



WHITE PAPER

TOP FIVE SECURITY ISSUES FOR SMALL AND MEDIUM-SIZED BUSINESSES

Cisco delivers Self-Defending Networks tailored for small and medium-sized businesses.

SUMMARY

Small and medium-sized businesses use the Internet and networked applications to reach new customers and serve their existing ones more effectively. At the same time, new security threats and legislation puts increased pressure on business networks to be reliable and secure. Cisco® delivers comprehensive, affordable, integrated security solutions tailored for small and medium-sized businesses that help ensure business continuity, maintain customer privacy, and reduce operating costs. Businesses can confidently spend more time growing their business, and less time focusing on network security issues.

BUSINESS CHALLENGES

Today's globally competitive business environment has small and medium-sized businesses focused on expanding their business and improving customer satisfaction while simultaneously controlling costs. Fortunately, the Internet and networked applications have leveled the playing field. Small and medium-sized businesses use their networks to extend their market reach and communicate with their customers and partners quickly and cost-effectively. But swift and agile e-business is a double-edged sword—access can also open up businesses to costly security breaches. It is more important than ever to have a reliable, secure, and available network.

SECURITY ISSUES

According to recent studies, security is the biggest challenge facing small and medium-sized businesses. Ever-changing security threats from both inside and outside the business network can wreak havoc on business operations, affecting profitability and customer satisfaction. Small and medium-sized businesses must also comply with new regulations and laws created to protect consumer privacy and secure electronic information.

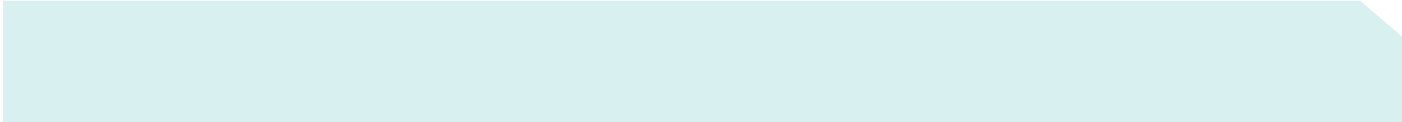
Security Issue #1—Worms and Viruses

Computer worms and viruses remain the most common security threat, with 75 percent of small and medium businesses affected by at least one virus in the last year*. Worms and viruses can have a devastating effect on business continuity and the bottom line. Smarter, more destructive strains are spreading faster than ever, infecting an entire office in seconds. Cleaning the infected computers takes much longer. The catastrophic results are lost orders, corrupted databases, and angry customers. As businesses struggle to update their computers with the latest operating system patches and antivirus software, new viruses can penetrate their defenses any day of the week. Meanwhile, employees spread viruses and spyware by unwittingly accessing malicious Websites, downloading untrustworthy material, or opening malicious e-mail attachments. These attacks are unintentionally invited into the organization, but still cause significant financial losses. Security systems must detect and repel worms, viruses, and spyware at all points in the network.

Security Issue #2—Information Theft

Information theft is big business today. Malevolent hackers break into business networks to steal credit card or social security numbers for profit. Small and medium-sized businesses are at risk because they are seen as an easier mark than large corporations. Protecting the perimeter of the network is a good start, but it isn't enough, since many information thefts have help from a trusted insider, such as an employee or contractor.

* Maritz Research, 2005



Information theft can be costly to small and medium-sized businesses, since they rely on satisfied customers and a good reputation to help grow their business. Businesses that don't adequately protect their information could face negative publicity, government fines, or even lawsuits. For example, new consumer laws enacted in California require any business that suspects customer information has been viewed by unauthorized people must notify ALL their customers. Any security strategy must prevent theft of sensitive electronic information from both inside and outside the business.

Security Issue #3—Business Availability

Computer worms and viruses can drastically affect the reliability of network resources, which in turn affects businesses' ability to respond quickly to their customers; but worms and viruses are not the only threat to business availability. With networks so critical to day-to-day business operations, cyber-terrorists have begun targeting businesses for blackmail, threatening to bring down Websites and e-commerce operations unless their demands are met. These denial-of-service (DoS) attacks send large volumes of traffic to a critical network element, either causing it to fail or to be unable to process legitimate traffic. Once again, the results are disastrous: data and orders are lost and customer requests are not answered. If these attacks become public, a company's credibility is damaged. While most of the publicity surrounding DoS outages has focused on major banks and global 500 companies, small and medium-sized businesses are not immune. They are viewed as less prepared for attacks than large corporations.

There are many other less dramatic but more likely attacks that threaten small and medium business availability and therefore profitability and customer satisfaction. For example, a resource theft attack breaches business computers and networks, using them for illegal file sharing of music, movies, or software. Often, businesses are unaware that a security breach is underway. Meanwhile, their computers and networks are slow to respond to customers, and their unwitting participation in illegal file sharing leaves them vulnerable to lawsuits.

Security Issue #4—The Unknown

With every new advance in computing and communications, some malicious hacker finds new ways to exploit that technology for gain or mischief. New hardware or software releases present a new opportunity. Peer-to-peer networking and Internet Messaging (IM) were still relatively new applications when their users were attacked by malicious code written specifically for them. Mobile phones are now targets of viruses. No one knows what's coming next, but the best defense is one that will be able to easily adapt to future threats without breaking the bank.

Security Issue #5—Security Legislation


Aside from these malicious security threats, new laws and regulations require that small and medium-sized businesses protect the privacy and integrity of the information entrusted to them. The European Union and many individual countries have legislation governing the protection of personal data in the hands of organizations. Countries have also drafted additional laws governing specific information, such as healthcare information. For example, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) requires health care organizations, including every doctor's office, to put safeguards in place to ensure the privacy of health information and prevent unauthorized access. The onus is on businesses to comply with laws and regulations that apply to their business in their markets. Unfortunately, many smaller businesses find their resources only stretch so far. Yet customers want assurance that the information they entrust to businesses is kept private.

All businesses must take steps to secure their business infrastructure, but small and medium-sized businesses in particular require simple, right-sized, affordable solutions. Cisco has developed a security solution specifically for small and medium-sized businesses (SMB) that incorporates the principles of the Cisco Self-Defending Network.

THE CISCO SELF-DEFENDING NETWORK

The Cisco Self-Defending Network is the Cisco long-term strategy to secure business processes by identifying, preventing, and adapting to both internal and external threats. The Cisco Self-Defending Network protects businesses today and adapts to future needs. With Cisco, businesses can protect not only their networks, but also their network investments. The results are improved business processes and substantial savings.

A Cisco Self-Defending Network has three unique characteristics: integration, collaboration, and adaptability. First, it integrates security into all elements in the network, ensuring every point in the network can defend itself from both internal and external threats. Second, these network



elements work together to exchange information to provide additional protection. Third, the network uses innovative behavioral recognition to adapt to new threats as they arise.

The Cisco Secure Network Foundation is a simplified yet comprehensive, cost-effective security solution for small and medium-sized businesses that creates reliable and self-defending networks.

SECURE NETWORK FOUNDATION OVERVIEW

The Cisco Secure Network Foundation allows small and medium-sized businesses to focus on profitability, rather than their network. It delivers consistent, secure services to all users—wired or wireless. Security services are integrated into Cisco routers, switches, and security appliances, helping small and medium-sized businesses to streamline operations and reduce costs.

The Cisco Secure Network Foundation incorporates Cisco Self-Defending Network technology that protects networks today and adapts to handle tomorrow's security needs. Businesses can continue to operate, even while threatened by attack, and can meet both customer and legal requirements for data security and privacy.

Stay Open for Business, Even While Under Attack

With attacks on the rise, businesses and customers need assurance they are protected from the disruption and cost-of-service outages or corrupted data. The proven Cisco Self-Defending Network is a multifaceted approach that protects businesses from the devastating effects of worms, viruses, cyber-terrorists, and other attacks.

Computer viruses, worms, and spyware typically enter businesses via e-mail or IM applications, Web downloads, or file transfers, although sophisticated attacks can enter via mobile wireless services or operating system services. Industry-leading Cisco Intrusion Prevention Systems (IPSs) scan and inspect all incoming traffic in real time, looking for known irregularities that may signal an attack. If an anomaly is detected, a Cisco security appliance rates the severity of the risk and communicates to other security-aware network components. This way, they can stop the threat at the source immediately and prevent it from spreading through the network.

Worms, viruses, and spyware aren't the only way businesses can be attacked. Cisco security appliances use the same traffic and application inspection capabilities to detect and repel DoS attacks, or other attacks so new they don't have a name yet.

Integrated security throughout the business stops known and unknown attacks in real time, and communication between network components allows them to adapt to changing security conditions. These layers of security allow small and medium-sized businesses to continue to respond to customers and stay open for business even while under attack

Maintain Customer Privacy

A Cisco Secure Network Foundation uses many tools to keep customer information from unauthorized users inside or outside the business. Virtual private networks (VPNs) allow small offices and traveling workers to communicate with each other and their head office in complete privacy, even when using the public Internet for transport. The highest user authentication standards ensure only valid users can access the VPN network. Strong encryption technologies make the data unintelligible to anyone attempting to intercept VPN communications across a public network.

Firewall and IPS at every network entry point helps stop worms, spyware, or hacker attempts from penetrating the business network to steal information. Firewalls are also useful in preventing internal users from accessing sensitive information. For example, internal firewall policies can prevent unauthorized employees from accessing finance, human resources, or accounting computers, or from viewing their traffic. Virtual LANs (VLANs) allow businesses to further segment internal communications within their organization. Sensitive financial or customer information can be placed on its own VLAN, logically separate from employee LANs.

The Cisco Secure Network Foundation helps businesses meet legal requirements for the security and privacy of customer information by protecting the network from security breaches or unauthorized intruders from inside or outside the network.

Control Costs

The Cisco Secure Network Foundation helps small and medium-sized businesses control costs in two ways: first, by avoiding the unnecessary costs associated with security breaches; and second, by using multifunction, affordable integrated security components that grow with businesses as their needs change. Integrated security simplifies network management and maintenance costs, reducing the total cost of network ownership.

Network security breaches have both obvious and hidden costs. For example, many security breaches, such as relatively innocuous viruses, cause little damage, and the obvious costs associated with them are the time and resources spent cleaning them off infected business systems. Costs rise with the number of infected systems, making protection and quick detection a money-saving endeavor. Less obvious costs include work time lost while employees' infected computers are being cleaned. Examples of hidden costs include lost opportunities, lost customers, diminished business reputations, or legal costs associated with security breaches. These costs, while less common, can be very large. Last year online crime cost British business £2.4bn**. The Cisco Secure Network Foundation solution helps businesses avoid both the obvious and hidden costs associated with security breaches, reducing business risk, and increasing credibility and customer confidence.

Small and medium-sized businesses do not have the staff resources or capital budgets to deploy and maintain complex security solutions. The Cisco Secure Network Foundation is secure, reliable, and simple, reducing their total cost of network ownership so organizations can focus on their business, not on their networks. It easily adapts to changing business needs and security conditions, making sure costs stay in line with business growth.

Building a Secure Network Foundation

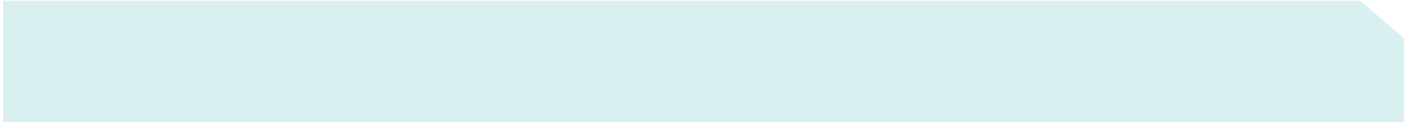
The Cisco Secure Network Foundation is built upon two main product families—the Cisco Integrated Services Router (ISR) family and the Cisco ASA 5500 Series Adaptive Security Appliance (ASA). These solutions provide the cornerstones of the Cisco Self-Defending Network for small and medium-sized businesses.

As their name implies, Cisco ISRs combine many functions in a single, reliable, affordable router platform suitable for a one-person office, or a small or medium-sized office. A Cisco ISR does the job of a DSL broadband access router with integrated redundant link, LAN switch, wireless access point, and a wireless LAN switch, all in one device. Since these capabilities can be added to Cisco ISRs on an as-needed basis, they can easily adjust to the changing requirements of small and medium-sized businesses. They also embed many basic security features, including firewall, IPS, and VPN capabilities.

The Cisco ASA 5500 Series Adaptive Security Appliance is a family of high-performance, integrated security appliances based on Cisco proven security technology that react and adapt to protect against known and unknown threats. The Cisco ASA 5500 Series combines best-of-breed firewall, IPS, network antivirus, application inspection, and remote access and site-to-site VPN services. A Cisco ASA 5500 provides the highest level of protection against unauthorized user access, worms, viruses, spyware, and insecure or malicious applications. This single device, integrating market-proven security technologies, is designed for today's small and medium-sized business networks. It is cost-effective, easily deployed and managed, and upgradeable. As new network security threats emerge, user-installed security extensions and upgrades will allow Cisco ASA products to adapt to continue to protect businesses. The Cisco ASA 5500 Series is the perfect choice for deploying at a main office or a branch office requiring comprehensive security.

An optional component in the Cisco Secure Network Foundation, the Cisco Catalyst® Express 500 Series Switch is a smart, simple, secure switch family designed specifically for small to mid-sized businesses. All Cisco Catalyst switches contain security features that detect traffic irregularities and prevent them from overwhelming the switch or spreading to other points in the network. Optimized for data, wireless, and voice capabilities, the Cisco Catalyst Express 500 Switch delivers the reliability and security of Catalyst switches in an affordable form factor that takes only minutes to install. Every Cisco Catalyst Express 500 Switch comes complete with a Cisco Network Assistant, a tool that helps configure the switch by recognizing other components in the network.

** National Hi-Tech Crime Unit



Another optional component, Cisco Aironet® Access Points, provide secure wireless LAN access for small and medium-sized offices. Cisco wireless products extend the same level of security, scalability, and manageability of a wired LAN. Cisco Aironet Access Points support fast, secure roaming when used with Cisco or compatible client devices, enabling authenticated users to roam securely from one access point to another.

Putting It All Together

Excellent, comprehensive service and support is important to the long-term success of any network solution. Cisco SMB Support Assistant is designed to meet the needs of small and medium-sized businesses. It is an easy-to-use, cost-effective support program that resolves issues typically encountered by SMBs, ensuring the network stays available and secure. Businesses can get timely diagnostic and troubleshooting tips and advance replacement of parts. A key component to the program is the Cisco SMB Support Assistant Portal, an online secure portfolio of tools that allows customers to recover passwords, access support documentation, perform network health checks, download software patches, and open technical support cases when needed.

WHY CISCO?

The Cisco Secure Network Foundation for small and medium-sized businesses keeps business processes running, makes sure customer information stays private, and controls costs associated with maintaining an available, secure, Self-Defending Network. In turn, this increases customer confidence, maintains or increases employee efficiency, helps businesses meet legal requirements, and lowers the total cost of network ownership.

The Cisco Secure Network Foundation is one of a series of intelligent Cisco SMB Class solutions designed to improve employee efficiency, support innovative services, improve customer satisfaction, and reduce operating costs. With enhanced capabilities in the areas of voice, security, and mobility and investment protection, Cisco SMB Class Solutions meet business needs now and into the future.

Cisco and its channel partners are committed to providing small and medium-sized businesses with the best possible customer experience. Financing options, award-winning service and support, and personalized training help businesses get the maximum amount of benefit from their Cisco SMB Class solution.

Cisco is a market leader in routing, switching and security, providing flexible solutions to meet business needs now and in the future, allowing for business growth and agility. Cisco's security strategy is based on the Cisco Self-Defending Network, which integrates security into every point in the infrastructure, collaborates to provide additional protection, and adapts to changing network conditions and new security threats.

NEXT STEPS

For more information on the Cisco Secure Network Foundation, contact your Cisco Partner or please visit <http://www.cisco.com/go/smbclass>.

To find a Cisco channel partner, please visit <http://www.cisco.com/go/partnerlocator>.

For more information on financing your Secure Network Foundation, visit <http://www.cisco.com/go/ciscocapital>.



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.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 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 Website at www.cisco.com/go/offices.**

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 © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R) 205364.1_ETMG_KL_9.05