CISCO

White Paper

Top Five Security Issues 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 have put increased pressure on business networks to be reliable and secure. Cisco Systems® 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. Companies can confidently spend more time growing their business, and less time focusing on network security issues.

BUSINESS CHALLENGES

Today's globally competitive marketplace has small and medium-sized businesses focused on expanding their organizations and improving customer satisfaction while controlling costs. Fortunately, the Internet and networked applications have created a more equitable competitive environment. 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 along with a swift and agile e-business, access can also open up businesses to costly security breaches. It is more important than ever to have a reliable, secure, and available network. It is equally important that the network be flexible and scalable to accommodate both future bandwidth needs and advanced services such as wireless or converged voice and data applications.

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 severely impair business operations, affecting profitability and customer satisfaction. In addition, small and medium-sized businesses must comply with new regulations and laws created to protect consumer privacy and secure electronic information.
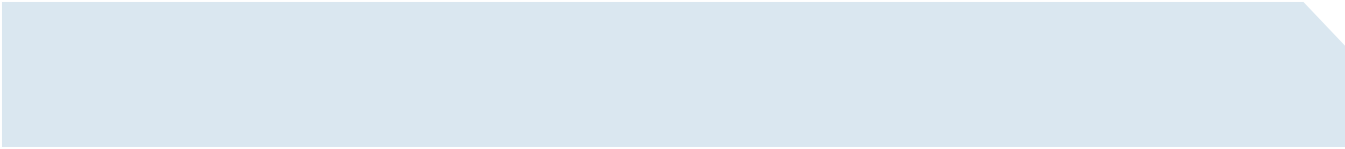
Security Issue No. 1: Worms and Viruses

Computer worms and viruses remain the most common security threat, with 75 percent of small and medium-sized businesses affected by at least one virus in the last year[1]. Worms and viruses can have a devastating effect on business continuity and profitability. Smarter, more destructive strains are spreading faster than ever, infecting entire offices in seconds. Cleaning the infected computers takes much longer, and the process often results in 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 at any time. Meanwhile, employees spread viruses and spyware by unwittingly accessing malicious Websites, downloading untrustworthy material, or opening e-mail attachments. These attacks are unintentionally invited into the organization, but can still cause significant financial losses. Security systems must detect and repel worms, viruses, and spyware at all points in the network.

Security Issue No. 2: Information Theft

Information theft is lucrative. Hackers break into business networks to steal credit card or social security numbers for profit. Small and medium-sized businesses are seen as an easier target than large corporations. Protecting the perimeter of the network is a good start, but it is not enough, since many information thefts are assisted by a trusted insider, such as an employee or contractor.

---

[1] 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 do not 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 No. 3: Business Availability

Computer worms and viruses are not the only threat to business availability. Denial-of-service (DoS) attacks can shut down Websites and e-commerce operations by sending large volumes of traffic to a critical network element and 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.

Many less dramatic but more likely attacks also threaten business availability. 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 No. 4: The Unknown

With every advance in computing and communications comes new ways to exploit that technology for gain or mischief. New hardware or software releases present such opportunities. When peer-to-peer networking and instant messaging were still relatively new applications, for example, their users were attacked by malicious code written specifically for them. Now, mobile phones are frequent targets of viruses. Without the ability to predict what is coming next, the best defense is one that can easily adapt to future threats, and that is affordable.

Security Issue No. 5: Security Legislation

Aside from these security threats, new laws and regulations require that small and medium-sized businesses protect the privacy and integrity of the information entrusted to them. In the European Union, for example, the EU Data Protection Act governs the protection of personal data in the hands of organizations. Nearly every industry has an example of legislation that regulates businesses and requires additional security measures. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare 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. Customers want assurance that their information will be kept private. All businesses must take steps to secure their business infrastructure, but with their limited budgets, small and medium-sized businesses, in particular, require simple, right-sized, affordable solutions.

THE CISCO SMART BUSINESS ROADMAP

The Cisco® Smart Business Roadmap enables small and medium-sized businesses to align their technology plans with their business priorities. It provides a structured evolution to help business proactively keep pace with change. And, it gives business and technical decision makers the confidence of knowing that their immediate technology investments will support their long-term goals.

To guide growing businesses through each development stage – foundation, growth, and optimization – the Cisco Smart Business Roadmap offers a two-phased approach:

- The Cisco Self-Defending Network
- The Cisco Secure Network Foundation

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 and provide additional protection. Third, the network uses innovative behavioral recognition to adapt to new threats as they arise. The Cisco Self-Defending Network is a simplified yet comprehensive, cost-effective security solution for small and medium-sized businesses that creates reliable and self-defending networks.

The Cisco Secure Network Foundation

The Cisco Secure Network Foundation is based on a Self-Defending Network framework. It allows small and medium-sized businesses to focus on profitability, rather than the 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, 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 of corrupted data. The Cisco Self-Defending Network is a proven, 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 instant messaging 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) – available in Cisco security appliances, routers, and switches – scan and inspect all incoming traffic in real time, looking for known irregularities that may signal an attack. If an anomaly is detected, the IPS rates the severity of the risk and communicates with other security-aware network components to stop the threat at the source and prevent it from spreading through the network.

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.

IP Security (IPsec) and Secure Socket Layer (SSL) virtual private networks (VPNs) allow small offices and remote workers to communicate with each other and their main 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. Strong encryption technologies make the data unintelligible to anyone attempting to intercept VPN communications across a public network. Cisco Secure Desktop endpoint security seeks to minimize data such as cookies, browser history, temporary files, and downloaded content from being left behind after an SSL VPN session terminates.

Firewall and IPS capabilities at every network entry point help 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 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 substantial. In 2005, online crime cost British business £2.4 billion[2]. 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, helping organizations reduce their total cost of network ownership so they can focus on their business, not on their networks. The Secure Network Foundation 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 on several Cisco products:

- Cisco integrated services routers
- Cisco ASA 5500 Series adaptive security appliances
- Cisco Catalyst® switches
- Cisco Aironet® access points

These products provide the cornerstones of the Cisco Self-Defending Network for small and medium-sized businesses.

Cisco Integrated Services Routers

Cisco integrated services routers combine many functions in a single, reliable, affordable router platform. A Cisco integrated services router combines the capabilities of a DSL or cable broadband access router with an integrated redundant link, a LAN switch, an IPS or VPN firewall, a wireless access point, and a wireless LAN switch – all in one device. Many of these capabilities can be added to Cisco integrated services routers on an as-needed basis, so businesses can add them as their requirements evolve. Suitable for a one-person office, or a small or medium-sized office, these devices offer an intelligent foundation for future network needs. Businesses can add security, wireless, and data and voice services when needed, without having to make additional capital equipment investments.

---

[2] National Hi-Tech Crime Unit

Cisco ASA 5500 Series Adaptive Security Appliance Business Edition

The Cisco ASA 5500 Series of high-performance, adaptive security appliances is based on proven Cisco security technology that reacts and adapts to protect against known and unknown threats. The Cisco ASA 5500 Series combines best-in-class firewall; IPS; anti-X protection against viruses, spam, and spyware; and remote-access and site-to-site VPN services. The Cisco ASA 5500 Series provides the highest level of protection against unauthorized user access, worms, viruses, spyware, and insecure or malicious applications. This single device is designed for today's small and medium-sized business networks. It is cost-effective, easily deployed and managed, and upgradable. 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.

Cisco Catalyst Switches

Cisco Catalyst switches deliver the features required to offer smart, simple, and secure networks. They are designed to meet demanding security, performance, and reliability requirements. By enabling the convergence of applications on a network, Cisco Catalyst switches enhance employee responsiveness to customers while significantly improving operational efficiency. 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.

Cisco Network Assistant is a free, easy-to-use suite of management tools for simple installation, configuration, network management, and troubleshooting for selected Cisco Catalyst switches. Smartports Advisor is an intelligent configuration tool that automatically detects all connected Cisco devices and recommends preset configurations for the switch port connected to the device. It simplifies network rollouts, freeing businesses to focus on advanced technology deployments. The Troubleshooting Advisor tool automatically identifies potential network issues such as cabling issues and configuration errors and records them in a convenient chart. It also provides problem descriptions and gives users the option to take corrective action with a single mouse click.

Cisco Aironet Access Points

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 Cisco Compatible client devices, enabling authenticated users to roam securely from one access point to another.

Smooth, Reliable Operation

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 small and medium-sized businesses, ensuring the network stays available and secure. Businesses can get timely diagnostic and troubleshooting tips and advance replacement of parts. The Cisco SMB Support Assistant Portal is 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 Smart Business Roadmap 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, mobility, and investment protection, Cisco Smart Business Roadmap solutions can meet business needs both now and in 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 Smart Business Roadmap 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. The company'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. Cisco offers a broad portfolio of products and the Cisco Smart Business Roadmap to help small and medium-sized businesses formulate an intelligent, structured growth path to make the most of their technology investments.

NEXT STEPS

For more information on the Cisco Secure Network Foundation, contact your Cisco partner or visit: http://www.cisco.com/en/US/netsol/ns644/networking_solutions_packages_list.html.

For more information on the Cisco Smart Business Roadmap, contact your Cisco partner or visit: http://www.cisco.com/go/sbr.

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

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

Printed in USA

C11-374971-00 10/06