

A Practical Approach to Security Risk Management

By Frank Wickham

Improper Risk Management can cause damage to an organization's reputation, cause direct or indirect financial loss, and lead to poor employee morale.

Risk Management (RM) is the reduction or removal of a risk as it relates to information systems security, sometimes referred to as risk mitigation. This paper will discuss risk as it is related to an organization's information systems, and the numerous negative implications that it can cause. Improper RM can cause damage to an organization's reputation, cause direct or indirect financial loss, i.e., direct financial loss to stock price if public, and indirect financial loss through fines or insurance coverage increases, and lead to poor employee morale.

RM will be defined as the systematic identification, analysis, control, and reduction of a loss of information or service that is associated with a specific event.

There are three primary areas we are concerned with as they affect information systems. They are availability, data integrity, and data confidentiality. Each has its own risk characteristics. Each organization has its own perception of how it is affected by each of these areas. Some of these risks include how much time and money could potentially be lost due to a loss of service and how much damage to the organization's reputation was inflicted due to a disclosure of employee or customer personal information. The possibility also exists of corporate officers such as the CEO or CIO going to prison for not protecting data assets properly.

RM looks to limit exposure in the following general areas:

- **Loss of availability** – The quality of access to an information service, such as the loss of a service or facility which is critical to the operations of an entire organization. A partial loss or delay of service could also be catastrophic in some cases.
- **Loss of data integrity** – Occurs when data has been modified and is no longer consistent. For example, employee data that is lost or damaged, cannot be

reproduced at a reasonable cost, is unreliable or has been rendered useless.

- **Loss of confidentiality** - The disclosure of data which was intended to be private. The release of information that could be damaging to the organization, its employees, customers, or general public if it were made public. Examples of this would be the release of credit card or social security information or the distribution of company or product specifics such as a recipes.

All of the above threats can be directly equated to damage to an organization's image or financial loss.¹

Risk management terms defined

A list of commonly used RM terms has been developed over the years and defined below.

Asset	A resource, something of value.
Asset Value (AV)	Monetary value to replace the asset or value due to loss of use.
Threat	Potential event or activity that causes an undesirable outcome.
Vulnerability	Susceptibility to a threat.
Safeguard	Method of preventing a possible threat.
Exposure Factors (EF)	Percentage of loss a threat event would have on a specific asset.
Single Loss Expectancy (SLE)	Monetary amount that is assigned to a single loss event.
AV x EF = SLE	
Annualized Rate of Occurrence (ARO)	Number of times a loss event occurs per year.
Annualized Loss Expectancy (ALE)	Annual monetary loss. SLE x ARO = ALE

¹ Ronald L. Krutz and Russell Dean Vines, *The CISSP Guide*, Second Edition, 2004.

Real world example

Let's use an example to show our knowledge of the formulas just defined. I am a T-shirt distributor. I take a raw material, in this case T-shirts, and put whatever someone wants to put on them. My entire business is based on orders of 20 or more T-shirts sold over the Internet or via phone calls. The average cost of a T-shirt is \$15.00. My annual sales revenue is \$750,000.00 or \$3,000.00 a day. I lost my 4000 entry customer database. For some, yet unknown, reason the data became corrupt. It was first noticed by someone entering an order for an existing customer. They reported the customer record contained corrupt address data and the phone numbers were displayed as symbols. Checking other entries, damage was found to be wide spread. The most recent backups were off site and their IT staff of one was not immediately available.

- The restoration took three full business days
- The average work year is based on 250 days
- So if we say this may happen once every three years, $ARO = 1/3$
- My average daily revenue is \$3,000.00 per day, $AV = \$3,000.00$
- My entire order operation was down so $EF = 100\%$
- My value for the three days of lost revenue was \$9,000.00, $AV \times EF = SLE = \$9,000.00$
- My Annualized Loss Expectancy (ALE) is $SLE \times ARO = ALE = \$3,000.00$

This loss was only 1.2 % of my annual sales revenue. The ALE for a loss of this type, which may only occur once every three years, is \$3,000.00 or .4 % of my annual revenue. In addition to direct loss of revenue, the company faced the loss of customers for good reason due to the organizations inability to fulfill orders. This is a minor loss as compared to the case of their entire office and warehouse space becoming unusable, for say a month, due to damage from a tropical storm. In the case of the tropical storm, just the loss of revenue approaches 10% of their sales, not to mention potentially lost inventory or repair of the damaged structures.

Risk Analysis

Let us compare quantitative and qualitative risk analysis. The definitions help us better understand their meanings and how they fit with risk analysis.

- **Quantitative** – An analysis expressed as a numeric value for measurement purposes which was the result of mathematical models or scientific methods. It may employ probability and statistical tools. In this case the possible units might be U.S. dollars or time in minutes/seconds.
- **Qualitative** – Expressing the result as a quality. An intuitive analysis based more on human feelings, behavior, and perception. The result is based on an intangible item rather than actual numbers.

When the definition is applied to quantitative risk analysis it would indicate the analysis is based on hard numeric values. When all elements (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability) are measured, rated, and assigned values, the process is considered fully quantitative.²

In the real world almost no organization will conduct a straight quantitative risk analysis of part or entire environment due to the extensive time and financial cost it would incur. In many cases the same findings and recommended controls would be the result without the exhaustive analysis.

Qualitative risk analysis deals with the softer more intangible factors other than costs of a risk. These are things like reputation and corporate image. These items are subjective, intangible and harder to apply a value to them.

Conducting an analysis

Analysis tools

Some of the tools that are used to conduct a risk analysis include:

- **Questionnaires** – a list of questions to determine the current or future management and operational controls in place in an organization.
- **Interviews** – An onsite visit to the staff for follow up questions from the information received from the questionnaire. Gather firsthand the physical, environmental, and operational security controls in place in an organization.
- **Document review** – Any documentation pertaining to the organization under review should be collected and studied as part of the analysis, such as security policy, organizational policy, system configurations, run books, listing of software packages in use, and reports from previous security related activities.
- **Automated scanning tools** – The use of tools to retrieve information about computer networks, including what is connected to them.
- **Automated risk analysis products** – automated tools which may be used to calculate risk which are not specific to an analysis of information systems.³

Identification of assets and value determination of resources

One of the more difficult and tedious tasks of performing risk analysis is the identification of all an organization's assets and attaching a value to them if they are lost, corrupted or delayed. Keep in mind that an organization that experiences a partial loss would apply a percentage-based value to its resources lost. When analyzing information systems we

² *ibid.*

³ Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology's (NIST) publication, Special Publication 800-30.

think of network connectivity and data services. If we look at it from the business side, those very items become our customer contact lists, databases and tools necessary for the organization to produce positive revenue.

Specific threats and vulnerabilities

Threats fall into three categories: malicious threats, unintentional threats, and physical threats, many of which could severely affect or interrupt information systems.⁴

Malicious Threats	Unintentional Threats	Physical Threats
Malicious Software	Equipment Malfunction	Fire Damage
Spoofing	Software Malfunction	Water Damage
Scanning	Human Error	Natural Disaster
Snooping/Scavenging	User/Operator Error	Power Loss
Tunneling	Trap Door	Civil Disorder/Vandalism
Spamming	Back Door	Battle Damage

Risk evaluation

The three components a security practitioner would use when evaluating risk are the likelihood of a threat, the magnitude of a threat, and the level of risk an organization is willing to take. Each of these may be unique to particular organizations.

Likelihood

Is an adverse event possible? What is the probability of an event happening to your organization? Are they common

⁴ Computer Security Threats, retrieved from <http://www.caci.com/business/ia/threats.html>

events? Is the probability high? Some events are possible and occur once a month. Some events are less common. Each threat will have a subjective likelihood depending on physical location, size of the organization, the business segment, product/services provided, and network connectivity.

Magnitude

How widespread is the adverse event? If it impacts a single employee, it is not as adverse as if it effects 23,000 employees. It may also be compared to a loss of data from a disk that could be restored in an hour affecting one employee. An adverse event may take down an entire storage array related to the organizations financial management systems.

Level of risk

What chance or exposure a given organization is willing to take. The tradeoff between how much a certain protection may cost to how often it will prevent against an adverse event. What would be the cost to recover from the adverse event if the protection or control is not put in place. A gamble with very high stakes.

Risk mitigation and its costs

Selection of safeguards and controls

Most threats have some type of safeguard that can be implemented to protect or eliminate them. A selection of an appropriate safeguard needs to be made. The safeguard may be informational or procedural which typically has a much lower cost. The safeguard may require the purchase of some specialized hardware or software. It then may require specialized knowledge or training to implement. All of these factors need to be studied prior to the selection of the most appropriate safeguard.

Step	Step Title	Description	Output
1	System Characterization	This is where the scope of the risk analysis is defined. How large or small? How is your data classified? Where is your data coming from and where does it go? How is the data used and by whom? This involves an extensive data gathering and documentation effort.	Complete picture of the environment under study with clear boundaries.
2	Threat Identification	An outline of the potential threats, including their source, motivation and typical threat actions that may follow.	Threat statement with threat sources including specific vulnerabilities.
3	Vulnerability Identification	What vulnerabilities exist. Where the threat may come from along with the threat actions defined above.	List of vulnerabilities that could be exercised.
4	Control Analysis	Review of the controls that have or will be implemented into this environment is conducted.	List of controls which are installed or will be implemented.
5	Likelihood Determination	Rating of the likelihood as it relates to the probability that a vulnerability will be exploited.	The likelihood rating assignment of (Low, Medium, High).
6	Impact Analysis	From step 1 a great deal of information was collected and will be used to determine how adverse of an impact a specific loss could be. The prevention of loss of integrity, availability, or confidentiality.	The magnitude of impact assigned (Low, Medium, High).
7	Risk Determination	Development of a risk scale and risk-level matrix to determine the various levels of risk. Based on likelihood, magnitude of impact, and implementation of security controls.	Level of risk assignment (Low, Medium, High).
8	Control Recommendations	During the entire process, security controls will be identified and recommended for implementation. Their selection will include a cost benefit review as detailed above.	Recommendation of controls to mitigate risk.
9	Results Documentation	Management ready report which assists an organization to make educated decisions with respect to mitigating their risk.	Risk assessment report that details threats, vulnerabilities, risk, and recommendations of controls.

Figure 1 – Risk Assessment Steps

Cost-benefit of a safeguard

Once specific threats have been identified they need to be deemed feasible to mitigate from a cost standpoint. What will the cost be to implement? How much will it cost to maintain yearly. Is a subscription service required to keep the safeguard current? As you can imagine some mitigation options will be cost-prohibitive to some organizations to implement.⁵

Operational costs to maintain a safeguard

The best safeguards for protecting against a threat are ones with limited or no manual intervention. Manual intervention by a person or group of individuals means additional staffing costs. When manual intervention is needed to mitigate a threat, it is prone to human error. If automated, it eliminates the human factor which can cause a failure in protection against a threat.

Audit and accountability

Once safeguards are implemented they must be constantly tested and verified that they are still protecting against their target threat. Verification that the threat is and continues to be protected is very important. Auditing of protections and controls needs to take place periodically. Some organizations will audit themselves while others will outsource the task to industry experts.

Accountability is a security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.⁶ In the context of our discussion it applies to prevention and deterrence.

The nine steps of a risk assessment

NIST has developed an extensive process to conduct a risk assessment. The nine-step process attempts to identify, rate, and reduce the risk of specific information systems resources.⁷ See Figure 1 on page 25 and Figure 2 to the right.

Summary

Risk management is key to the protection of an organizations assets and intangible resources. Officers of an organization could be terminated, fined, or sent to jail for failure to apply appropriate controls or protections. It is very important to show due diligence in the protection of an organization’s information assets while at the same time the type and level of threats are ever increasing. No two or-

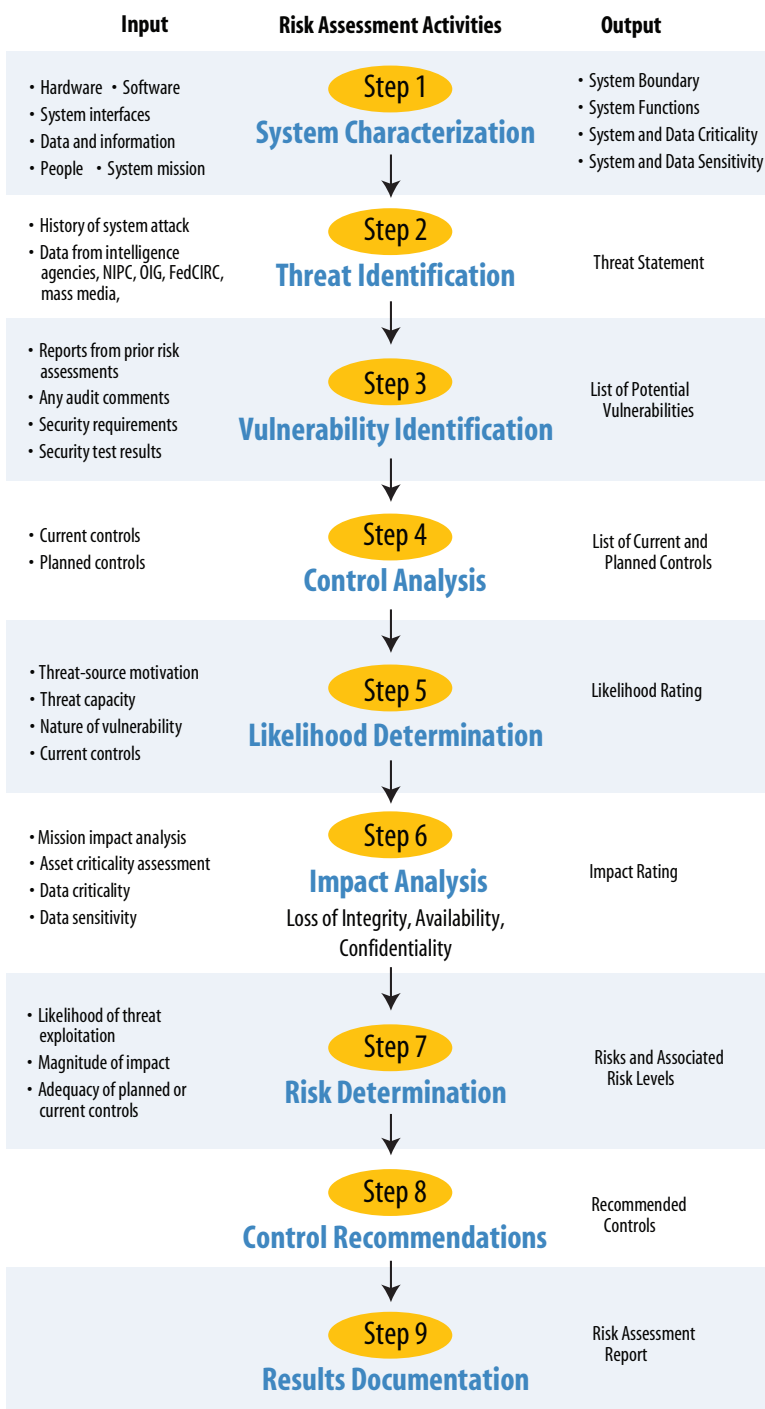


Figure 2 – 9 Steps of Risk Assessment

ganizations will have the same issues as they relate to threats. Each will have to develop a unique model of their own based on whom and what they trust. To mitigate risk, a systematic process similar to the process presented must be applied to be successful.

About the Author

Frank Wickham, CISSP, is a Senior Architect with Sun Microsystems, Inc. He can be reached at fwickham@sun.com.

5 Merike Kaeo, *Designing Network Security*, Second Edition, Cisco Press.

6 Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology’s (NIST) publication, Special Publication 800-30.

7 *ibid.*