

[united states](#)

- [global sites](#)
- [licensing](#)
- [archives](#)
- [shop](#)
- [newsletter](#)
- [trialware](#)
- [products](#)
- [enterprise security](#)
- [about symantec](#)
- [search](#)
- [feedback](#)

© 1995-2002 Symantec Corporation.
All rights reserved.
[Legal Notices](#)
[Privacy Policy](#)

Does Your Business Need a Security Audit?



A hacker invaded Microsoft, pranksters took down Yahoo, and in less than a day the "I Love You" virus unfolded its wrath on computers all over the world. Imagine what a security breach could do to *your* business.

Small businesses are just as susceptible to hacker intrusion as larger companies. But many small businesses leave their network vulnerable because they can't afford to hire a full-time IT staff. Hackers know this and exploit the unprotected systems.

You realize you need to bolster your online security to protect your customer data, payroll information, and trade secrets, but you're not sure which parts of your system are vulnerable and you're not sure where to start. A security audit can help you identify the weak spots -- or gaping holes -- in your business' network protection.

Small Business Security Challenges

Businesses lose billions of dollars a year to hackers, frauds, and viruses. Most businesses don't have enough skilled IT resources and few companies employ full-time network security personnel. Even if you have access to these sources, you may find keeping up with explosive virus growth and evolving hacking techniques a challenge.

Firewalls can also create a false sense of security -- they are not foolproof, and become even less so when they are not configured frequently to stay current with a swiftly changing network. There is also the unpleasant fact that much computer crime comes from inside the business world. Discontented employees may have access to more information than they need, enabling them to make malicious use of that data. And unsecured remote-access terminals and modems provide a portal for hackers, who view firewalls as simply a minor challenge.

What Do Security Audits Tell You?

A data security audit provides you with an assessment of your network and workstation vulnerabilities. Security audits should be performed regularly to ensure utmost compatibility in a changing and growing workplace. First-time audits and risk assessments often reveal serious shortcomings in a security system. Your business may be no different.

A security audit evaluates your strength of security by examining any combination of crucial security areas: password strength, access control, user account restrictions, system monitoring, data integrity, and confidentiality.

The audit helps you evaluate your network security by:

- Allowing you to see your network as a hacker would -- from the outside
- Evaluating DNS inconsistencies
- Performing a variety of scans, such as TCP/IP
- Informing you which ports are open and scanning them for security weak spots

An audit can provide vulnerability assessments for the following:

- Denial of service (DoS) and Windows-based attacks
- Your mail server and firewall
- Remote access
- Backdoors
- FTP

Could You Benefit From a Security Audit?

One way to look at the issue is not whether or not you think you're vulnerable, but how much your loss of information assets would set you back. When considering your security, bear in mind what data you are protecting and how much your business would be injured if you lost it. What impact would the loss of confidentiality or availability have on your business? How about corrupted or stolen data?

What Is Involved in a Security Audit?

Security audits are used to assess not only your system vulnerabilities, but

Not sure what you need?
Small Business
ProductSelector go

smallbiz products

antivirus
problem solving
remote/productivity
internet security
Macintosh products

multi-user packs
Save Time and Money go

smallbiz resources

sign up to receive our
monthly newsletter go

smallbiz security

virus alert go

W32.Goner.A@mm

is your system safe?
find out... **Symantec Security Check** go

a free service to help you understand and protect against security threats

essentially those of your security policies as well. With the help of auditing software, you are able to compare current levels of security to what you'd like those levels to be. You may believe that you have instated a clever password policy, but an audit can show you exactly how effective that policy really is.

Current Security Approach Assessment

The first stages of an audit involve scrutinizing the business' current security approach, including encryption methods, data storage, and login/password usage. Assess your main security goal: Is it secure file transmission or internal HR protection? You also want to take into account the way in which your company does business. There are e-commerce security issues, and concerns about the storage of confidential customer data. Does your e-commerce site accept credit cards? Knowing that this is a sensitive process, do you have adequate encryption? Is it functioning optimally?

Network Mapping

The next step is to map your network with the help of auditing software, which compiles a list of all servers, routers, and workstations. It is essential to confirm that all of your components are recognized by the auditor and represented correctly. Then using a variety of non-intrusive probes, the auditor determines operating systems and applications and looks for potential vulnerabilities in your servers and infrastructure.

The auditing software detects network characteristics and then presents a series of potential problem areas:

- Insecure or anonymous logins
- Hacker-friendly writable directories
- Bounce-attack spam compliance
- Mail gateway or Web server vulnerabilities

Port Scanning

During port scanning, the auditing program conducts a more intense examination of your network. There are several different types of scan methods, the TCP connect scan being the most basic. It calls to open a connection to every port on the destination machine, logging those where the connection is successful. You can limit the port scan to "known" services, or to a range of ports on your machine. A well-known services scan, which is completed quickly, scans ports where specific services are usually located. For example, http is normally found on port 80. And if you have a firewall, you can test its impassibility.

How to Get Audited

You've decided to assess the security of your network. What's the next step? There are a few different ways to have a complete risk analysis performed. Depending on how much time and money you are willing to spend, you can either purchase software to do it yourself, or you can hire professional network security analysts to do the job for you. Performing the process yourself is of course less expensive, and some small business owners find the information they learn about their network during an audit useful to future security decisions.

If you prefer the approach of having an expert risk analysis consultant in house, there are many resources to help you select the right one. Word of mouth is usually a reliable method, so ask your fellow small business owners if they can recommend someone to do the job. Or you can check out the following online resources to get you on your way to a safer network. The [Information Systems Audit and Control Association](#) (ISACA) is a recognized global leader in IT governance, control and assurance. If you prefer a directory type format, go to the [IT Audit Yellow Pages](#) for further assistance selecting a consultant. Both [More House](#) and [DMOZ](#) offer expansive lists of security auditors, and [Audit Net](#) features names and resources to answer your in depth questions about the audit process.

Symantec Expert and Symantec Retriever team together to deliver comprehensive risk analysis for your network. Retriever performs customizable audits, maps your network, identifies vulnerabilities, and provides policy recommendations. Expert then identifies assets and critical business function, and assesses the potential impact of a security breach. Easy to install, use, and maintain, these solutions can be rapidly deployed throughout an organization with minimal effort and cost. Used together, [Symantec Expert](#) and [Symantec Retriever](#) enable your organization to make intelligent, proactive business decisions about your network security and protect one of your most vital assets - information.

After the Audit

Once the audit is completed and you have the results, it may be time to adjust your current privacy policy or its enforcement. Auditing is only helpful if you use the information you gain. Here are some areas of particular concern that your business should be addressing:

- **Awareness.** Make sure all employees understand the importance of computer security, policies, and procedures.

- **Policy Implementation.** Be proactive in addressing IT issues by developing policies and standards and ensuring that the policies are implemented.
- **Growth.** As your small business grows, update security policies to ensure proper protection for an increased workforce.

Once you are aware of your system's vulnerabilities, you are able to better protect your customers and data, communicate with employees on the topic of security, and adjust your policies so they best fit your business' needs. A safe connection and secure data storage will allow you to stop worrying about online dangers and start concentrating on growing an even more successful business.

[> home](#) [> find a solution](#) [> need more than 10?](#) [> tech resources](#)