Information Security and Risk Management

Thomas M. Chen
Southern Methodist University, USA

INTRODUCTION

It is easy to find news reports of incidents where an organization's security has been compromised. For example, a laptop was lost or stolen, or a private server was accessed. These incidents are noteworthy because confidential data might have been lost. Modern society depends on the trusted storage, transmission, and consumption of information. Information is a valuable asset that is expected to be protected.

Information security is often considered to consist of confidentiality, integrity, availability, and accountability (Blakley, McDermott, & Geer, 2002). Confidentiality is the protection of information against theft and eavesdropping. Integrity is the protection of information against unauthorized modification and masquerade. Availability refers to dependable access of users to authorized information, particularly in light of attacks such as denial of service against information systems. Accountability is the assignment of responsibilities and traceability of actions to all involved parties.

Naturally, any organization has limited resources to dedicate to information security. An organization's limited resources must be balanced against the value of its information assets and the possible threats against them. It is often said that information security is essentially a problem of risk management (Schneier, 2000). It is unreasonable to believe that all valuable information can be kept perfectly safe against all attacks (Decker, 2001). An attacker with unlimited determination and resources can accomplish anything. Given any defenses, there will always exist a possibility of successful compromise. Instead of eliminating all risks, a more practical approach is to strategically craft security defenses to mitigate or minimize risks to acceptable levels. In order to accomplish this goal, it is necessary to perform a methodical risk analysis (Peltier, 2005). This article gives an overview of the risk management process.

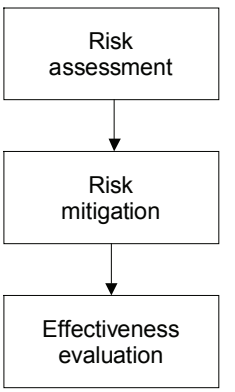
BACKGROUND

Risk management may be divided into the three processes, shown in Figure 1 (Alberts & Dorofee, 2002; Farahmand, Navathe, Sharp, & Enslow, 2003; NIST, 2002; Vorster & Labuschagne, 2005). It should be noted that there is no universal agreement on these processes, but most views share the common elements of risk assessment and risk mitigation (Hoo, 2000; Microsoft, 2004). Risk assessment is generally done to understand the system storing and processing the valuable information, system vulnerabilities, possible threats, likely impact of those threats, and the risks posed to the system.

Risk assessment would be simply an academic exercise without the process of risk mitigation. Risk mitigation is a strategic plan to prioritize the risks identified in risk assessment and take steps to selectively reduce the highest priority risks under the constraints of an organization's limited resources.

The third process is effectiveness assessment. The goal is to measure and verify that the objectives of risk mitigation have been met. If not, the steps in risk assessment and risk mitigation may have to be updated.

Figure 1. Steps in risk management



Essentially, effectiveness assessment gives feedback to the first two processes to ensure correctness. Also, an organization's environment is not static. There should be a continual evaluation process to update the risk mitigation strategy with new information.

RISK ASSESSMENT

It is impossible to know for certain what attacks will happen. Risks are based on what might happen. Hence, risk depends on the likelihood of a threat. Also, a threat is not much of a risk if the protected system is not vulnerable to that threat or the potential loss is not significant. Risk is also a function of vulnerabilities and the expected impact of threats.

Risk assessment involves a number of steps to understand the value of assets, system vulnerabilities, possible threats, threat likelihoods, and expected impacts. An overview of the process is shown in Figure 2. Specific steps are described below.

1. **System characterization:** It is obviously necessary to identify the information to protect its value and the elements of the system (hardware, software, networks, processes, people) that supports the storage, processing, and transmission of information. This is often referred to as the information technology (IT) system. In other words, the entire IT environment should be characterized in terms of assets, equipment, flow of information, and personnel responsibilities.
System characterization can be done through some combination of personnel interviews, questionnaires, reviews of documentation, on-site inspections, and automated scanning. A number of free and commercial scanning tools are available, such as Sam Spade, Cheops, CyberKit, NetScanTools, iNetTools, Nmap, Strobe, Netcat, and Winscan.
2. **Threat assessment:** It is not possible to devise a defense strategy without first understanding what to defend against (Decker, 2001). A threat is the potential for some damage or trouble to the IT environment. It is useful to identify the possible causes or sources of threats. Although malicious attacks by human sources may come to mind first, the sources of threats are not necessarily human. Sources can also be natural, for example, bad weather, floods, earthquakes, tornadoes, landslides, avalanches, and so forth. Sources can also be factors in the environment, such as power failures.
Of course, human threats are typically the most worrisome because malicious attacks will be driven by intelligence and strategy. Not all human threats have a malicious intention; for example, a threat might arise from negligence (such as forgetting to change a default computer account) or accident (perhaps misconfiguring a firewall to allow unwanted traffic, or unknowingly downloading malicious software).
Malicious human attackers are hard to categorize because their motivations and actions could vary widely (McClure, Scambray, & Kurtz, 2001). Broadly speaking, human attackers can be classified as internal or external. The stereotypical internal attacker is a disgruntled employee seeking revenge against the organization or a dishonest employee snooping for proprietary information or personal information belonging to other employees. In a way, internal attackers are the most worrisome because they presumably have direct access to an organization's valuable assets and perhaps have computer accounts with high user privileges (e.g., Unix root or Windows admin). In contrast, external attackers must penetrate an organization's defenses (such as firewalls) to gain access, and then would likely have difficulty

Figure 2. Steps in risk assessment