Developing An IT Risk Assessment Framework

Mirza B. Murtaza, (E-mail: mmurtaza@mtsu.edu), Middle Tennessee State University

ABSTRACT

In today's business environment, almost all information is captured and stored in electronic form. This digital storage of data in a networked environment provides far greater access to information than ever before. But unfortunately, this also exposes the organization to a variety of new threats that can have impact on the confidentiality, integrity, and availability of information. Organizations need a way to understand their information risks and to create new strategies for addressing those risks. A systematic approach to assessing information security risks and developing an appropriate protection strategy is a major component of an effective information security and risk management program. This paper outlines an Analytic Hierarchy Process based approach for analyzing risk factors and sub factors and ascertaining the major areas of security elements where an organization should focus on.

INTRODUCTION

Information Technology (IT) security has increasingly become an important topic for small and big organizations alike. Awareness of its importance continues to grow as new reports of hackers and even potential for terrorists exploiting technology for their own purposes and motives exists. Several organizations have suffered losses that can no longer be considered a cost of doing daily business. The Computer Security Institute in its annual CSI/FBI survey reported that 56% of respondents experienced a security breach in 2005. Today, virtually all information is captured, stored, and accessed in digital form. From patient records to personnel data, grocery store inventory to national security databases, all types of organizations rely on digital data that is accessible, dependable, and protected from misuse. All types of businesses have established computer networks and web presence in recent years, therefore the need for secure networks is greater than ever before. Several business sectors such as banking and financial institutions, health-care and telecommunication organizations are dependent on the availability of reliable and secure networks. Although awareness and efforts towards security have increased, unfortunately, this increase does not appear to be mitigating the number or cost of incidents from either internal or external sources.

One reason for the problem is that the technology is changing faster than what financially-strapped businesses and information technology (IT) departments can handle. Most organizations are not only increasing the size of their networks but also adding new types of connectivity and complexity. For example, acquisition and implementation of different types of systems because of back-end business process integration with suppliers and other partners and front-end process integration with clients and customers. In some cases, this kind of integration is forced due to mergers and acquisitions. In several instances, market's competitive pressures on hardware and software vendors forces them to implement security features and test products prior to product release in a shortened time span and compromise security. A lot of times security is an after thought and it turns out to be an add-in into existing systems and applications which is difficult, expensive, and, in some cases, impossible without serious operational impact. Even if security mechanisms exist, there is another fundamental problem involving the implementation of controls.

Most organizations do not invest in a thorough risk assessment process before implementing controls. This could result in some threats being overlooked, and also financial and other resources applied wrongly to threats that either do not exist or do not have serious impact (Anderson 1998). Risk is generally defined as a threat or potential

for loss. Risk to some degree is unavoidable but what is needed is an approach to risk that enables organizations to systematically identify information systems risks, prioritize those risks, and take appropriate steps to manage them. Risk assessment is the analysis of the likelihood of loss due to a particular threat against a specific asset in relation to any safeguards to determine vulnerabilities. Assets can be both physical like hardware and virtual like data that has value to an organization.

Risk management can be defined as a "systematic process for the identification, analysis, control and communication of risks" (Paul 2000). Identification and evaluation of threats is a complicated process, it involves the analysis of multiple technologies and how they inter-operate. It also includes the analysis of methods, access, skill levels, and costs required to exploit a given weakness. Unfortunately, threats to information assets are not just the technological weaknesses in the system. They also include potential breaches in physical controls, business and operational processes, telecommunications, and employee awareness programs. The effectiveness of any risk assessment process relies on the accuracy and completeness of the inputs. The results of any risk assessment effort only provide a snapshot of vulnerabilities in a dynamic system. In larger organizations, there are frequent changes in the number and types of systems, telecommunication architecture, and software. Additionally, data, information and physical assets, and business requirements also keep evolving. Therefore, risk assessments must be part of an ongoing process of evaluation of existing vulnerabilities and identifying new ones that crop up frequently. Once actual threats and vulnerabilities are analyzed and understood, security policy and risk management decisions can be implemented.

Risk can be defined using an equation (Lucent 2005): Risk = (Threat * Vulnerabilities) / Controls

In the above equation, threat includes both the likelihood of a threat and the impact (i.e., what assets would be affected). The objective generally of a risk management plan is to bring this risk level to an acceptable level as it is not feasible bring the risk level down to zero.

In a risk assessment process, the individuals within the organization must provide important information to analysts. What the risk evaluation effort suppose to determine includes:

1. What are important information assets?
2. What are potential vulnerabilities or threats to those assets? What are the security requirements of the assets with respect to confidentiality, integrity, and availability?
3. Prioritize the risk or determine the vulnerability of the threat to the asset.
4. What steps the organization should take to protect its information assets, i.e., the protection strategy? Implement the controls or safeguards.
5. Monitoring the effectiveness of those controls or safeguards. (Peltier 2001)

The risk assessment is one element within the broader set of risk management activities. The risk assessment provides a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Risk assessment offers a means of providing decision makers with the information needed to understand factors that can negatively influence operations and outcomes, and make informed judgments concerning the extent of actions needed to mitigate the risk. All risk assessment methods (GAO Report 1999) generally include the following steps:

1. Identifying threats that could harm, and thus, adversely affect critical operations and assets.
2. Estimating the likelihood/probabilities that such threats will materialize based on historical information and/or the judgment of knowledgeable individuals.
3. Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected.
4. Estimating the potential losses or damages including recovery costs.
5. Identifying cost-effective actions to mitigate risk, which include information security policies as well as technical and physical controls.

There are two approaches generally used in risk assessment: a quantitative approach and a qualitative approach. A quantitative approach estimates the monetary costs of risk and risk mitigation techniques based on the likelihood that a damaging event will occur, the costs of potential losses, and the costs of actions that could be taken. When reliable data on likelihood and costs are not available, a qualitative approach can be taken by defining risk in more subjective terms. Table 1 describes the major differences between quantitative and qualitative approaches. It is also possible to use some combination of quantitative and qualitative methods. There are some quantitative risk assessment methodologies available today, e.g., COBRA (Consultative, Objective and Bi-functional Risk Analysis), OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation), and FRAP (Facilitated Risk Assessment Process). Some of these methodologies, like OCTAVE, are publicly available, while others are for the exclusive use of the organizations that developed them.

APPROACHES TO RISK ASSESSMENT

The qualitative risk assessment process is relatively simpler of the two approaches. It is particularly useful for identifying and categorizing physical security problems and other vulnerabilities. A risk assessment team identifies and evaluates the dangers to specific vital assets from catastrophic events, theft, or other threats. A qualitative risk assessment is usually based on a physical survey of locations where data are stored and processed, combined with a review of security procedures already in place. Among items the risk assessment team may consider are geophysical and political factors, reported problems with destruction or loss of records, number and types of employees who have access to records, records handling procedures that may result in damage to or loss of records, physical security, building construction, and access controls in records storage areas, the proximity of records storage areas to laboratories, factories, or other facilities that contain flammable materials or hazardous substances, availability of fire control apparatus and fire department services, and ability to reconstruct recorded information through backup procedures or other methods.

Although the nature and frequency of destructive weather, misfiles, theft of records, or other adverse events are examined and evaluated, qualitative risk assessments do not estimate their statistical probabilities or the financial impact of resulting losses. Instead, consequences and probabilities are evaluated in general terms. Consequences associated with the loss of specific records series, for example, may be categorized as devastating, serious, limited, or negligible. Similarly, the likelihood of significant information loss associated with specific threats may be described as very low, low, medium, high, or very high.

In the project team's assessment, these evaluative designations should be accompanied by definitions or a clarifying narrative. The greatest concern is for vital records with high exposure to threats that have a high probability of occurrence with sudden, unpredictable onset - for example, researchers' notebooks stored in laboratory areas where flammable chemicals are routinely used in scientific experiments, or confidential product specifications and pricing information stored in file cabinets or left on desktops in unsecured office areas.

Quantitative risk assessment, like its qualitative counterpart, relies on location evaluation, discussions, and other methodologies to identify risks, but it uses numeric calculations to estimate the likelihood and impact of losses associated with specific assets. The potential losses are expressed as dollar amounts, which can be related to the cost of proposed protection methods. Compared with qualitative methods, quantitative risk assessment provides a more structured framework for comparing exposures for different assets and prioritizing their protection recommendations.

Although various quantitative assessment techniques have been proposed, almost all are based on the general risk assessment formula. The risk assessment formula measures risk, sometimes called the annualized loss expectancy (ALE), as the probable annual dollar loss associated with a specific assets (Day 2003). The total expected annual loss to an organization is the sum of the expected annualized losses calculated for each asset.

Quantitative risk assessment begins with the determination of probabilities associated with specific events and the calculation of annualized loss multipliers based on those probabilities. The determination of the probabilities is subjective in nature. Knowledgeable individuals familiar with a given asset are asked to estimate the likelihood of

occurrence of specific threats. Whenever possible, their estimates should be based on the historical data regarding adverse events, which can be accurately determined in some cases but only approximated in others. Reliable frequency information is easiest and most conveniently obtained for incidents such as theft, fires, power outages, equipment malfunctions, software failures, network security breaches, and virus attacks for which security reports, maintenance statistics, or other documentation already exists. Once probabilities are estimated, annual loss multipliers can be calculated in any of several ways. Finally, the probability value is multiplied by the estimated cost of the loss if the event occurs. Factors that might be considered when determining costs associated with the loss of assets include, cost of file reconstruction, the value of lost customer orders, lost accounts, or other business losses resulting from the inability to perform specific operations since the needed records are unavailable, and cost of potential legal actions.

AN ANALYTIC APPROACH TO RISK ASSESSMENT

Measuring security level has been a difficult challenge for organizations. Current assessment techniques provide a snapshot of the security situation on a given moment. Once the assessment is performed and corrective steps are taken, there is no evaluation or assessment is done until next scheduled assessment point. This type of approach might leave the organization vulnerable for a while.

The author in this paper suggest the use of analytic hierarchy process (AHP) for assessing risks related to various technology assets in an organization. AHP is one of the commonly used methods for multi attribute decision making. The analytic hierarchy process has been successfully applied to numerous decision areas. The essence of AHP is in permitting the decision-maker to perform pair-wise comparisons of each of the factors or criteria -- one-on-one -- to derive overall priorities. These pair-wise comparisons may be stated verbally as in "Asset/Threat A is equally, moderately more, or strongly more important/significant than Asset/Threat B." The adjectives *likely* or *preferable* may be substituted for *important*. These are converted to numerical values (generally in pre-specified range like 1 to 9) in the traditional AHP approach.

The AHP approach involves four essential steps (Zahedi 1986) that can be summarized as follows:

1. Reduce the decision problem into a hierarchy of interrelated decision elements (factors/criteria and alternatives),
2. collect input data by pair-wise comparisons of decision elements,
3. use the eigenvalue method to estimate the relative weights of decision elements, and
4. aggregate the relative weights of decision elements to arrive at a set of ratings for the decision alternatives.

The AHP process determines the priority any alternative has on the overall goal of the problem of interest. The analyst creates a model of the problem by developing a hierarchical decomposition representation. At the top of the hierarchy is the overall goal or main objective the user or analyst is seeking to achieve. The succeeding lower levels represent the progressive decomposition of the problem. The analyst, or other team members, completes a pair-wise comparison of all elements in each level relative to each of the elements in the next higher level of the hierarchy. The composition of these judgments assesses the relative priority of elements in the lowest level where the final solution lies relative to achieving the top-most objective.

The application of AHP to risk assessment would require first to identify potential threats/categories (Fig. 1) (Myerson 2002). Note that this specific model is not to be used as is by any organization. Specific security models must be established by an organization and they will vary considerably from one organization to another as information security issues for a small retailer would be very different from those of a large national/international organization and would be reflected in the model. Once the model is determined, the following step would be pair-wise comparison and ranking of risks associated with each threat element as determined by an experienced assessment team. Each threat would be compared against each other to establish its relative priority. And each alternative (Table 2) would be compared against each other to determine how well it fares in alleviating the threat. Finally, the application of AHP process would create a prioritization of alternatives. The use of prioritization of factors will assist greatly in the quantification of risk. The difficulty has always been in justifying the protection of

IT assets. Using this approach, the management would be better able to understand the implications of the threat and vulnerabilities when they are quantifiable and measurable.

Since security technologies can fail due to several reasons, security experts recommend using more than one countermeasure against expected threats. This security engineering principle is known as defense-in-depth (Anderson 2001). Using the defense-in-depth model, security technologies can be grouped into protection, detection, and recovery mechanisms (Butler 2002). Almost all security tools fall into one or more categories, a partial listing is provided in Table 2. The major function of a protection mechanism is to prevent the threat from succeeding. On the other hand, detection and recovery mechanisms alleviate threats from an already compromised system. A detection mechanism would identify an attack as it occurs or once it has already occurred. The recovery mechanisms detect potential damage and give IT administrators the ability to restore system integrity as much as possible.

CONCLUSIONS

In today's business environment, almost all information is captured and stored in electronic form. This digital storage of data in a networked environment provides far greater access to information than ever before. But unfortunately, this also exposes the organization to a variety of new threats that can have impact on the confidentiality, integrity, and availability of information. Organizations need a way to understand their information risks and to create new strategies for addressing those risks. A systematic approach to assessing information security risks and developing an appropriate protection strategy is a major component of an effective information security and risk management program. This paper outlines an Analytic Hierarchy Process based approach for analyzing risk factors and sub factors and ascertaining the major areas of security elements where an organization should focus on.

The threat and risk assessment process is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of the infrastructure. The framework discussed in this paper can assist in making a relatively easy process that can be repeated frequently and easily.

REFERENCES

1. Anderson, K. (1998). Intelligence-Based Threat Assessments for Information Networks and Infrastructures: White Paper. Global Technology Research, Inc., March 11, 1998.
2. Anderson, Ross. (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Publishing.
3. Butler, S. A. (2002) Security Attribute Evaluation Method: A Cost-Benefit Approach, Proceedings of the 24th International Conference on Software Engineering, Orlando, Florida.
4. Day, K. (2003). *Inside the Security Mind: Making the Tough Decisions,* Prentice Hall, Upper Saddle River, NJ.
5. GAO Report (1999). Information Security Risk Assessment – Practices of Leading Organizations, Report No. AIMD-99-139.
6. Lucent Technologies, (2005). Risk management is an inherent part of responsible corporate governance. www.lucent.com
7. Myerson, J. M. (2002) Identifying enterprise network vulnerabilities. *Int. J. Network Mgmt*. Vol. 12, 135 – 144
8. Paul, B. (2000). Some Methodologies for Risk Assessment, *Network Computing*.
9. Peltier, T. (2001). *Information Security Risk Analysis*, CRC Press, Boca Raton, FL.
10. Spinellis, D., Kokolakis, S., and Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7/3, 121 - 128.
11. Zahedi, F. (1986) The Analytic Hierarchy Process-A Survey of the Method and its Applications, *Interfaces*, Vol. 16, 96-108.

Table 1: Comparison of Quantitative and Qualitative Approaches to risk assessment

Quantitative Approaches	Qualitative Approaches
Results are based on objective measures	Results are based on subjective measures.
Cost and benefit issues are important	Monetary value of assets is not important.
Requires large amount of historical information like threat frequency, likelihood, etc.	Limited effort is required to develop monetary value, threat frequency
More complex process, mathematical tools are required	Relatively straight forward, mathematical tools are not needed
Mostly performed by technical and security staff	Can be performed by non-technical and non-security staff

Figure 1: Main factors and sub-factors used in risk assessment

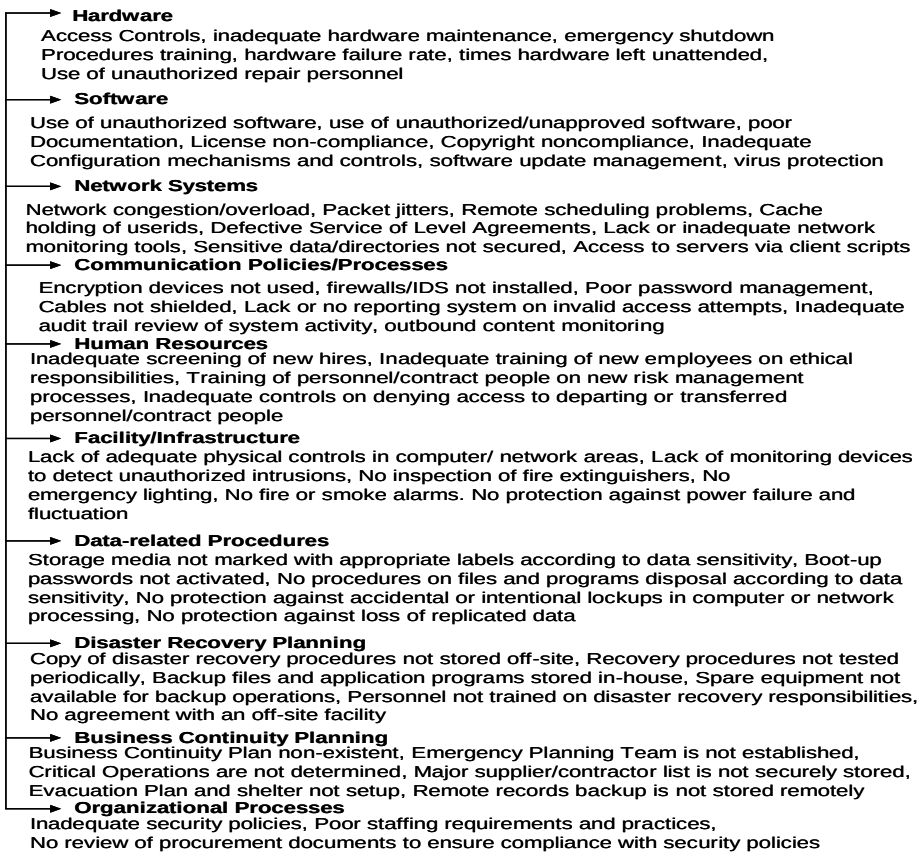

Table 2: Common Security Technologies

Category	Tools
Protection	Packet Filter Firewall Application-level Firewall Biometric measures Authentication Policy Servers Virtual Private Networking Email Content Inspection Anti-virus Software – Servers Anti-virus Software – Clients Encryption Tools Operating Systems Security Tools Internet Server Lockdowns Outbound Content Filtering Employee Training
Detection	Host-Based Intrusion Detection Systems Network-Based Intrusion Detection Systems Real-Time Network Monitors Auditing
Recovery	Log Analysis Applications Operating System Event Logs Web Server Logs Auditing Tools Intrusion Detection Tools Back-up and Recovery Tools Load Balancing Forensic Software Tools

NOTES