A Practical Approach to Threat Modeling

Tom Olzak
March 2006

Today's security management efforts are based on risk management principles. In other words, security resources are applied to vulnerabilities that pose the greatest risk to the business. There are several processes for identifying and prioritizing risk. One of the most effective is threat modeling.

There has been much written about threat modeling. But most of the papers and books come at the problem of threat and vulnerability management from an academic perspective. The papers and articles that do take a business management approach typically cover one or two aspects of the process.

This paper is a practical, high-level guide to conducting threat modeling activities within a business environment. It begins by exploring why threat modeling is important. This is followed by a step-by-step process, including some tools you might find helpful.

Why Threat Modeling?

It's common for security teams to receive reports of vulnerabilities with requests for immediate action to eliminate them. One big source of these requests is an organization's internal audit team. Another common source of fix-it-now-because-the-press/vendor-says-it's-critical messages is management, including many IS Directors. But should all vulnerabilities be considered emergencies? Are all vulnerabilities worthy of your security budget dollars?

One of the basic tenets of risk management is that not every vulnerability presents a threat to a network. Only a vulnerability that can be exploited is a threat to business operations and information assets. Threat modeling helps to identify those vulnerabilities that are actually critical in the unique environment that is your network. The threat modeling process should:

1. Identify potential threats and the conditions that must exist for an attack to be successful
2. Provide information about how existing safeguards affect required attack conditions
3. Provide information about which attack condition and vulnerability remediation activities add the most value
4. Help you understand which conditions or vulnerabilities, when eliminated or mitigated, affect multiple threats; this optimizes your security investment

The Process

The description of the threat modeling process varies depending on who's doing the telling. The following process is based on research covering several different approaches. Based on my experience as a security manager, I took what I believe to be best practices and compiled them into a hybrid model. This model consists of six steps, or phases:

1. Identify critical assets
2. Decompose the system to be assessed
3. Identify possible points of attack
4. Identify threats
5. Categorize and prioritize the threats
6. Mitigate

Identify Critical Assets

Before spending time assessing a system, you need to be sure it's important enough to your business to warrant the necessary time and resources. In this first step, you should list all critical assets and the systems on which they reside. Whether an asset is critical to business operations isn't an IS-only decision. The business users must also play a part in determining which assets can't be compromised without serious negative consequences.

Decompose the System

Once you identify your critical assets, select a system for which you'll create a threat model. A system is defined as an environment within your network that provides a specific set of related functions. Your human resources application, with all related servers, routers, switches, operating systems, user workstations, etc. is an example of a system. System decomposition produces two deliverables: a network diagram and a functionality (interaction) diagram. Figure 1 is an example of a network diagram.

The format of the diagram is a variation of the UML, or Unified Modeling Language standard. Each component in the ESI Financial System (a fictitious entity) is represented by a box. Each Workstation and server box includes information about the corresponding real-world device's hardware and software configuration. In addition to the actual hardware connectivity, logical flow of data is also indicated. Finally, the network diagram should include interfaces to outside entities. In this case, the connection to the Internet is depicted.

It's a common mistake when putting a network diagram together to omit pieces that aren't considered critical to the system's operation. Make sure you include EVERY component, interface, and user access point that touches the system in any way. Also identify any interdependencies with other systems.

Figure 2 is an example of a simplified Functionality or interaction diagram.

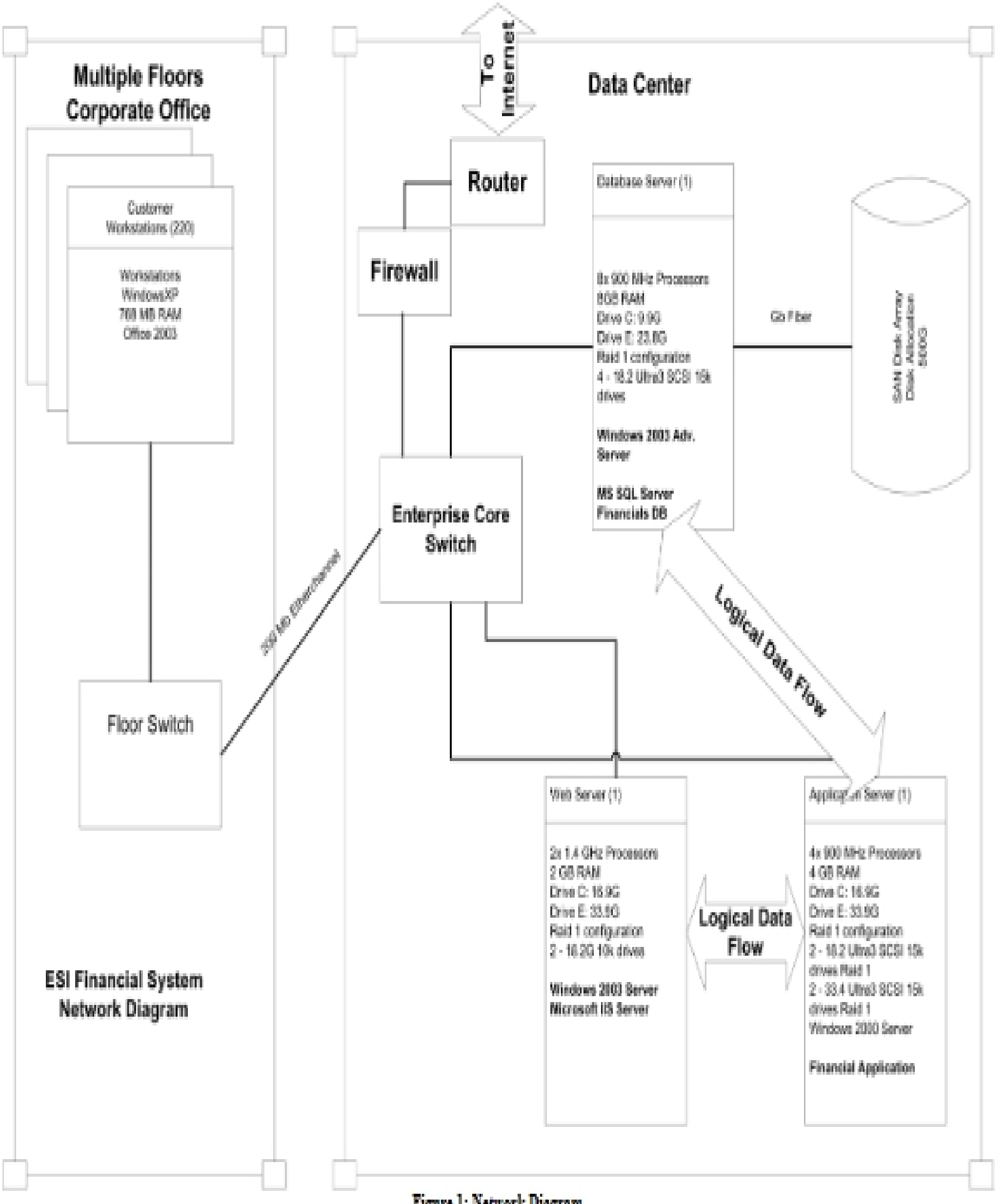

Figure 1: Network Diagram