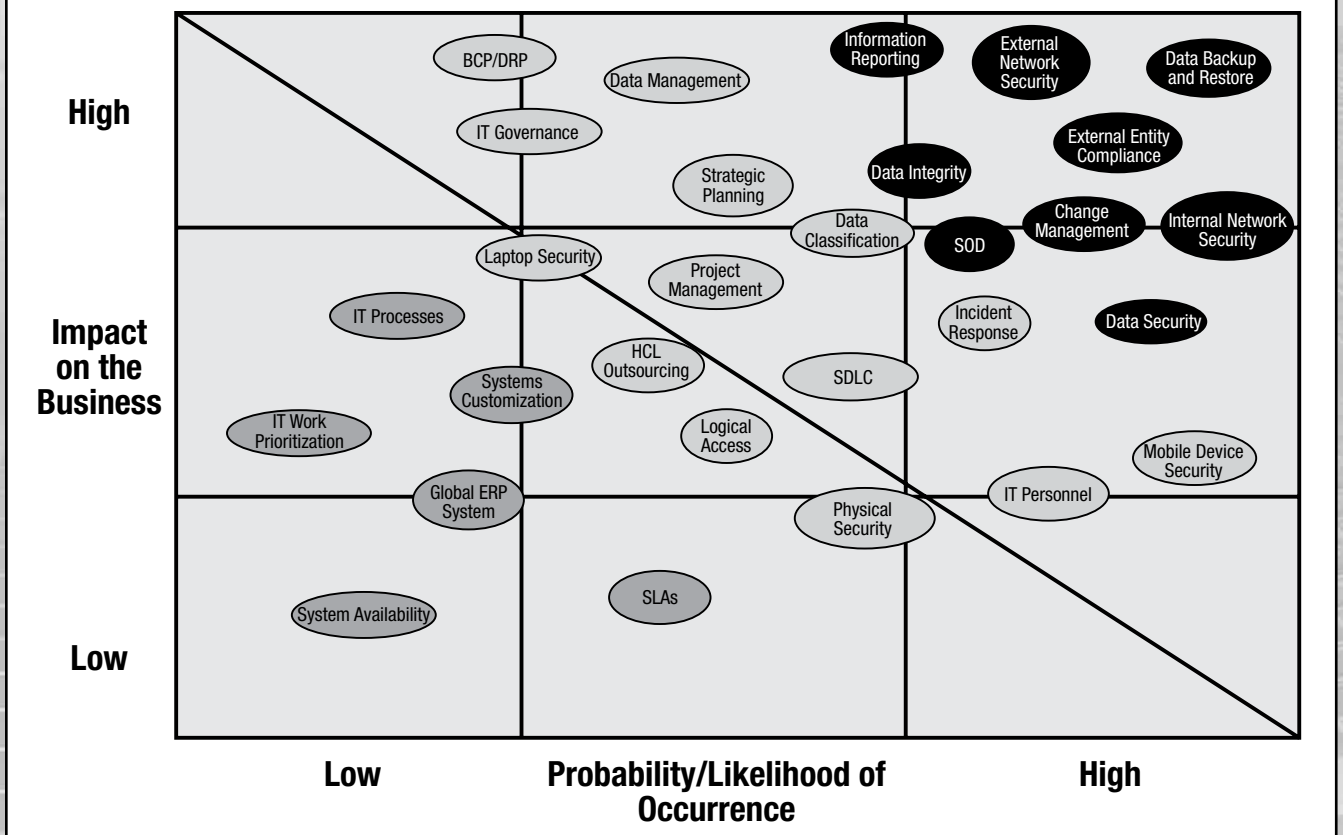
For each identified risk, its impact and likelihood must be determined to give an overall estimated level of risk. Assumptions should be clearly defined when making the estimation. This two-dimensional measurement of risk makes for an easy visual representation of the conclusions of the assessment. See **figure 1** for an example risk map.

ORGANIZATIONAL VALUE

Institutionalizing a practical risk assessment program is important to supporting an organization's business activities and provides several benefits:

1. Risk assessment programs help ensure that the greatest risks to the organization are identified and addressed on a continuing basis. Such programs help ensure that the expertise and best judgments of personnel, both in IT and the larger organization, are tapped to develop reasonable steps for preventing or mitigating situations that could interfere with accomplishing the organization's mission.
2. Risk assessments help personnel throughout the organization better understand risks to business operations. They also teach them how to avoid risky practices, such as disclosing passwords or other sensitive information, and

Figure 1—Risk Map



recognize suspicious events. This understanding grows, in part, from improved communication among business managers, system support staff and security specialists.

3. Risk assessments provide a mechanism for reaching a consensus as to which risks are the greatest and what steps are appropriate for mitigating them. The processes used encourage discussion and generally require that disagreements be resolved. This, in turn, makes it more likely that business managers will understand the need for agreed-upon controls, feel that the controls are aligned with the organization's business goals and support their effective implementation. Executives have found that controls selected in this manner are more likely to be effectively adopted than controls that are imposed by personnel outside of the organization.
4. A formal risk assessment program provides an efficient means for communicating assessment findings and recommending actions to business unit managers as well as to senior corporate officials. Standard report formats and the periodic nature of the assessments provide organizations a means of readily understanding reported information and comparing results between units over time.

Ultimately, enterprise security risk assessments performed with measurably appropriate care are an indispensable part of prioritizing security concerns. Carrying out such assessments informally can be a valuable addition to a security issue tracking process, and formal assessments are of critical importance when determining time and budget allocations in large organizations.

In contrast, taking a haphazard approach to security concern prioritization can lead to disaster, particularly if a problem falls into a high-risk category and then ends up neglected. IT-specific benefits of performing an enterprise security risk assessment include:

- Providing an objective approach for IT security expenditure budgeting and cost estimation
- Enabling a strategic approach to IT security management by providing alternative solutions for decision making and consideration
- Providing a basis for future comparisons of changes made in IT security measures

PITFALLS/LESSONS LEARNED

One of the key dangers of performing an enterprise security risk assessment is assuming where all the risks lie. It is important when structuring an enterprise security risk assessment to include as many stakeholders as possible. In one recent assessment, only IT management was to be interviewed, with the exception of a few internal audit organization members. While they certainly had many valid concerns, the group did not have the breadth of experience to form a complete picture of risk within the organization. By including a wider selection of operational, finance and human resources management, high-risk potentialities can be identified in areas such as research and development, HIPAA compliance, and sales management.

It is important to include personnel who are not only experienced in the complexities of systems and processes, but also have the ability to probe for areas of risk. A checklist is a good guideline, but is only the starting point in the process. With an experienced interviewer, the process can be as educational for the interviewee as it is for identifying risks.

Organizational executives have limited time, and it is often difficult to get on their calendars. There are three key steps to ease this part of the process:

1. Request that the executive sponsor directly address the interviewees by announcing the purpose of the risk assessment and its importance to the organization.
2. Within 48 hours of that communication, have the sponsor's office schedule the initial interview.
3. Send a tailored checklist to the executive prior to the interview and ask him/her to review it. This last step is to prepare him/her for the subject areas of the risk assessment, so that any apprehensions or reservations are allayed as he/she understands the boundaries of the interview.

It is important not to underestimate the value of an experienced facilitator, particularly for the higher-level interviews and the process of determining the ranking of risk likelihood. The use of experienced external resources should be considered to bring even more objectivity to the assessment.

CONCLUSION

An information security framework is important because it provides a road map for the implementation, evaluation and improvement of information security practices. As an organization implements its framework, it will be able to articulate goals and drive ownership of them, evaluate the security of information over time, and determine the need for additional measures.

> "Overall, an organization must have a solid base for its information security framework."

A common element in most security best practices is the need for the support of senior management, but few documents clarify how that support is to be given. This may represent the biggest challenge for the organization's ongoing security initiatives, as it addresses or prioritizes its risks.

Specifically, an enterprise security risk assessment is intended to be suitable for the following, which could be specific to any organization:

- A way to ensure that security risks are managed in a cost-effective manner
- A process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met
- A definition of new information security management processes
- Use by management to determine the status of information security management activities
- Use by internal and external auditors to determine the degree of compliance with the policies, directives and standards adopted by the organization
- For implementation of business-enabling information security
- To provide relevant information about information security to customers

Overall, an organization must have a solid base for its information security framework. The risks and vulnerabilities to the organization will change over time; however, if the organization continues to follow its framework, it will be in a good position to address any new risks and/or vulnerabilities that arise.

ENDNOTES

[1] The COSO *Enterprise Risk Management—Integrated Framework*, published in 2004, defines ERM as a "…process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

[2] COSO is a voluntary private-sector organization, established in the US, dedicated to providing guidance to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud and financial reporting.

[3] COSO, *Enterprise Risk Management—Integrated Framework Executive Summary*, September 2004, *www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf*

[4] US Congress, Sarbanes-Oxley Act of 2002, section 404, "Assessment of Internal Control," USA, 2002

[5] US Congress, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Title 2, "Administrative Simplification," USA, 1996

[6] US Environmental Protection Agency (EPA), "What Is Risk Assessment?," USA, *www.epa.gov/risk/basicinformation.htm#arisk*

[7] Office of Environmental Health Hazard Assessment, "A Guide to Health Risk Assessment," California Environmental Protection Agency, *http://oehha.ca.gov/pdf/HRSguide2001.pdf*

[8] Standard & Poor's, RatingsDirect® Global Credit Portal, *www.standardandpoors.com/ratingsdirect,* 7 May 2008