

Securing Your Business Information— Strategies for Outsourcing Security Measures

Information is as important as capital for businesses. No matter what kind of business you're in, networks and digital information underpin your operations. And when networks are compromised or information is lost or misused, your business can suffer serious financial consequences.

Securing data—protecting any form of information that is vital to your business interests and company's well being—is becoming increasingly difficult. All business networks are subject to network attacks, yet not all businesses have the resources necessary to proactively monitor, manage, and keep current with the latest security advances to prevent a network attack from being successful. Now, small and medium-sized businesses, branch offices, and telecommuters can ensure information security using the same techniques that large corporations employ. By outsourcing their network security needs, companies of any size can choose the security measures that make the most sense for their businesses and budgets.

Employing security measures isn't a luxury. It's a necessity. Today, businesses can secure business information with a range of secure network routing platforms from Cisco Systems—and integrate them with security services provisioned and managed by Cisco Powered Network service providers. This overview will help you assess your company's risk and determine the best strategies for managing it using today's secure networking products and services.

Security Breaches—Real or Imagined?

When you think about the average network's complexity, it's no wonder that securing a network is so difficult. Networks have become increasingly complex because they support virtually all of a company's business operations. The need to enable access by customers, partners, and employees also requires that your network be open. However, the trade-off is assuming increased risk to network security.

Growing Risk

Network security threats are multiplying. According to the CERT Coordination Center at the Software Engineering Institute (CERT/CC), the number of reported network security incidents has almost tripled—from 21,756 in 2000 to 73,359 at the end of Q3 2002 (source: <http://www.cisshl.com>). And these are only the incidents reported—the estimated number of actual breaches may be double these figures (CSI/FBI Computer Crime and Security Survey 2001).

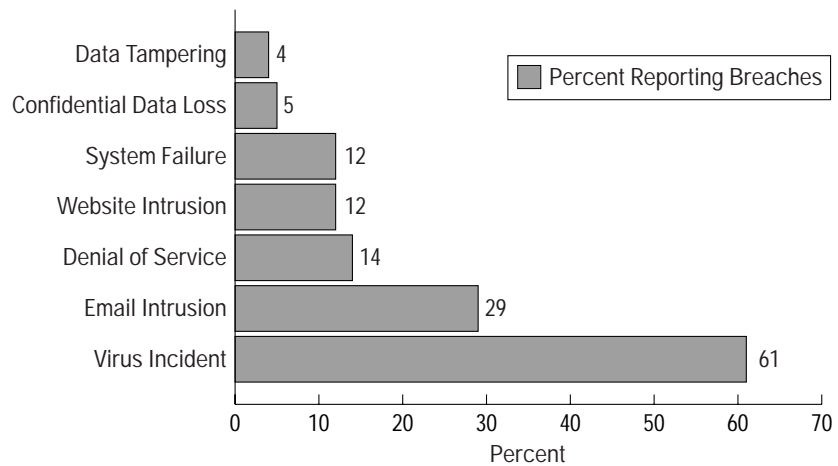


Figure 1
Security at Home



The types of attacks occurring are also becoming more sophisticated and potentially devastating. While the majority of network attacks are viruses, intrusions (e-mail and Web site), automated attacks (denial of service), and data tampering cases are increasing.

Figure 2
Frequency of Security Breaches

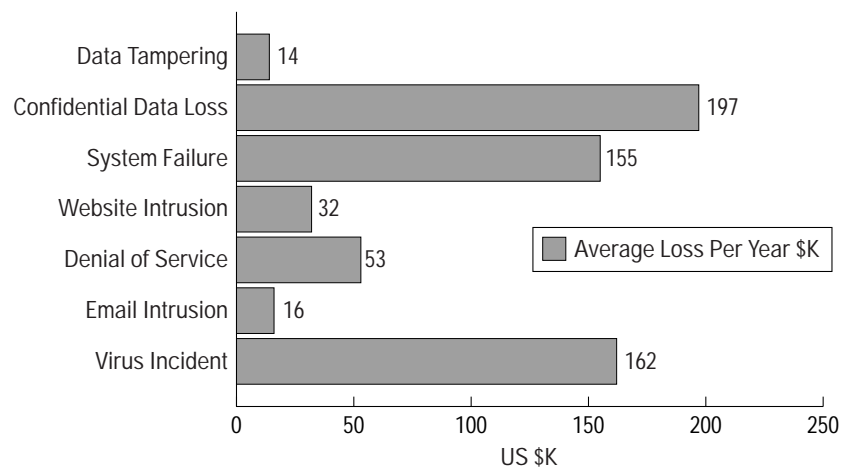




The Cost of Breaches

These breaches are more than annoying. They're expensive. Even though virus attacks are among the less serious attacks, they are the second most costly to remedy and the most common security breaches for small and medium-sized businesses. Data loss, data tampering, and system failures can be even more costly because they can be harder to detect and cause lost opportunities, lost competitive advantage, and long-lasting damage to customer relations.

Figure 3
Cost of Security Breaches



What's a Business to Do?

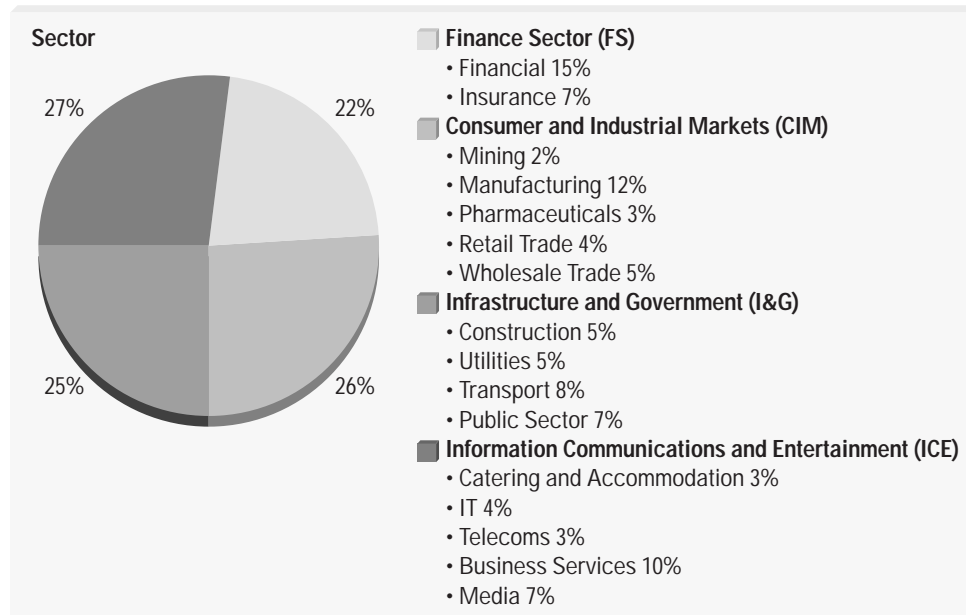
Early network security strategies were designed to build strong walls around the business. Today, however, your network must often connect employees, customers, and partners—making an isolationist strategy obsolete. Instead, security strategies must be smart and dynamic. They must simultaneously permit access by authorized users, identify intruders, prevent intruders from doing damage, and ensure security for a wide range of protocols, data types, and user needs. Achieving this kind of network security coverage requires businesses to commit significant financial, human, and planning resources. And because of the cost and difficulty in building in-house solutions, many companies need other options.

Turning to Experts Through Outsourcing

Increasingly, businesses—and small businesses in particular—are choosing to outsource their network security measures. The Gartner Group estimates that managed security services will grow at 30.6 percent compound annual growth rate (CAGR) through the year 2005. Similarly, The Yankee Group estimates that service provider revenues for managed security services will reach almost US\$2.6 billion by 2005 (*Managed Security Services in Mid-2002: Alive, Kicking, and Evolving*, July 2002). These services include ongoing firewall management and monitoring, virtual private networks (VPNs), intrusion detection systems (IDSs), virus scanning, Web site security assessments, applet scanning, content inspection, and URL blocking. Already, approximately 66 percent of businesses across every sector outsource various aspects of their network security plans, according to the *KPMG Global Information Security Survey 2002*.



Figure 4
The KPMG Global Information Security Survey 2002



Expertise, Cost Effectiveness, Reliability

Companies outsource network security for a number of reasons:

Lack of Internal Technical Expertise

Specialized expertise is required for security solution implementation, monitoring, management, backup planning, emergency response preparedness, ensuring data and system redundancy, and forensic analysis. With this type of expertise in high demand, it's difficult to find qualified people.

Ensuring network security for a business is a full-time job and as a result, only the largest companies can afford the luxury of a dedicated staff required for providing 24x7x365 coverage. Service providers have access to a wide range of skilled technical experts and are staffed around the clock, so business customers can free their own staff to focus on core business objectives and eliminate the need to recruit highly specialized technical help. In addition, many service providers' services are compatible with a company's existing network equipment, making the implementation as seamless as possible.

Cost

The cost of staff is high enough, but a comprehensive network security strategy also demands hardened systems, software, training, ongoing maintenance, and legal expertise. Outsourcing offers cost control and predictability over time, allowing a business to secure its assets with minimal expense and up-front cost.



Service Reliability

Service providers offer service-level agreements (SLAs), allowing a business to balance cost against level of services desired and ensure that service deliverables are met. Businesses that need comprehensive around-the-clock services can be sure to receive them, while companies that only want to outsource portions of their security can do that too. Service providers can quickly deploy solutions for your business, provide a range of support services (such as reporting, for example), and scale your services as necessary.

In addition, service providers have the infrastructure and staff to ensure 24x7x365 monitoring, technical expertise, alerting systems, and reporting mechanisms. Constant vigilance enables rapid response to network intrusions and incidents—ensuring high reliability and greater security.

Determining Risk Levels

Companies considering outsourcing their network security measures can use the following discussion points to determine the level of risk they face. This information can then be used to build an appropriate security foundation, identify threats, and determine the value of information assets. Each company must decide how it wants to manage risk, and then focus strategies and budgets accordingly.

Table 1 Assessing and Managing Risk

Value of Information Assets	Consider the amount and value of customer data, financial data, online commerce revenue streams, intellectual property, research and development data, and supply chain information that crosses the network.
Threats	Estimate the impact of viruses, Web site intrusion, e-mail system intrusion, data tampering, data loss, system failure, network downtime, denial-of-service attacks, unintentional misconfigurations or data disruption, and cost of restoring systems, business, and the company's reputation.
Vulnerabilities	Determine how many network components, operating systems, connections to other networks, and other pathways exist into your network. These can include wireless access links, untethered devices, remote sites, and links to outside suppliers.
Probability	Consider how many breaches have already occurred, and how likely they are to occur.
Existing Controls	Identify firewalls, intrusion detection, encryption, access controls, and other network security measures already implemented, in conjunction with the frequency with which they are monitored and updated.
Residual Risk	The business can decide to accept, transfer, or mitigate risk by implementing new policies and procedures or technical controls.



Finding a Security Service Provider

Because network security issues rank near the top of major business concerns, many service providers are expanding their services to meet the needs of a wider range of customers. These are the primary providers of managed security services today. Your business may already have established relationships with one or more of these providers, and it would be worth evaluating their offerings first.

- *Systems integrators*—Large enterprises that outsource IT operations may be able to add managed security services to their existing contract.
- *Service providers*—Many service providers will manage security gateways (firewalls, for example) on the end of a connection they provide. Hosting providers may already provide basic network security services around the servers they host in their data center, as well as enhanced offerings.
- *Consultants*—Some consultants specialize in security services and offer a complete full range of services, both on site and remotely.
- *Network security product vendors*—Companies that deliver security hardware and/or software solutions sometimes provide technical services when a business deploys their products. For example, the vendor may provide outsourced monitoring services if a company deploys its intrusion detection service.

Outsourcing Your Network Security Strategy

The range of network security services that can be outsourced is broad—from basic managed firewalls and dedicated Internet access to comprehensive managed strategy, policy, and implementation services. Many providers can tailor a menu of services to meet your specific business needs. After assessing your company's needs and risk management strategies, one or more of the following services may enable you to achieve your goals.

- *Access control services*—Controlling access to networks and information usually takes the form of passwords and authentication policies. A service provider can help you establish access controls and provision authentication policies if you don't have any in place, or scale your existing controls.
- *Firewalls*—Firewalls can be one or more systems that enforce access control policies between two networks. Firewalls are primarily designed to keep unauthorized intruders out of your network while still allowing you to easily use all of the network features and capabilities. The firewall enforces a policy—a set of rules established to determine what kinds of traffic are allowed to enter and leave the network it guards. The firewall configuration imposes its policy on all devices behind it, so configuring a firewall properly is critical to keeping unwanted traffic out without limiting access and capabilities to authorized traffic. Managed firewall services involve updating the configuration and software of the firewall and monitoring its activity logs to determine network attack levels.
- *Intrusion detection systems (IDSs)*—These systems monitor traffic and alert network managers to attempts at unauthorized access. Host-based IDSs monitor systems or application log files, responding with an alarm or countermeasure when a user attempts to gain access to unauthorized data, files, or services. Network-based IDSs monitor network traffic to identify traffic patterns that would indicate a denial-of-service attack or other unusual activity. Managed IDS services respond to alarms that IDS nodes generate to stop an attack as it occurs. Service providers can update the sensors as new attack signatures are developed and can perform in-depth threat analysis across a company's entire network.
- *Virtual private networks (VPNs)*—A VPN allows an organization to have its own “private network” using authenticated, secure connections. These secure connections are established as needed to allow employees, partners, and customers secure access to a corporate network. VPNs are an important part of a layered security



strategy, and other security solutions can augment their capabilities. Managed VPN services establish IP Security (IPSec) and/or Multiprotocol Label Switching (MPLS) connections to securely interconnect geographically separated networks across a public network. This permits your business to use cost-effective public networks while minimizing transit security concerns.

- *Content filtering*—Content filtering services can monitor network traffic down to the packet level to identify and prevent harmful or unauthorized access to a company's secure network. Your company establishes the rules that determine which types of traffic, which users, and which kinds of data are allowed in. The service provider enforces these policies.
- *Managed antivirus protection*—Service providers can provide network-wide antivirus protection, eliminating the need for your company to install, manage, continually monitor, and update rapidly changing network security software.
- *Encryption*—Encryption protects data in transit and usually involves creating and sharing a secret key for encrypting and decrypting messages. A public key infrastructure (PKI) enables Internet users to securely exchange data and money over the network. A series of public and private cryptographic key pairs is issued by a trusted authority and used to encrypt and decrypt messages as well as authenticate users. A number of products enable companies to implement a PKI, or service providers can both implement and manage a PKI.
- *Physical network security*—Physical network security is achieved through a wide range of measures taken to ensure that access to the network's actual physical components is restricted to authorized people. For example, secure data centers may have fingerprint or retina scanners to authenticate staff members, video cameras to monitor people coming and going, and other ways of ensuring that only authorized people can access network devices. While not frequently offered through network service providers, physical network security should not be overlooked when considering overall network security.
- *Traditional outsourcing*—Businesses can outsource full security lifecycle management services. Once implemented, the service provider can establish service-level agreements (SLAs) and monitor activity. Complete services can include provisions for physical plant security, device management, 24x7x365 monitoring, and emergency response.
- *Remote management*—Organizations can outsource managed network security offsite, through remote management services. These services can manage and monitor network devices, hosting devices, point solutions, firewalls, and anti-virus solutions from a service provider's central location. This eliminates the need to have non-employee staff on your site and can often be more cost-effective.
- *Network security strategy and policy services*—Many companies need help in assessing their risks and establishing risk management tactics. Service providers can offer assistance with vulnerability scanning to identify weaknesses, risk assessment, policy development, security infrastructure design and implementation, administration and log management, emergency response, compliance, and business continuity planning.

Managing the Outsourcing Process

As with any strategic business decision, your company should follow best practices in defining requirements, evaluating different providers, conducting due diligence, and fully defining how your company and the service provider will integrate roles and responsibilities. It's also important to have an independent organization audit your security service. Outside testing can uncover overlooked vulnerabilities and contribute to a strong security implementation.



Securing the Enterprise

Cisco provides a range of secure networking platforms designed to ensure that small and medium-sized businesses can improve internal information security and at the same time take advantage of advanced managed security and VPN services available from service providers. From the central offices of large service providers, through critical access points to customers' premises—Cisco can extend network security features to businesses of any size.

Cisco IOS Software—The Foundation

Cisco IOS[®] Software is the cornerstone of a secure, multiservice-enabling network. The Cisco IOS Software platform embeds support for multiple network security services, including VPNs, firewall services, intrusion detection capabilities, and quality of service (QoS) for voice and video traffic. With these services, businesses using Cisco networks can ensure end-to-end secure networking—even extending to integration with Cisco Powered Network service providers. New enhancements to Cisco IOS Software include:

- Ability to ensure nonstop secure communications for critical business applications
- Dial backup support on new edge routers to enable secure communication in the event of a broadband connection failure
- Expanded intrusion signature support, including both atomic and compound signatures
- Increased router performance with minimum-impact firewall and IDS services
- Support for Advanced Encryption Standard (AES), the most recent encryption standard

Secure Routing Platforms for Every Business

New and enhanced Cisco routers include advanced capabilities that are normally only found on large, high-end routing platforms. These capabilities ensure secure network services all the way to the edge of the network, enabling even the smallest businesses to take advantage of advanced IP services delivered by leading service providers.

Cisco SOHO 90 Series

Cisco SOHO 90 Series routers deliver outstanding routing performance and support dual Ethernet connections. These small-office/home-office (SOHO) routers include an integrated firewall, a 4-port 10/100 Ethernet switch, IPsec VPN capabilities, out-of-band management, and dial backup. The Cisco SOHO 97 routers are additionally optimized for ADSL broadband connectivity.

Cisco 830 Series

Cisco 830 Series routers deliver the same features as the Cisco SOHO 90 Series plus integrated intrusion detection with URL filtering, hardware-accelerated VPN capabilities, and QoS for voice and video traffic. The Cisco 837 Router is also optimized for ADSL broadband connectivity.

New Acceleration Modules

Cisco has also introduced new acceleration modules for Cisco 2600, 3600, and 3700 series branch-office routers. These modules can increase VPN throughput by five to ten times while decreasing CPU use by half. Support for the new AES encryption standard is also integrated in addition to Layer 3 compression. Acceleration modules can increase bandwidth at branch offices, enable businesses to take advantage of new managed services, and extend the life of already-deployed access routers.

New Modules for Catalyst Switches

Versatile Cisco 6500 Catalyst® switches can now be expanded with a range of high-capacity modules that include IPSec VPN and network security features. A new Firewall Services module can support 100,000 connections per second with a throughput capacity of 5 Gbps. Each Cisco Catalyst 6500 chassis can support up to four modules for a total throughput capacity of 20 Gbps. The module also supports stateful failover for increased resiliency. A new IPSec VPN Services module will support up to 8000 simultaneous tunnels and encrypted throughput of 1.9 Gbps. The versatile Cisco Catalyst 6500 can satisfy the most demanding for secure converged services—from the wiring closet to the WAN edge.

Secure Your Company's Information—and Gain Peace of Mind

No network is immune from attack. However, you can protect your company's vital interests from harm with a well-planned risk management process. You can also cost-effectively implement a solid network security foundation with Cisco secure routing platforms and managed security services. To learn more about Cisco secure network solutions, visit:

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



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: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.
(0208R) KW/LW3840 11/02