Information System Security: How Much Is Enough?
Lawrence Troffer
August 21, 2000

Two generally accepted notions of information system security are that it is expensive, and that a system's usefulness is inversely proportional to its degree of security. Senior policy- and decision-makers face a daunting challenge in determining "how much security". Adding layer after layer of security measures can become unaffordable, in terms of direct and indirect costs and diminishing utility of the information system. Further, a haphazard application of security measures may leave critical vulnerabilities exposed, or result in unnecessary protection being applied.

In the development of systems of any type, good systems engineering practice calls for a thorough requirement analysis and a process to trace requirements throughout system development in order to ensure that the final product meets the original need. In the field of information system security, the equivalent of the requirement analysis is a risk assessment. When established in policy as a specified methodology tailored to an organization's needs, it serves multiple purposes. It can be a disciplined, repeatable process for identifying security needs. It forms a basis for subsequent security review during the lifecycle of an information system. It can aid management in making decisions on expenditures, and also assist the security professional by presenting sound justification to management for particular measures. The ideal outcome obviously, would be to implement sufficient security, yet no more security than is affordable and whose cost is properly justified.

The Department of Defense and the armed services within it have established extensive policies regarding information system security. A part of those policies is the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), a deliberate process that leads to an appropriate level of security certification and finally accreditation by a Designated Approving Authority (DAA). The final accreditation is a part of the "building permit" required prior to installation or modification of an information system. The DITSCAP applies to all information systems, whether classified or unclassified, and is tailored to each system according to the sensitivity of the information it processes.

When security measures are applied to a system, there is always some remaining, or residual, risk. For example, although a well-designed firewall provides significant protection to a network, there is still risk of insider attacks or data-driven attacks being introduced via legitimate access protocols. Accreditation by the DAA implies that the DAA has reviewed the system's security posture, and deems any residual risk as acceptable. The DITSCAP prescribes a Risk Assessment as the basis for identifying appropriate and effective security measures and for aiding the DAA in determining the residual risk. Specific risk assessment methodologies are numerous and almost always tailored to the system under consideration. The remainder of this paper discusses one approach.

Risk Assessment 101.

The elements of a good risk assessment include:

Business or operational assessment
Asset valuation
Threat assessment
Vulnerability assessment
Risk analysis
Countermeasure assessment and implementation
Test

The business or operational assessment is done to gain an understanding of the people, systems and processes of an organization, and an estimate of the external environment in which they operate. It provides necessary context for the remainder of the risk assessment. It provides insight that will be needed later in the process for making decisions.

The asset valuation consists of identifying assets and assigning each a value. The effort requires some thought, because the term, "asset", means more than physical items like computers or network infrastructure. Intellectual property, proprietary information and professional reputation are less tangible, but are assets nonetheless, and are vulnerable to various security problems. Also, an organization's assets may have value to others outside the organization, which should perhaps be considered in this process. The analysis may be quantitative or qualitative or both. For example, real property has a clear monetary cost associated. The value of professional reputation is much harder to quantify. However, in order to make subsequent decisions on the basis of cost-benefit tradeoffs, some kind of cost or weight that indicates the consequences of losing each asset is required.

For purposes of the risk assessment, threats are defined as events or circumstances that can harm a system. In the threat assessment, all possible threats are first identified. Then the likelihood of each threat is estimated. To be thorough, the threat identification should include anything that can compromise the confidentiality, integrity or availability of a system. That means that fire, theft, natural disaster and others need to be considered alongside viruses, network penetration and denial of service attacks. The likelihood of some threats may be estimated through historical data, while that of others will be based on experience and judgement. The threat likelihood is expressed as a probability between 0 and 1.

The vulnerability assessment is the deliberate examination of the system to determine its weaknesses. Vulnerabilities are deficiencies in design, controls, procedures etc. that can be exploited. The vulnerability assessment considers existing security countermeasures, and is used to determine which threats are carried forward to the next step of the risk assessment. There is clearly no need to consider implementing countermeasures for a threat against which a system is deemed not vulnerable. It is important however to initially list all threats and vulnerabilities for purposes of future review. Sources for identifying potential vulnerabilities include:

- Previous vulnerability test and audit reports
- Interviews with system management, operations, and maintenance personnel
- Vendor advisory information
- Computer Incident Response Team (CIRT) bulletins
- System software security analyses
- System anomaly reports
- Experience on similar systems
- Security incident reports.

Checklist driven, non-technical means (observation, demonstration, interview, and document analysis) are used to provide information pertinent to the physical, personnel, administrative, procedural, and operations security factors of the vulnerability assessment. Technical tools such as network security tools, password crackers and war dialers may be employed in internal or external attack modes to determine the level of access that a valid user or intruder could obtain.

Risk is the combination of the probability of a threat, and the resulting impact on assets. The risk analysis is the process of analyzing the threat probabilities and resultant consequences from the previous steps of the risk assessment. It considers which assets are vulnerable to which threats, and to what degree. It is intended to highlight the difference between low-value assets vulnerable to low-probability threats versus high-value assets vulnerable to high-probability threats, and all combinations in between. A simple method: first estimate which assets are vulnerable to which threats. Multiply the threat probabilities times the values of the assets each threat may effect. This provides a "weight" that is a measure of risk.

The countermeasure assessment identifies countermeasures that may be required and strikes a balance between risk identified in the previous step and the cost of implementing specific countermeasures to reduce it. Further, this assessment should help determine the sequence in which countermeasures will be implemented should time or money preclude simultaneous implementation. It is certainly conceivable that the risk analysis and countermeasure assessment will show that no additional countermeasures are needed.

Finally, a test is conducted to validate the work. The validation testing may repeat some of the activity of the vulnerability assessment, but is in no way limited to that. The interest is in being thorough, in order to determine risk remaining after application of selected countermeasures.

A thoroughly documented risk assessment requires considerable time and effort, but is well worth the expense on all but the most trivial networks and systems. It provides facts, rather than guesses, regarding specific security measures to be implemented for a given system. It provides a complete picture and a common understanding to both top level management and the security practitioner and enables sound decisions regarding cost, system utility and adequate security.

References.

1. “An Introduction to Computer Security: The NIST Handbook”. July 2, 1996. http://csrc.ncsl.nist.gov/nistpubs/800-12 (23 June 2000).
2. “Defense Information Technology Security Certification and Accreditation Process”. December 30, 1997. http://web7.whs.osd.mil/text/i520040p.txt (26 June 2000)
3. “Introduction to Certification and Accreditation Concepts”. January 1994. http://www.radium.ncsc.mil/pep/library/rainbow/ncsc-tg-029.txt (27 June 2000).