BUSINESS
FOR THE CONSUMER
www.ftc.gov
FEDERAL TRADE COMMISSION
1-877-FTC-HELP



# Security Check: Reducing Risks to your Computer Systems

When consumers open an account, register to receive information or purchase a product from your business, it's very likely that they entrust their personal information to you as part of the process. If their information is compromised, the consequences can be far – reaching: consumers can be at risk of identity theft, or they can become less willing – or even unwilling – to continue to do business with you.

These days, it's just common sense that any business that collects personal information from consumers also would have a security plan to protect the confidentiality and integrity of the information. For financial institutions, it's an imperative: The Gramm-Leach-Bliley Act and the Safeguards Rule, enforced by the Federal Trade Commission, require financial institutions to have a security plan for just that purpose.

The threats to the security of your information are varied – from computer hackers to disgruntled employees to simple carelessness. While protecting computer systems is an important aspect of information security, it is only part of the process. Here are some points to consider – and resources to help – as you design and implement your information security plan.

## Starting Out

Sound security for businesses means regular risk assessment, effective coordination and oversight, and prompt response to new developments. Basic steps in information security planning include:

- identifying internal and external risks to the security, confidentiality and integrity of your customers' personal information;
- designing and implementing safeguards to control the risks;
- periodically monitoring and testing the safeguards to be sure they are working effectively;
- adjusting your security plan according to the results of testing, changes in operations or other circumstances that might impact information security; and
- overseeing the information handling practices of service providers and business partners who have access to the personal information. If you give another organization access to your records or computer network, you should make sure they have good security programs too.

When setting up a security program, your business should consider all the relevant areas of its operations, including employee management and training; information systems, including network and software design, and information processing, storage, transmission and disposal, and contingencies, including preventing, detecting and responding to a system failure. Although the security planning process is universal, there's no "one size fits all" security plan. Every business faces its own special risks. The administrative, technical, and physical safeguards that are appropriate really depend on the size and complexity of the business, the nature and scope of the business and the sensitivity of the consumer information it keeps.

## Determining Priorities Among Risks: Computer Systems

Although computer systems aren't your only responsibility related to information security, they are an important one. With new vulnerabilities announced almost weekly, many businesses may feel overwhelmed trying to keep current. Guidance is available from leading security professionals who put together consensus lists of vulnerabilities and defenses so that every organization, regardless of its resources or expertise in information security, can take basic steps to reduce its risks. The lists identify the commonly exploited vulnerabilities that pose the greatest risk of harm to your information systems. Use these lists to help prioritize your efforts so you can tackle the most serious threats first.

- **The 20 Most Critical Internet Security Vulnerabilities** (www.sans.org/top20) was produced by the SANS Institute and the FBI. It describes the 20 most commonly exploited vulnerabilities in Windows and UNIX. Although thousands of security incidents affect these operating systems each year, the majority of successful attacks target one or more of the vulnerabilities on this list. This site also has links to scanning tools and services to help you monitor your own network vulnerabilities at www.sans.org/top20/tools.pdf.
- **The 10 Most Critical Web Application Security Vulnerabilities** (www.owasp.org) was produced by the Open Web Application Security Project (OWASP). It describes common vulnerabilities for web applications and databases and the most effective ways to address them. Attacks on web applications often pass undetected through firewalls and other network defense systems, putting at risk the sensitive information that these applications access. Application vulnerabilities are often neglected, but they are as important to deal with as network issues.

While you are designing and implementing your own safeguards program, don't forget that you should oversee service providers and business partners that have access to your computer network or consumers' personal information. Check periodically whether they monitor and defend against common vulnerabilities as part of their regular safeguards program.

For more information on privacy, information security, and the Gramm-Leach-Bliley Safeguards Rule, visit www.ftc.gov/privacy.

## For More Information

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

## Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.