Global Information Assurance Certification Paper

Mark A. McMichael

Risk Analysis

In an age where large amounts of data are transferred via electronic means on a daily basis, millions, if not billions, of dollars in business transactions take place across the Internet and other various network connections, information has become its own commodity. As a bank protects its cash assets by moving them around in armored cars with trained security guards and precise routine, such is the nature of protecting information. Securing information involves a wide array of planning, action and implementation to protect the confidentiality, integrity and availability of sensitive information. As is the nature of any project or operation, *planning* is the key to accomplishment. When planning information security practices or implementing set security standards into a project, careful analysis of the threat or potential threats that will be faced is paramount. This facet is handled through **Risk Analysis**.

Information Security is now considered a business issue. Security reviews are often pivotal factors to determining budget parameters for IT-related projects. Risk analysis comes into play to provide cost justification for the potential threats to which an organization may be exposed. C&A Systems Security Ltd. cites that [Risk Analysis] is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. For a business providing a service or product dealing with little or no sensitive data, it doesn't make sense to allocate the time and money necessary to implement a system of "air-tight" security. Such overhead could take away from or eliminate any forecasted profit. Conversely, a financial institution conducting millions of dollars in Internet-based transactions on a daily basis would want to make a serious investment towards securing account data, credit information and the actual transactions taking place. This also holds true for Internet-based businesses that want to ensure privacy and protection for the customers who utilize their service. **Risk Analysis** determines the level of security necessary to maintain the bedrock principles of *confidentiality*, *integrity* and *availability* as they pertain to protecting information and data.

Risk Management

Risk analysis is defined as a means of:

1. Providing decision-makers with information needed to understand factors that can negatively affect operations and their results.

AND

2. Making informed judgements concerning the extent of actions needed to reduce risk.

To appropriately effect a comprehensive risk analysis, various levels of risk management must be employed. Critical success factors involve obtaining senior management support and involvement and designating focal points (groups or individuals) tasked to oversee and guide the risk assessment process. Senior management involvement is necessary to ensure that the analysis is taken seriously at an organization's lower levels, that resources

are available to implement the program, and that the findings of the assessment are given due consideration with appropriate actions being taken. The designated "focal points" facilitate the planning, performance and reporting of the risk analysis.

Planning

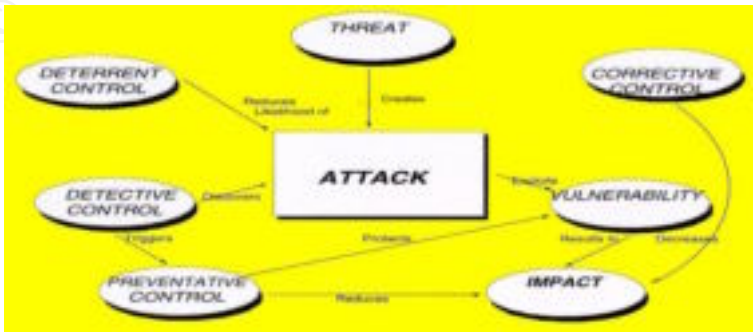
The first step to risk assessment is developing the execution plan. This should cover the objectives and methodology, the team size and compilation, and the information requirements necessary to conduct the analysis. Here, the assessment coordinator works with the management of the business unit to outline the steps by which the analysis operation will commence. "Risk Analysis should not only direct appropriate information at both department management and IT staff, but play a major and pro-active role in enhancing the understanding of each, of the needs and role of the other." (C&A Systems Security) Once the guidelines are in place and the necessities are communicated to the proper areas, the team is assembled and inquiries are determined.

Considerations must be made for all aspects of a project including present security policies, user data, ID's and passwords, electronic mail, Internet access and utilization, encryption utilization, firewall parameters, remote access, control usage (i.e. Active X and Java) and even vendor support requirements—to name a few.

Performance

During this phase, the assessment team will collect and analyze data on threats and vulnerabilities and recommend corrective actions. Research, gathering and analyzing data, discussions with key personnel (vendors, developers, administrators) are essential actions to be mitigated by focal points. Business analysts may be employed to illuminate various aspects of the impact security measures may have upon performance and functionality.

In a paper on the security assessment practices of leading organizations, the U.S. General Accounting Office cites the use of a specialized group that collects threat data from not only internal sources, but also from external sources including federal intelligence agencies and emergency response centers. This ensures that all credible threats are considered and allows for the development of a "baseline threat statement" to provide a comprehensive statement regarding the most potential and available threats conducive to the organization's operations. From this, often times, an organization can design a threat model or diagram to lend some illustration to the scope of its assessment. One such relational model is shown here:



Reporting

The final phase of the risk analysis is reporting the findings and ensuring that agreed-upon actions are taken. Once the vulnerabilities and risks are determined, the risk assessment team develops and recommends corrective actions. Upon final approval, these steps are given to the business unit for implementation. Many times, alternative solutions may be provided to assist in mobility and functionality.

Before going into production, a final assessment of the implementations should be conducted to ensure compliance with the Risk Analysis. Once complete, periodic updates and verification should be conducted to maintain optimum security.

Sources:

Bagwill, Robert and Barbara Guttman. NIST Special Publication 800-XX. "Internet Security Policy: A Technical Guide." #3 Risk Profiling.
URL: http://csrc.nist.gov/isptg/html/ISPTG-3.html (July 1997)

C&A Systems Security, Ltd. "Introduction to Risk Analysis"
URL: http://www.securitypolicy.co.uk/riskanalysis/introduction.htm (2000)

C&A Systems Security, Ltd. "The Benefits of Risk Analysis"
URL: http://www.pcorp.u-net.com/riskben.htm

GAO: United States General Accounting Office. "Information Security Risk Assessment: Practices of Leading Organizations"
URL: http://www.securitymanagement.com/library/GAOAIMD99139.txt (Aug. 1999)

Parker, Donn B. Fighting Computer Crime. (pp. 261-267) Wiley Computer Publishing. New York: 1998.