

Netsoft Technologies, Inc.

www.ISAExpress.com

323 Regatta Dr. Avon Lake, Ohio 44012 voice: 440-796-8500

Information Security Assessment (ISA) Express

@copyright 2005

Why is a layered security defense necessary?

Build a layered defense to guard against threats and lower vulnerability:

When building an “Information System” defense a layered approach should be utilized. This includes securing the infrastructure, the communications protocols, servers, applications that run on the servers, and the file system. Some form of user authentication is also recommended.

- A strong layered defense requires an intruder to break through several layers to reach their objectives. To compromise a file server that is part of a network, a hacker must break the network security defense, break the server security, break the applications security and then break the local file system security. It is more difficult for a hacker to break through four layers of protection vs. a single layer defense.

Securing the Network Infrastructure:

- Network system hardening – remove unused services on the LAN/WAN.
- Ensure the latest security patches and service packs are applied.
- Limit personnel with administrator privileges.

Hardening the network infrastructure system minimizes the risk of a security breach using the network.

Securing Communications Protocols:

- Remove or eliminate any unnecessary communications transport protocols – i.e. NetBIOS, IPX/SPX, AppleTalk, RAS, remote dial-up, FTP, HTTP, HTTPS.

Securing the Applications:

- Apply the latest security patches.
- Enforcing user level security for web server applications, client server and local PC based applications.

Hardening the applications on a system minimizes the chance of a security breach using an application.

Securing the Local File System:

- Use access control permissions and security authentications to protect all production files.
- Use encryption of files to secure sensitive information.

