

Creating Effective Security for Small Business

Information is the life blood of any business. Information such as secret product designs, specific service processes, marketing strategy, financial statements, and client lists are all important assets for running a business. Knowing where and how this critical information is stored and protected is the most important piece of knowledge a business owner can have.

The problem is many small companies do not know what information is critical to their business. One of the first steps a small business should take when starting to think about information security is data identification and classification. This involves determining the criticality of company information based on its business impact, sensitivity, and its vulnerability to loss or theft.

Regardless if a company has only one computer or makes use of a network file server, make sure that business files are stored in a hierarchical directory structure, and access controls are set up to prevent unauthorized users from viewing or modifying sensitive business files. Storing and categorizing information in a single logical location allows a business to gain a proper perspective on the information they have and gain an appreciation for it's value to the business.

The next step that small businesses can take to protect themselves is to appropriately choose an operating system that will effectively balance productivity, usability, and security. Windows 95, 98 and ME may be required for certain business applications, but do not provide adequate security measures for most businesses. Linux or BSD based operating systems often provide good security, but at the cost of lowered business functionality and inconsistent support. Windows 2000 or XP and Mac OS/X allow for good business functionality while providing a decent level of protection.

Once an operating system has been chosen and installed, it should be brought up-to-date with the latest patches and service packs available. Regularly look for new patches for your systems, as 99% of all successful computer exploits are based on known vulnerabilities where patches were readily available.

Once information is properly identified and basic infrastructure is in place, what can be done to improve security even further and prevent attacks? Two of the most common preventative measures that should be implemented are virus scanners and a firewall to protect your business against attackers. However, installing them is only half the battle. These technologies must be properly maintained, which includes updating virus definition lists, modifying firewall rules and access controls and monitoring of these systems.

The widely-accepted rule of thumb in the industry regarding information security is this: *For every \$1000 of infrastructure or intellectual property owned, a company should spend approximately \$150 protecting it, or 15% of the total value of the asset.*

In a business environment where change and risk are inevitable, small businesses need to take information security seriously and take steps to mitigate the risk of using information technology and the Internet. Knowing where and how your critical information is stored and protected could make the difference between the success and failure of your business.

For more information download the [Securis Information Security Checklist](#) from the Securis website (www.securis.com). The checklist details sixteen of the top information security topics that companies should be looking at in order to improve their security posture.