



WHAT YOU NEED TO KNOW ABOUT NETWORK SECURITY

WHAT YOU NEED TO KNOW ABOUT NETWORK SECURITY

BY FRED SANDSMARK



While networking technology and the Internet have created new opportunities for small and medium-sized businesses (SMBs) to grow and compete, they have also highlighted a need to protect computer systems against a wide range of security threats. In a 2003 survey, the Computer Security Institute (CSI) reports that 78% of its respondents experienced “frequent” attacks via their Internet connections, compared with 59% in 2000.

These days, even very small businesses feel pressure to bring their operations online and have made moves to do so. However, “they often overlook security, but it should be top of mind,” says Jim Browning, vice president and research director for SMBs at research firm Gartner.

Without proper protection, every part of a network is vulnerable to a security breach or unauthorized activity from hackers, competitors, or even employees. Through 2005, 40% of SMBs that manage their own network security and use the Internet for more than e-mail will experience a successful network attack, according to Gartner—and more than half of these companies won’t even know they were attacked.

“Smaller companies get lulled into a state of complacency,” says Browning. “They usually react to the last virus, or the most recent defacing of their Web site. But they’re stuck in a situation where they only have so much [budget] to spend on security.”

The Basics

As with all crime, the threats against networks and resources come from a small element of the population. But although this element may be small, it’s growing, in part because free, downloadable tools are available online that enable a novice to launch an attack that exploits known vulnerabilities in computer systems. The people behind intentional network intrusion threats might be hackers, crackers, or snoops.

- **Hackers** are content just to get into a system to say they’ve been there, much like mountaineers who climb a mountain “because it’s there.”
- **Crackers** are more malicious and intentionally do damage once they get into an organization’s computer network, often by modifying a Web page or by stealing or damaging data.
- **Snoops** are generally employees who access private information because they are curious or mischievous.

Common security threats include network attacks and social **engineering**, as well as viruses, worms, and **spyware**. Technically, politically, or financially motivated sophisticated network attacks usually target a particular company or system. They may render a user database corrupt, steal account or proprietary information, or install undetected agents within a network allowing the intruder to launch an attack using your resources.

Network attacks come in the following three basic forms:

- **Reconnaissance attacks** are information-gathering activities in which intruders collect data to later compromise a network.
- **Access attacks** exploit weaknesses in network access points.
- **Denial-of-service attacks** send large numbers of requests to a server, essentially creating a traffic jam and rendering the server inaccessible by legitimate users.

You must optimize the defenses you use to protect your network from outside attacks to also protect valuable assets from a potential internal attacker. In fact, Gartner estimates that 70% of all attacks that cause more than \$50,000 in damage involve a company insider.

Social engineering—deception, essentially—is also used to learn sensitive information about a company’s network and its entry points. Unsuspecting employees often aid these efforts. For example, social engineering may involve a phone call from someone posing as a technical-support representative requesting password information to update a system.

Computer viruses, Trojan horses, worms, and new breeds of threats that blend these together can have a devastating impact on your company’s productivity and bottom line. These threats seldom target a specific company and are usually unleashed on the Internet and arbitrarily seek out systems to infect. Viruses and Trojan horses normally rely on unsuspecting users to inadvertently propagate the infection, whereas worms are self-replicating and self-propagating, enabling them to spread globally in a matter of hours or even minutes to infect unpatched systems. The total number of these threats has grown from around 27,000 in 2000 to nearly 60,500 in 2003, according to security-software firm PestPatrol.

Solutions

Identifying—and then eliminating or reducing—security vulnerabilities is critical to minimizing risk. Usually, the first step is to create a formal, written security policy. For most growing companies, the need for such a policy becomes apparent when human resources (HR) activities become formalized. “Companies that have a formal HR process are including Internet and e-mail use policies as part of the hiring process,” explains Browning. “That includes the fact that a company PC, and the data on it, is the property of the company, not the employee.”

A written policy becomes especially important when an employee is caught improperly using company assets, which can become grounds for termination based on a violation of the corporate “appropriate use” policy.

Once a security policy is in place, experts recommend that you conduct a thorough security assessment. “The No. 1 priority is that you assess your technology and identify all the risks and exposure that you have based on the technology you have adopted,” advises Browning. A security posture assessment identifies the current level of security readiness in the organization and evaluates the effectiveness of existing security measures, policies, and response mechanisms.

Defined:

- **Access Control:** Validates a user's identity and determines what he or she can access on a network. Authentication methods range from simple password systems to biometric devices that scan users' fingerprints or faces.
- **Firewall:** A software or hardware solution that blocks intrusion attempts and allows only authorized data to enter a network—the digital equivalent of a locked door. Firewalls are becoming increasingly available as a managed service.
- **Identity Management:** Identifies users and their current state of acceptance; defines and enforces network and resource access rights.
- **Intrusion Detection:** Software capability that analyzes network activity, detects security breaches, and sends alarms to administrators.
- **Threat Defense:** Collaboration of security technologies (firewalls, intrusion detection/protection) and network intelligence services to minimize impact of both known and unknown threats.
- **Trojan Horse:** A malicious program that is disguised as something benign, such as a game.
- **Virus:** A program that searches out other programs on network devices and “infects” them by embedding a copy of itself in them. When these programs are executed, the embedded virus is executed too, thus propagating the infection. This normally happens invisibly to the user. Unlike a worm, a virus cannot infect other computers without assistance.
- **VPN:** Virtual private network technology allows computers to connect securely to a company's systems over the public Internet. Usually consisting of a hardware device on the company network and special software on the remote computer, companies can use VPNs for small satellite offices, telecommuters, and employees who travel.
- **Worm:** A program that propagates itself over a network, reproducing itself as it goes.

Once your company has assessed its security needs, a combination of tactics can reduce or even eliminate many of today's security headaches. These span the gamut from deploying the appropriate technologies to detect and prevent network abuses and security breaches to developing employee training and consistent enforcement of security policies.

What To Watch For

Several new developments are helping SMBs navigate the network security landscape. Vendors that have traditionally provided security products to large enterprises are creating solutions specifically for the SMB market. Many companies don't have the time, manpower, budget, or expertise to piece together all of the technologies required to protect the company's productivity and assets from today's threats.

“SMBs want an easy-to-use, easy-to-deploy product,” says Browning.

Fortunately, leading vendors now integrate multiple security features into every level of their networking products, improving network interoperability and minimizing the learning curve associated with the introduction of new devices.

Securing the network and associated resources also requires updating and patching systems on a regular basis. The Slammer and Blaster computer worms both attacked vulnerabilities in Microsoft Corp. operating systems for which a patch was available prior to the release of the worms.

Some SMBs choose to outsource their security needs to a managed security service provider (MSSP). Many MSSPs are able to perform a security posture assessment and then design, configure, and provide around-the-clock management of the security solution for a fixed monthly fee. “We definitely see a lot of SMBs looking at managed security services, but the adoption is still pretty low,” says Browning.

He attributes the slow uptake to “the whole muddy issue of outsourcing.” SMBs like the idea of a fixed monthly fee, but they struggle to find a vendor they can trust, according to Browning. Nevertheless, he anticipates an increase in the adoption of managed security services by SMBs.

Bottom-Line Impact

Internet security can directly affect a company's bottom line. The 2003 CSI survey, conducted jointly with the FBI's Computer Intrusion Squad, reports that 75% of the companies surveyed acknowledged a financial loss due to a security breach. For the 47% of respondents that could quantify their losses (or chose to disclose this information, which many do not), the total was a staggering \$201.8 million. Theft of proprietary information, denial-of-service, and computer viruses were the three most expensive types of attacks. And these aren't all happening to Fortune 500 companies. Indeed, 18% of CSI respondents had fewer than 100 employees, and 23% reported less than \$10 million in annual revenues.

**From Cisco:
Security Systems Evolve**

As security threats have evolved, so too have the solutions to protect your IT infrastructure. For smaller networks, vendors are augmenting or replacing special-purpose security point products with full-service, integrated networking devices. Features once considered security-specific are now becoming embedded in the network infrastructure.

In the future, closer collaboration between the network, desktop, and host computing environments will be necessary for companies to pursue a seamless, inherent, and transparent security posture.

Today's best practices lead to system-level approaches in the area of secure connectivity, threat defense, and identity/admission control.

The damaging effects of recent computer worms highlight the need for server and desktop patch control. This can be overwhelming for IT managers of small and large networks alike. New "behavior"-based security software is required to prevent security exploits even when system vulnerabilities exist. This category of "zero update" applications, sometimes known as "host intrusion protection," will protect a device from new, previously unseen attacks. This technology greatly reduces the dependency on frequent system patches and antivirus definition updates.

A cost-effective, tightly integrated, end-to-end security solution that protects the network infrastructure and critical endpoints, controls access, and protects external communications is necessary to enable business growth.

More difficult to quantify, but especially important to SMBs, is the downtime and productivity loss associated with security-incident response. In many cases, companies must temporarily remove critical servers, desktop systems, and supply-chain links from service immediately following a security breach. In 2001, the average annual economic impact of malicious attacks for a company reliant on Internet communications with 100 nodes (desktops, servers, and other network devices) was \$233,370, according to estimates by IT-research firm Computer Economics.

But even in the face of huge potential losses, smaller companies are often reluctant to spend money on security precautions. "A lot of SMBs look at security products like insurance," Browning says. "They hate paying for this stuff. They think it's something they're never going to use."

That's usually about the time a computer virus hits.

In The Real World

Though it's hard to paint a clear picture of the security landscape—as noted, companies are often reluctant to admit it—there are success stories among SMBs.

When Hahn & Hessen, a Manhattan-based financial-services law firm with 50 attorneys and 40 support staffers, moved its offices recently, it deployed a single Internet Protocol (IP) network for its computer data and telephone communications. A vital part of the new network is a Cisco PIX 515 Firewall at the network "edge"—the point at which the company's internal network connects to the outside world. Because its staff members sometimes work from home, remote offices, client sites, or while traveling, the firm also installed a Cisco VPN 3005 Concentrator, which provides secure connections for staff members who access the company network over the Internet. Hahn & Hessen also plans to install Cisco PIX firewalls and other network gear in some of its attorneys' homes.

Based in Austin, Texas, Vignette Corp. provides software to help companies rapidly build, manage, and deploy Web applications. With close to 900 employees and offices worldwide, having a secure network is critical. When the company redesigned the network, it used a modular approach based on the SAFE Blueprint from Cisco. "This gave us control over most viruses, network management, deployment, and growth," says Selim Nart, senior network engineer. Vignette implemented security solutions in stages, beginning with firewalls, then VPNs and intrusion-detection systems.

Vignette's IT staff was impressed by the amount of activity thwarted by the intrusion-protection solutions but was having difficulty keeping up. "We were receiving about 90,000 alarms per month," Nart recalls. "We did not have the personnel to handle it." Adding Cisco Threat Response software to the implementation solved the problem. "The software creates a sort of artificial intelligence that is about 25 times faster than a regular engineer who receives alarms, investigates them, and then reports on their severity and whether we should pay attention to them," says Nart. He calculates that the software

Next Steps:

- Go to cisco.com/go/smb-security for more information about Cisco network security solutions for SMBs.
- Find more information about Cisco Security Agent at cisco.com/go/csa.
- For more information about the Cisco SAFE Blueprint, go to cisco.com/go/safe.

The Computer Security Institute's 2003 survey is available free of charge at gocsi.com.

delivered a 95% reduction in alarms, eliminating more than 85,000 false alarms in one month alone.

What To Do Next

Security threats—and the technology to minimize them—are constantly evolving. Successful protection requires an ongoing, process-oriented approach, including the following:

- Conduct periodic reviews of security policies and security assessments.
- Deploy security technologies that provide secure connectivity, threat defense, and identity management capabilities when and where appropriate.
- Patch and protect endpoints, servers, and desktops against known and unknown threats.

It is important to realize that there is no single security technology “silver bullet.” Even in small networks, a layered strategy, in which security is integrated throughout all devices, provides the most effective protection.

Many basic security steps don't require a lot of money or effort. SMBs can take simple and affordable steps to improve their security posture, from disabling inactive user accounts to blocking potentially dangerous e-mail attachments, according to Browning.

“Small and midsize businesses can avoid the most common Internet attacks, protect against break-ins, and greatly reduce the extent of damage from attacks,” says Browning.

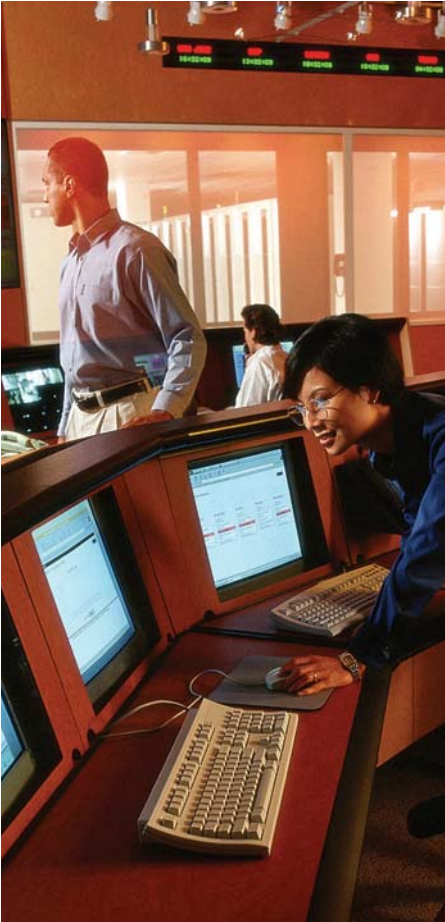
Just because SMBs represent smaller targets than enterprises doesn't mean they're any less vulnerable, but they can still protect themselves by performing affordable, common-sense, preventive activities.

iQ Magazine, First Quarter 2004

<http://www.cisco.com/go/iqmagazine>

SECURING BUSINESS NETWORKS

BY JAMES A. MARTIN



Do you open up Pandora’s box when you open up your network to B2B transactions with trading partners and suppliers? Companies that use their networks to link applications with those of other companies often realize compelling benefits. In an uncertain economy, the efficiencies and potential cost savings that can result from these links, including the ability to outsource payroll and invoice processing to a third-party provider over the Internet, are particularly attractive.

At the same time, concerns about network security continue to rise. For example, companies reported 82,094 security incidents to the CERT Coordination Center (CERT/CC) in 2002, compared with 52,658 in 2001 and 21,756 in 2000. CERT/CC is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Vulnerability Concerns

To some degree, security risks are greater with online transactions than with traditional methods, according to Laura Koetzle, a senior analyst in Forrester Research’s infrastructure and telecommunications area. The increased risk stems primarily from more companies linking electronically with partners to cut costs. And dealing with partners and suppliers by any method has never been entirely secure, Koetzle adds.

“Often in the past, transactions were conducted back and forth over fax machines—and that wasn’t exactly secure, either,” says Koetzle.

At the same time, some businesses—particularly those with fewer than 5,000 employees—frequently take unnecessary risks with their B2B transactions, according to Jim Hurley, vice president and managing director for security and privacy at the Aberdeen Group research firm. For instance, some companies communicate sensitive information to partners in unencrypted e-mail and conduct unsecured Web-based transactions, even though adding extra e-mail and browser security is relatively easy and inexpensive.

How much network access a company gives to its partners or suppliers affects the company’s risk level, as do the security and data-recovery strategies of the partners. When you integrate your network with those of other companies, then “whatever happens to them can happen to you,” Koetzle warns.

Security risks from B2B transactions often relate to privacy, including protecting credit-card information and other data from outsiders. Authentication is another concern; it’s critical for companies to verify that the people with whom they are transacting business are who they claim to be.

Then there is legal liability. “Your network is only as strong as its weakest link,” says Clint Kreitner, president and CEO of the Center for Internet Security (CIS), a nonprofit organization dedicated to helping organizations manage data-related security risks. “If you connect to a partner’s network and you accept its vulnerabilities, then you are putting the information on your own network at risk. And you can be legally liable if your customer’s sensitive data is stolen.”

From Cisco:

Cisco Secures the Entire Network

In the current economy, organizations depend on their networks more than ever to enhance productivity and reduce costs. Meanwhile, intruders have developed increasingly sophisticated network-penetrating tools, and governments have imposed stricter regulations for protecting information and privacy online, both of which increase the importance of network security, according to Kevin Flynn, senior manager of security technology marketing for Cisco Systems. Fortunately, businesses have many options for protecting their networks.

“Look at security as a process, not just as hardware and software,” advises Flynn. Just as important as the solutions themselves is analyzing how information flows throughout the organization. Companies can then deploy security solutions accordingly.

Integrating and layering security throughout the network and for all devices that access it offers maximum protection.

“Everything on the network should be seen as a potential point of attack as well as a point of protection,” says Flynn.

Cisco Integrated Network Security Solutions help organizations implement end-to-end security. These solutions include the Cisco PIX Security Appliance series of firewall products, as well as integrated security within routers, switches, wireless networking, IP Communications, and other products.

As important as vigilance around network security is today, it will be more critical in the future as organizations plan and deploy network-reliant solutions such as IP telephony.

“The trick to good security is to integrate it into your network today while also building a strong security foundation for tomorrow,” concludes Flynn.

Sophisticated Solutions

Strong network security makes it possible to boost productivity and reduce operating costs. By integrating and layering security throughout a network, your organization can deploy network-enabled operations, such as B2B transactions, wireless networking, and Internet Protocol (IP) Communications, with minimal risks.

The keys to securing the network are keeping current on emerging security solutions and developing strong IT security policies. Some of the current security solutions relevant to B2B transactions include the following:

- **Virtual Private Networking (VPN):** About 65% of the top 3,000 organizations worldwide have implemented VPNs, according to Hurley. A VPN encrypts data transmitted over the public Internet, enabling remote users such as distributors, suppliers, partners, and teleworking employees to securely access a company’s network. Combined with firewalls, intrusion detection, proper authentication, and other security tools, VPNs provide robust, scalable, low-cost security.
- **Secure Sockets Layer (SSL):** The SSL protocol establishes a temporary, private, browser-based, point-to-point connection on the public Internet. Widely used in consumer and B2B transactions, SSL encrypts data as it moves across the Internet but does not protect the records of completed transactions.
- **Digital Certificates:** Similar to electronic identification cards, digital certificates verify the authenticity of a digital signature. Doing so requires a public key infrastructure (PKI), which can be complicated to deploy within an enterprise and even more difficult to facilitate with outside partners and vendors, according to Robert Richardson, editorial director of the Computer Security Institute. Although digital certificates and signatures are “terrific technology,” says Richardson, companies have been slow to adopt their use.
- **XML Key Management Specification (XKMS):** Extensible markup language (XML) is a software tool that facilitates interoperability between applications. XKMS is an emerging XML-based security specification that should make it easier for businesses to trust one another online using PKI, according to Richardson.

Reduced Risk

Companies can take several precautions to make their B2B transactions more secure, including the following:

- Hire a security consultant. Most companies don’t have the expertise to fully implement security, so it’s important to get help from experts who specialize in security, according to Koetzle.
- Ask partners or suppliers to conduct internal security audits. Ask to see the results, suggests Richardson. When conducted properly, an audit will uncover gaps in a company’s security that could put its network—and potentially yours—at risk. One way to conduct an audit is with a benchmarking tool. CIS, for example, provides free, downloadable benchmarking tools that assess operating-system security configurations at various levels.

Defined

- **Firewall:** A set of programs, located at the gateway between the internal network and the public Internet, that protect the internal network from intrusion.
- **PKI:** A public key infrastructure allows users to conduct secure and private transactions over the public Internet with a set of cryptographic “keys.”
- **XML:** Extensible markup language is used in Web applications to create documents that can define, transmit, validate, and interpret data between them.

Next Steps

- View the Cisco SAFE Blueprint for security and VPN solutions, which enables organizations to plan network security effectively.
<http://www.cisco.com/safe>
- Download the free CIS benchmarking tools.
<http://www.cisecurity.org/>

- Get partners’ or suppliers’ data-security policies in writing. Smaller companies often haven’t put their policies in writing, according to Richardson. But larger enterprises—particularly those in regulated industries, such as health care—have security standards to which they must comply and are more likely to have written policies.

Proactive Approach

In the near future, companies will increasingly connect with partners and suppliers to more effectively compete, reduce operating costs, and streamline operations.

“Over the next year or so, B2B transactions will be something that most companies will need to seriously consider if they haven’t already,” says Koetzle. “Businesses will require better, more integrated links with their suppliers and partners. And one of the questions that will come up right away is, How do you secure those links?”

Ultimately, the question is not, How secure are your B2B transactions but rather, How secure is your network and the networks of your trading partners?

iQ Magazine, September/October 2003

<http://www.cisco.com/go/iqmagazine>

SECURITY FOR SMALL AND MEDIUM-SIZED FIRMS: DOES IT MATTER?

BY JOHN N. STEWART

When it comes to security, the world is different for small and medium sized firms than it is for large firms. Smaller firms tend to have limited internal IT resources. Most do not have a Chief Security Officer. Because they generally have smaller budgets, the pressure to save money can be overwhelming. However, all firms with a computer network and an Internet connection have essentially the same things at stake: the reputation, intellectual property, even the very life of the firm itself.

Without an army of experts and a bottomless budget, how can a smaller firm ensure its security in an online world? By thinking about security the right way, and then acting accordingly. The following principles and guidelines will help with this.

Top-level Participation

The first key idea is that top management must believe that security is important. This is true for two reasons. First, security strategy should always be a function of business strategy. Put simply, the purpose of the security function is to enable the safe and uninterrupted operation of the business. This means that understanding the strategy, processes and priorities of the business itself is a pre-requisite for setting security policy and spending.

The second reason is that organizational policy is set at the top. It's an unfortunate fact that no amount of cajoling, exhorting or encouragement from the IT organization can compensate for a lack of interest in security at the executive level. No memo from a systems administrator can replace a CEO's assertion that "Security is very important to us. That's why we do things this way." Top-level involvement ensures the participation of all employees in the security effort, and effectively grows the security team to the size of the company. There is no substitute for executive-level involvement in security.

Proportional Approach

While it is understandable to envy the freedom that comes from a larger budget, it's important to realize that even a large firm must prioritize its security spending, and look for return on investment wherever possible. Fortunately, appropriate security spending tends to scale with the size of an organization. A \$10 million firm should spend about a tenth as much on security as a \$100 million firm.

The key idea is to set security spending proportionate to what is being protected. Much like insurance, there is a certain percentage of an asset's value that it is appropriate to spend in order to decrease the risk of losing the asset, or having its operation disrupted. That percentage will vary with the importance of the asset to the business, and the expected effectiveness of the protection afforded. By understanding its business strategy, and the risks it is willing (and unwilling) to run, a firm can set and apply its security budget most effectively.



Further Reading

For more information on this topic, be sure to see the video on demand interview with John N. Stewart.

<http://tools.cisco.com/cmn/jsp/index.jsp>

Designated Security Expert

When considering ways to improve network and information security, a good question to ask is: “What percent of your organization’s personnel is devoted strictly to security?” Zero is not a good answer. But that is often the answer many firms give. When I speak to smaller firms, they frequently tell me that they don’t have the budget for a security team. My response is that one person, or even part of one person, is a lot better than no one at all.

Who should this person be, and where should she report? Some firms put security in the IT organization, and other put it in the financial organization. Still others have the top security expert report directly to the CEO. But answering this question is actually less important than understanding what the security expert’s role should be inside the organization.

The Security Expert’s Role

First and foremost, the security expert must devote some portion of her time to thinking only about security problems. Allowing security to be “just another thing that IT does” blurs accountability, and with it, the championing for security within a business. Recognizing security as its own discipline is an important step to improving the level of security. Second, the designated expert should have organization-wide authority for security matters. The entire firm should be made aware that she is the “go-to” person for security issues.

In terms of responsibilities, the security expert should identify, based on discussions with senior management and/or a thorough knowledge of the business, the top security risks for the organization. She should then develop plans for reducing those risks to acceptable levels, along with an associated budget and timeline. It is common to determine that a problem can be solved over, say, twelve months with a given budget, but can be addressed in just three months with a higher budget. Senior management must ultimately make these “risk vs. cost” trade-offs as part of the process of allocating all company resources.

Security is a Path not a Destination

Security is a matter of degree, rather than an absolute state. Further, there is no single product, person or policy that can provide security. The right way to approach security is incrementally. Any company can improve its level of security by following a simple, three-step process:

- Develop policies and requirements
- Implement solutions
- Audit the results

This closed-loop process, repeated over and over, will lead to continuous improvement in a company’s security level.

Choose Security Vendors Wisely

So far I have focused on the aspects of security that are internal to an organization. External security vendors also play a very important role.

When selecting security vendors, smaller firms often place too high an emphasis on immediate cost savings, and not enough emphasis on cost of operation. For example, buying mix-and-match equipment from a range of different vendors can reduce the initial cash outlay, but will increase integration costs, and typically result in a decreased level of security.

This is because security is a holistic problem, a problem of the “cracks between components” as much as it is about the components themselves. By sourcing pieces of a security solution from different vendors, the cost-conscious firm suddenly finds itself in the role of security systems integrator. This is a complex and difficult task, made more so by the different protocols, management interfaces, support contracts, and more that each vendor will require it to learn. Secondly, when a security event happens, and they do, calling multiple vendors and coordinating their answers is not what you want to be doing when fighting off an attack.

Greater security and lower cost of operation can be achieved by choosing a vendor that thinks about security pervasively, and provides seamlessly interoperating equipment and software in all areas of the network, including firewalls, internal network components, desktop machines, VPNs and more. In general, fewer vendors leads to less variability and better, more efficient security.

Summary

Firms of all sizes run essentially the same security risks: risks to intellectual property, company reputation, and the ability to conduct business. But small and medium sized firms face the additional challenge of having to address these risks with fewer internal resources devoted to security. This can be overcome by involving top management in security planning, by keeping security strategy firmly tied to business strategy, by designating at least one person to focus on security, and by choosing security vendors wisely. The payoff is higher security at lower cost.

Business Industries & Solutions, September 1, 2003

<http://www.cisco.com/go/business>



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0402R) VM/JSI/04.04