Risk Assessment in the University Setting

Kent Knudsen
March 2, 2001

INTRODUCTION

The goal of an information security program is to protect the confidentiality, integrity, and availability of information. One essential component of the information security program is the management of risk through a process called risk assessment. The areas of risk assessment and risk management tend to be misunderstood as well as difficult to implement in a decentralized university setting.

> "Current approaches to information-security risk management tend to be incomplete. They fail to include all components of risk (assets, threats, and vulnerabilities). [*Often*] the organization has insufficient data to fully match a protection strategy to its security risks.
>
> In addition, many organizations outsource information security risk evaluations, which can have drawbacks. An organization has no way to know if the risk assessment is adequate for their enterprise. It is also impossible for an external expert to assume the perspectives of the organization. Self-directed assessments provide the context to understand the risks and to make informed decisions and tradeoffs when developing a protection strategy."[1]

The risk assessment process is further complicated by the fact that there are so many ways to identify and analyze risks. There are several methodologies for conducting a risk assessment, and not all information security professionals agree on which method is the best. In the university setting, there is little real understanding of the process of analyzing risks and/or wide variance in the methodology chosen by the various university entities.

All risk assessment methodologies attempt to effectively calculate (quantitatively or qualitatively) the chance of experiencing an adverse event as well as the magnitude of the event's impact. In order to accomplish this, one must be aware of and understand the elements of risk and their relationship to each other. This, in a nutshell, is the process of risk analysis and assessment.[2]

For the university setting, the landscape for conducting a risk assessment is considerably more complex. Unlike a business setting where standards are set for the information systems, a university is often structured like the Internet itself - a collection of LANs and WANs that consist of numerous computing platforms and network topologies. Each department or college has their own information technology staff (or worse, no staff) which determine the "lay of the LAN". Therefore, it is difficult to perform a single risk assessment for the entire university as a whole. For the campus with decentralized information security, this presents a significant challenge.

One of the first significant hurdles is deciding on which methodology to use for assessing risk. From 1979 to the present, there persist two major types of risk assessment methodologies - qualitative and quantitative.

QUALITATIVE VS. QUANTITATIVE

"The earliest efforts to develop an information risk assessment methodology were reflected originally in the National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) FIPSPUB-31 Automated Data Processing Physical Security and Risk Management, published in 1974. That idea was subsequently articulated in detail with the publication of FIPSPUB-65 Guidelines for Automated Data Processing Risk Assessment, published in August of 1979... As a consequence, while some developers launched and continued efforts to develop credible and efficient automated quantitative risk assessment tools, others developed more expedient qualitative approaches that did not require independently objective metrics -- and OMB A-130, an update to OMB A-71, was released, lifting the 'qualitative' requirement for risk assessment in the federal government."[3]

The following table lists the pros and cons of both approaches (adapted from the "Information Security Management Handbook")[4]:

Method	Pros	Cons
Quantitative	- The assessment and results are based on independently objective processes (meaningful statistical	- Calculations are complex (management may mistrust the results of "black box"
Qualitative	- Calculations, if any, are simple and readily understood and executed.	- The risk assessment and results are essentially subjective in process.

	significant areas of risk that should be addressed is provided.	subjective).

Regardless of which methodology or approach you choose (qualitative or quantitative), the risk management process flow is fairly generic:[5]

1. **Define the scope, boundary, and methodology**
    - The boundary may include the LAN as a whole or parts of the LAN, such as the data communications function, the server function, the applications, etc.
    - The scope distinguishes the different areas of the LAN (within the boundary) and the different levels of detail used during the risk management process.
    - The methodology should be defined as qualitative or quantitative.
2. **Identify and value assets**
    - Asset valuation identifies and assigns value to the assets of the LAN.
    - The risk assessment methodology should define the representation of the asset values.
3. **Identify threats and determine likelihood of occurrence**
    - Threats and vulnerabilities need to be identified and the likelihood that a threat will occur needs to be determined.
    - As specific threats and related vulnerabilities are identified, a likelihood measure needs to be associated with the threat/vulnerability pair (i.e. What is the likelihood that a threat will be realized, given that the vulnerability is exploited?)
4. **Measure risk**
    - The risk measure could be defined in qualitative terms, quantitative terms, one dimensional, multidimensional, or some combination of these.
        - One dimensional approach (risk = magnitude of loss X frequency of loss).
        - Two dimensional approach (risk = threat X magnitude of loss X frequency of loss).
5. **Select appropriate safeguards**
    - Selecting appropriate safeguards is a subjective process. When considering the cost measure of the safeguard mechanism, it is important that the cost of the safeguard be related to the risk measure to determine if the safeguard will be cost-effective.
6. **Implement and test safeguards**
    - The goal of this process is to ensure that the safeguards are implemented correctly, are compatible with other LAN functionalities and safeguards, and provide expected protection.
    - Each safeguard should first be tested independently of other safeguards to ensure that it provides the expected protection.
7. **Accept residual risk**
    - After all safeguards are implemented, tested and found acceptable, the resulting risk level should be reexamined. The risk associated with the threat/vulnerability relationships should now be reduced to an acceptable level or eliminated. If this is not the case, then the decisions made in the previous steps should be reconsidered to determine what the proper protections should be.

Step 4 above sounds so deceptively simple. The equations are easy enough to understand, but the real challenge lies in producing meaningful quantities for the equation variables. It is this aspect of risk assessment, which requires experience and knowledge that most IT personnel will require years to acquire proficiency and credibility. John Johnson points out the fundamental difficulty of risk assessment in the following quote:

> "Determine the probability that a potential threat will even exploit any vulnerability to define the level of risk. Assign a priority or other measurement to this risk factor. The method used to evaluate this information could result in a subjective instead of objective assessment. The more objective an assessment, the more realistic your determination will be, yet measuring risk is not an exact science."[6]

One solution is to purchase an automated product with the threats, vulnerabilities, and countermeasures already pre- configured. In this way the "experts" have already built into the product their experience and knowledge. This is a tempting solution until you find yourself trying to explain to management exactly how the "black box" produced the results, and why the results can be trusted. Also, add to that fact that most automated software packages providing this "built-in experience" come at a significant cost - not such a good solution when the licensing requires each and every departmental entity to acquire their own copy.

SUMMARY

For the decentralized security environment (typically found at large universities), the challenge is to provide a risk assessment methodology that will be platform independent, and allow for the results to be combined for an overall risk assessment viewpoint. One possible solution is to create a web based risk assessment tool that focuses on security from a LAN and/or desktop perspective. The advantages that such a web based tool would provide are:

- It could require the various departmental entities to store their risk assessment results in a collective database. The database of individual risk assessments could then be used to derive the overall risk assessment.
- Security policy compliance could be measured by asking if specific aspects of the security policy are being adhered to, or are in place.
- The web based tool could also serve as an awareness tool for the security policy.
- And finally, the risk database will provide a method to contact individual departments when there is a virus or other malicious attack which affects their systems. For example, you could query the database for all departments which have Microsoft Windows systems and send them a notice about a new virus or vulnerability.

Each university must make a determination as to which risk assessment methodology suits their operational and environmental constraints. For the decentralized university setting, a risk assessment which is LAN-centric could be used to assess risk for each departmental entity. In this manner, the process could be "standardized" and allow the university to compile a composite risk assessment. A web based risk assessment methodology would overcome any platform specific issues, and allow the results to be collected into a single database for building the composite risk assessment.

RESOURCES

1. Fred Cohen and others have authored a paper ("A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses") which lists 94 attacks, 37 threats, and 140 defenses.
2. The Department of Health and Human Services has published "Guide to Protecting LANs and WANs" which details various aspects to include in a risk assessment for LANs and WANs.
3. LEGAL CONSIDERATIONS (USA) for risk analysis[7]:

   In the U.S. the following laws should be considered during a risk analysis. There are probably additional relevant laws (e.g. in different states, or concerning civil liability) not listed here.

   - Accreditation Manual for Hospitals
   - Banking Circular 177 from the Office on the Controller of the Currency
   - Bulletin R-67 from the Federal Home Loan Bank
   - Clinical Laboratory Information Act
   - Computer Fraud and Abuse Act, 1986 (USC 1030)
   - Computer Security Act, 1987 (Public Law 100-235)
   - Copyright Violation (USC 506b, title 17)

- Electronic Funds Transfer (USC 1693n, title 15)
- Electronic Privacy Act, 1986 (USC 2701)
- Emergency Planning and Community Right-to-know Act, 1986 (3USC 300)
- Fair Credit Reporting Act
- Federal Procurement Regulations
- Foreign Corrupt Practices Act, 1977
- Letter #161 from the National Credit Union Association
- Letter A-130 from the Office of Management and Budget (OMB)
- Privacy Act, 1974 (5USC 552a)
- Wire Fraud (USC 1341, title 18)

REFERENCES:

1. Alberts, Christopher and Dorofee, Audrey. "An Introduction to the OCTAVE Method". 30 Jan. 2001.
URL: http://www.cert.org/octave/methodintro.html. [24 Feb. 2001].

2. Tipton, Harold F. and Krause, Micki. "Information Security Management Handbook". Dec., 1999.
URL: http://secinf.net/info/misc/handbook/223-228.html [24 Feb. 2001].

3. Tipton, Harold F. and Krause, Micki. "Information Security Management Handbook". Dec., 1999.
URL: http://secinf.net/info/misc/handbook/239-242.html [24 Feb. 2001].

4. Tipton, Harold F. and Krause, Micki. "Information Security Management Handbook". Dec., 1999.
URL: http://secinf.net/info/misc/handbook/242-244.html [24 Feb. 2001].

5. National Institute of Standards and Technology, "Guideline For The Analysis Of Local Area Network Security [FIPSPUB 191]", 9 Nov. 1994,
URL: http://www.itl.nist.gov/fipspubs/fip191.htm [24 Feb. 2001].

6. Johnson, John D. "Conducting Risk Analysis to Evaluate Enterprise Security". 5 Nov. 1999.
URL: http://securityportal.com/topnews/conduct-risk.html [24 Feb. 2001].

7. Boran, Sean. "IT Security Cookbook". 24 Oct. 1999.
URL: http://secinf.net/info/misc/boran/misc.html#Heading5 [24 Feb. 2001].