Global Information Assurance Certification Paper

Information Systems Risk Analysis, Assessment and Management

By Allan L. Micksch
13 September, 2000

First here is an explanation of terminology used in the title. *Risk analysis* is the process of discovering, to the fullest extent possible, all information systems assets and the level of any threats (however slight) to which they may be vulnerable.

To generate a *risk assessment*, the results of the risk analysis are evaluated in conjunction with the criticality of each asset to determine a level of concern for each asset-risk combination.

Using the results of the risk assessment for making decisions about allocating resources and/or implementing programs to alleviate or reduce the risks and maintain a low-risk environment in the most cost-effective manner is *risk management*.

In any organization; corporate, academic, non-profit; large or small, the battle for funding is paramount. Information security requirements are going to be weighed and compared with all the others. While general awareness of security issues is on the rise due to recent events, it is still necessary to convince "Mr. Pocketbook" that your assets are vulnerable and need protection.

A proper risk assessment is a very good tool for scooping out your share of budget. There are two problems.

Problem one is the cost of the risk assessment itself. Even when done in-house this can tie up a fair amount of time and other resources but it is important to know the risks and what they can cost your organization.

The second problem is what may happen while waiting for the risk assessment results. The experts agree that security measures should be implemented without delay. Standing by for the results of a risk assessment could be disastrous. It is probably true that most organizations have put in place a number of security controls without having done a risk assessment.

Resources to assist in conducting risk analysis/ assessment/management are available but searching on the Internet mostly returns references to services, software and books. Information is scarce. The subject area is large and even to present just an overview in a short paper may prove difficult but it appears to be needed.

The first step is to perform the analysis. Identify all your assets and any hazards that comes to mind. Several people in a brainstorming session can be helpful.

Include everything, no matter how trivial or ridiculous; a hurricane in Omaha, a typo by an executive secretary, time bombs installed in your equipment by the manufacturer. Your assets include the obvious hardware, software, data and documentation, as well as people, supplies and facilities.

Consider the chance and severity of each threat against each asset. Determine what effect each would have; would it destroy the asset, reduce the effectiveness, or have no effect.

Next, generate the risk assessment. For each risk-threat scenario assign a severity rating (often a monetary value of the expected loss on an annual basis). You should consider how critical the asset is to your organization, how long it will take to recover, and what you will do until you have recovered.

One major problem here is being consistent in the method of evaluation, especially if different people review different scenarios. The value of the loss and the cost of recovery must be based on the same foundation for each scenario.

In the risk management step, every possible method of prevention and/or recovery should be evaluated and the cost of implementation compared to the loss determined by the risk assessment. Sometimes the more cost-effective method is to let the problem occur and fix it afterwards.

Risk analysis/assessment/management is a continual process even if your assets and threats don't change. As new methods of prevention and/or recovery become available

or their costs change, the scenarios must be re-evaluated. Fortunately this should be easier the second time around.

When new assets are acquired or new threats become known, they must be added to process. These will usually fall neatly into place with previous entries or be similar enough to allow easy integration.

Even if your system has no changes the full process; analysis, assessment, and management; should be reviewed often.

This paper has attempted to provide a brief overview of the risk analysis/assessment/management process. For more detailed information, please check the references listed at the end.

To help you get started here is a list of some assets you may want to protect.

HARDWARE:
Circuit cards, external tape and disk drives, routers/switches, cords/cables, converters/adapters, UPS's, test equipment, tools, spare parts.

SOFTWARE:
Source and object, locally written and purchased, O/S, utilities, diagnostics, communication programs, backups, documentation.

DATA:
Online, offline (archived), log files, databases, in transit (on comm. lines).

PEOPLE:
Users, programmers, administrators, electronic maintenance (computers, comm. Lines), facilities maintenance (movers, janitors, electricians), operators, managers, delivery, vendors, consultants, tours.

DOCUMENTS:
Software/hardware manuals/procedures, licenses/contracts, physical and online access control lists, training materials.

SUPPLIES:
Magnetic media, forms, printer ribbons, paper, toner, cleaning materials, static bags.

OTHER:
Buildings, furniture/furnishings, power panels, water, air conditioning, vehicles.

Every one of the listed items can be exploited in some way. The threats are real though sometimes minimal. Your job is to analyze, assess, and manage your risks in the most economical way. Do you spend money on recovery or prevention?

It's not a win/lose situation: it's what it's going to cost, one way or another.

References:

Boran, Sean. "Combining Organizational, Physical & IT Security." "An Overview of Corporate Information Security." 13 Dec. 1999. URL: http://securityportal.com/cover/coverstory19991213.html (11 Sep. 2000).

C & A Systems Security Ltd. "The Benefits of Risk Analysis." 1999. URL: http://www.pcorp.u-net.com/riskben.htm (11 Sep. 2000).

C & A Systems Security Ltd. "THE NEW ERA IN SECURITY RISK MANAGEMENT." 1999. URL: http://www.pcorp.u-net.com/risk.htm (11 Sep. 2000).

Cohen, Fred. "Risk Management or Risk Analysis?" "Managing Network Security." 1997. URL: http://www.all.net/journal/netsec/9703.html (11 Sep. 2000).

Hurwitz Group, Inc. "Risk Management: The New IT Challenge - BindView." Mar. 2000. URL: http://www.bindview.com/hurwitz_wp (11 Sep. 2000).

Information Systems Security Organization. "INFOSEC Assessment Methodology." 24 Jul. 2000. URL: http://www.nsa.gov/isso/iam/index.htm (11 Sep. 2000).

"INTRODUCTION TO RISK ANALYSIS". URL: http://www.riskserver.co.uk/introduction.htm (11 Sep. 2000).

Johnson, John D. "Conducting Risk Analysis to Evaluate Enterprise Security." 5 Nov. 1999. URL: http://securityportal.com/topnews/conduct-risk.html (11 Sep. 2000).

The SANS Institute. "Essential Security Actions: Step By Step." 1999. URL: http://www.sans.org/newlook/resources/esa.htm (11 Sep. 2000).