

iQ

SMALL  
MEDIUM  
BUSINESS

Your Business Just Got Smarter  
SECOND QUARTER 2005

# A Better Way

DISCOVER THE POWER  
OF IP COMMUNICATIONS

PAGE 24

IAN SMITH, NEW YORK CITY  
ECONOMIC DEVELOPMENT  
CORPORATION

CISCO SYSTEMS



[CISCO.COM/GO/IQMAGAZINE](http://CISCO.COM/GO/IQMAGAZINE)

# ADDRESSING NETWORK SECURITY

Many SMBs do not have adequate network security in place. Here's help to make sure you do.

**NOW MORE THAN** ever, small and medium-sized businesses (SMBs) are relying on their networks for internal and external communications, inventory, billing, sales, and trading with partners—in short, for just about everything. And yet, many SMBs haven't adequately protected their networks.

Why? Because to many SMBs, network security can seem too complex and too resource intensive to tackle. Many companies see network security as an expense that won't help them grow. "They would rather use any extra resources they have on sales and marketing," says Larry Clinton, chief operating officer of the Internet Security Alliance (ISA).

In addition, some SMB leaders believe that their companies are less likely to become targets of hacker attacks than are larger companies. Meanwhile, many larger enterprises have further bolstered their network security. As hackers and others with malicious intentions find it increasingly harder to infiltrate the networks of larger enterprises, they will turn their attention to SMBs networks.

The numbers bear this out. For example, the Mydoom worm in 2004 affected one out of three SMBs, but only one out of six larger companies, according to Clinton.

## START CLEAN

To begin, broaden your view of network security. Rather than categorizing it as an IT concern, you should instead consider it as a business-continuity issue. Networks have become an intrinsic part of conducting business, making security planning as important as sales and marketing planning.

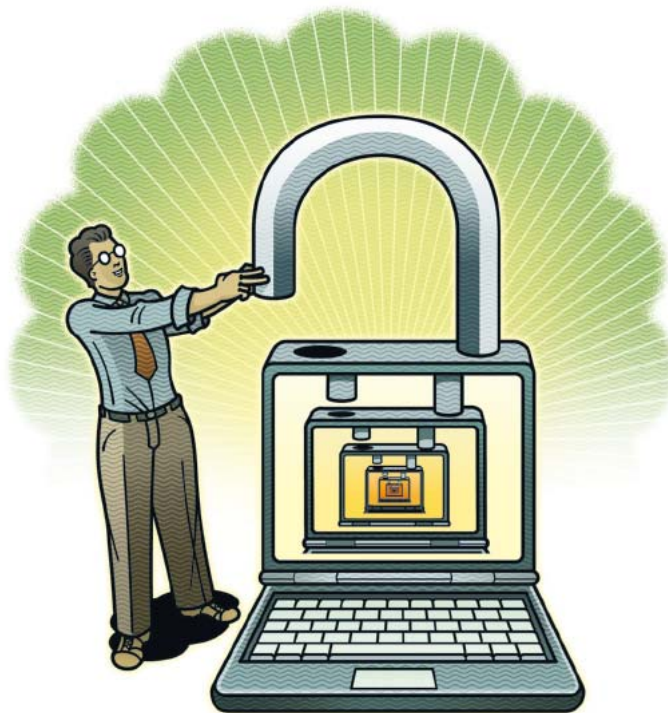


ILLUSTRATION BY PETER HOEY

Before any planning, start with a clean slate. Most SMBs have at least some network security in place. But is your current level of security enough? It will serve you well to question everything and assume nothing.

## PUT IT IN WRITING

Once you've finished an internal network-security assessment, it's often useful to have an outside consultant perform an independent assessment. Compare the consultant's results to your own in order to identify any gaps. Armed with this information, you can develop (or revise) your written network-security plan. If you've enlisted outside help, your consultant can help you with this task. It's critical to document your plan in order to maintain a consistent approach to network security; with a written plan in place, you can compare results over time,

troubleshoot, educate employees, and track your progress in each area.

Finally, it's important to realize that your network security must be both consistent and flexible. Policies—especially those created with your business's most important assets in mind—aren't likely to change significantly unless your business itself does. However, you should evaluate and update the procedures used to enforce these policies when the need arises.

The following tips should help you develop—and win support for—an effective network-security plan:

- In discussions with financial or other officers, focus on return on value rather than return on investment. Point to the potentially devastating impact of security breaches—such as loss of revenue or customer litigation.
- Never assume network attacks will only

come from outsiders. Loyal employees can inadvertently create security vulnerabilities, and disgruntled or former employees can cause considerable damage.

- Develop a companywide security strategy. Don't be tempted to confront security concerns with a piecemeal approach rather than a single, unified strategy.
- Work with other company officers to develop and implement security strategies, focusing on technology, training, physical site security, and more.
- Find the right balance between security and usability. The more secure your network is, the more difficult it is to use.

Ultimately, a process of continual revision is critical to the success of any network-security plan. "The most effective network-security plan," concludes Clinton, "is one that is always a work in progress."

JAMES A. MARTIN WRITES FREQUENTLY ABOUT NETWORK SECURITY AND IS A PRINCIPAL OF MARTIN PARHAM GROUP IN SAN FRANCISCO.

### NEXT STEPS

Learn about the latest adaptive security solutions, which make it easier for SMBs to keep network defenses current, in "Self-Defending Networks" on page 40.

Use the Cisco Security Policy Builder ([cisco.com/go/iq-spb](http://cisco.com/go/iq-spb)), a free and simple online tool, to help you start developing a sound network-security policy.

## NETWORK-SECURITY CHECKLIST

Every SMB should have a written (and thoughtfully prepared) network-security plan in place. Answering the following questions can help you develop your own policy:

### TAKE INVENTORY OF YOUR CURRENT SECURITY TECHNOLOGIES

Do you have any of the following?

- |  |   |
|--|---|
| <input type="checkbox"/> Firewall                | <input type="checkbox"/> Secured wireless network |
| <input type="checkbox"/> Virtual private network | <input type="checkbox"/> Anomaly detection        |
| <input type="checkbox"/> Intrusion prevention    | <input type="checkbox"/> Identity management      |
| <input type="checkbox"/> Virus protection        | <input type="checkbox"/> Compliance validation    |

### IDENTIFY YOUR MOST IMPORTANT DIGITAL ASSETS AND HOW THEY CAN BE ACCESSED

- Exactly what are your company's digital assets? What are they worth?
- Where do those assets reside?
- Who has access to these assets, and why? Do all employees have the same level of network and application access?
- Do you extend access to partners and customers?
- How do you control, validate, and monitor that access?

### EVALUATE THE POTENTIAL IMPACT OF A SECURITY BREACH

- What is the potential financial impact of a network outage due to a security breach?
- Would a security breach be likely to disrupt your supply chain, and (if so) how?
- What would happen if your Web site went down? How long could the site be unavailable before you suffered a significant financial impact? Minutes? Hours? Days?
- Do you have e-commerce features on your site? How long could your storefront be unavailable before you suffered a significant financial impact? Minutes? Hours? Days?
- Does your company have insurance against cyber attacks, or against the misuse of your customers' data? If so, is this insurance adequate?

### CONSIDER BOTH CURRENT AND FUTURE NEEDS

- In what ways do you expect your business plan to evolve over the next few years?
- How recently have you updated your network equipment? Software? Virus definitions?
- What type of security training—if any—do you provide to your employees?
- How will growth affect your digital assets and their value to your business as a whole?
- In the future, are you likely to have a greater need for remote employees, customers, or partners to access those digital assets?