Simplifying Technology:

How to Secure Your Business

Brought to you by the Cisco Innovators Program | www.cisco.com/go/innovators

Securing your business data and systems is a basic responsibility—but it can be a complex challenge. It's a balancing act between giving users access to information and protecting the business.

Whether it's hacker attacks, property theft, employee safety, the loss of customer data, or employees using company information while away from the office—it's a lot to think about.

With good reason: 99% of businesses with fewer than 100 employees have suffered a security breach. Half of them had proprietary information stolen; 82% suffered denial-of-service attacks.[1]

And online threats are only growing more sophisticated.

This guide can help to relieve your worries about risk exposure. It presents simple, affordable ways to protect your business assets while providing appropriate access to information.

In less than 10 minutes you can read this guide and learn:

- **Why** it makes sense to invest in business-class security: The ROI
- **Where** you need security
- **How** a business can do it: The security triad and its technologies
- **What** you can do now to protect your business

[1] AMI Partners research report, "2009-10 U.S. Small Business Annual Market Overview"

Why Invest in Business-Class Security: The ROI

Security gaps are costly. Among small and midsized businesses that experienced data loss or system downtime, 33% lost sales and 20% lost customers.[2]

Business-class security is the level of protection required to minimize business disruption, downtime, and loss. It's priced higher than consumer-class security, and delivers much higher value.

Its return on investment (ROI) typically includes at

[2] Symantec Corp., Rubicon Consulting data published in the Symantec Business Protection Guide, 2010, pg. 2

least two of these four metrics:

1. Reduces the costs of data and property loss, litigation, and business disruption
2. Increases operational efficiency by enabling task automation, digital connections with suppliers and other partners, and employee mobility
3. Improves customer trust and loyalty
4. Increases staff productivity by ensuring the network is available for work

Consider these real-life small-business examples:

A healthcare provider integrated its office network with Cisco IP video surveillance and data storage that includes apps for streaming multimedia. The ROI:

- Reduced risk and equipment costs, and the labor costs for a receptionist
- Increased productivity and security by allowing staff to visually monitor the entire office from any computer
- Improved customers' experience by monitoring the waiting room, and by streaming entertainment videos to patients being treated

A services startup invested in integrated security to entice mobile business customers. Its Cisco Smart Business Communications System with built-in secured Internet access, firewall, and intrusion prevention provides voice, video, and data services. The ROI:

- A competitive advantage due to reliable, fast, and secure connections
- Revenues from secure Wi-Fi access, document management, and conferencing services
- High customer loyalty and trust, from protecting the privacy of data sent over the Internet

A retail business upgraded its sites with Cisco routers that provide fast, reliable data exchanges and virtual private networks (VPNs). The ROI:

- Reduced risk of costly data loss by securely transmitting credit card information, sales data, and IP video surveillance
- Improved productivity with built-in security that simplifies network use for staff, including mobile managers
- Increased operations efficiency by automating tasks and providing managers with real-time sales reports

Where Do You Need Security?

To quickly identify where the risks and security gaps are at your business, answer these five questions:

Y N **Does your business have enough protection against Internet threats?** The most likely threats are malware: botnets, spyware, worms, computer viruses, rootkits, and Trojan horses. Blocking them involves more than running antivirus software on individual computers.

Y N **Do you safeguard your business-critical data**—in laptops, PCs, servers, smartphones, and USB sticks—with secure storage and backup?

Y N **Is the internal business information that employees need to do their jobs** readily available to them—wherever they are working? Do you control who can access specific types of information?

Y N **Are your property and employees** protected by video surveillance?

Y N **When you give visitors Wi-Fi service**—or share applications on your network with business partners—do you control their access? Are you sure that passersby and neighbors cannot use your wireless network?

Wherever you answered no to any question, you do need business-class security.

Who: Your People Power

Before you delve into security technologies, consider who will be using them and how to lead a successful program.

- Favor technologies that are fast and easy for employees and partners to use—so they will use them.
- Create a written network security policy that defines the types of network use that are required, allowed, and prohibited. Model it yourself. The policy should be concise, clear, kept current, and enforced.
- Educate employees on security risks and train them on your policy, informally as needed and more formally at least annually. Use security problems that arise as opportunities to learn and increase awareness.
- Reward employees who exemplify smart security behavior.

How a Business Does It: The Security Triad and Its Technologies

We keep it simple to give you a useful, quick understanding of the essentials of business-class digital security: confidentiality, integrity, and availability (CIA). Around the world, Certified Information Systems Security Professionals (CISSP) base their work on the CIA model.

Cybercriminals aim at the most vulnerable and lucrative targets. For example, mobile devices will be likely targets in 2011, particularly those using the Apple iOS and Google Android OS.[3]

No single technology can meet all security needs. Multiple layers of security software and hardware are required. And everything must be continually reviewed and updated to protect against new threats.

Confidentiality

Keep private information that is on the business's network and devices away from individuals who should not have access.

Technologies for protecting confidentiality include:

- **Identity management** to control which individuals and devices can access the network. Cisco offers multiple layers of authentication technologies.
- **Firewall** to block unauthorized network access from—or to—the Internet. For example, Cisco firewalls use rules to deny unwanted access to your network from the Internet and can stop employees going to file-sharing websites.
- **VPNs** to allow workers at home, at remote sites, or traveling to securely connect to your network. Cisco routers provide a variety of VPNs so you can apply the best levels of security for employees' and business partners' use.
- **Virtual LAN (VLAN)** to segment access within your network. For example, Cisco switches and routers can restrict the use of financial applications or customer files to specific users.

Businesses subject to PCI DSS, Sarbanes-Oxley, HIPAA, or other regulatory compliance are prudent to consult a security specialist, such as a Cisco partner who is a CISSP.

Integrity

Ensure that data on the business network and devices—or in transit—is not lost or altered.

Technologies for protecting data integrity include:

- **Secure storage** to centralize data protection and automate the backup of critical data. For example, Cisco NSS300 Series Smart Storage can protect up to 12 TB of data onsite and offers an integrated online service for offsite backup and recovery.
- **Data encryption** to protect data that is in transit or storage from

[3] Cisco 2010 Annual Security Report

unauthorized access or alteration. Cisco supports extensive encryption standards for wireless and wired network connections.

- **Virus scanning** to prevent malware from entering the network and devices. For example, Cisco security products can scan all of a business's incoming email to block malware.
- **Web security software** to prevent dangerous websites from reaching your data. For example, Cisco ProtectLink Web blocks employee connections to websites known to host malware; it can also block employee connections to non-work-related websites. Automated updates keep the protection current.

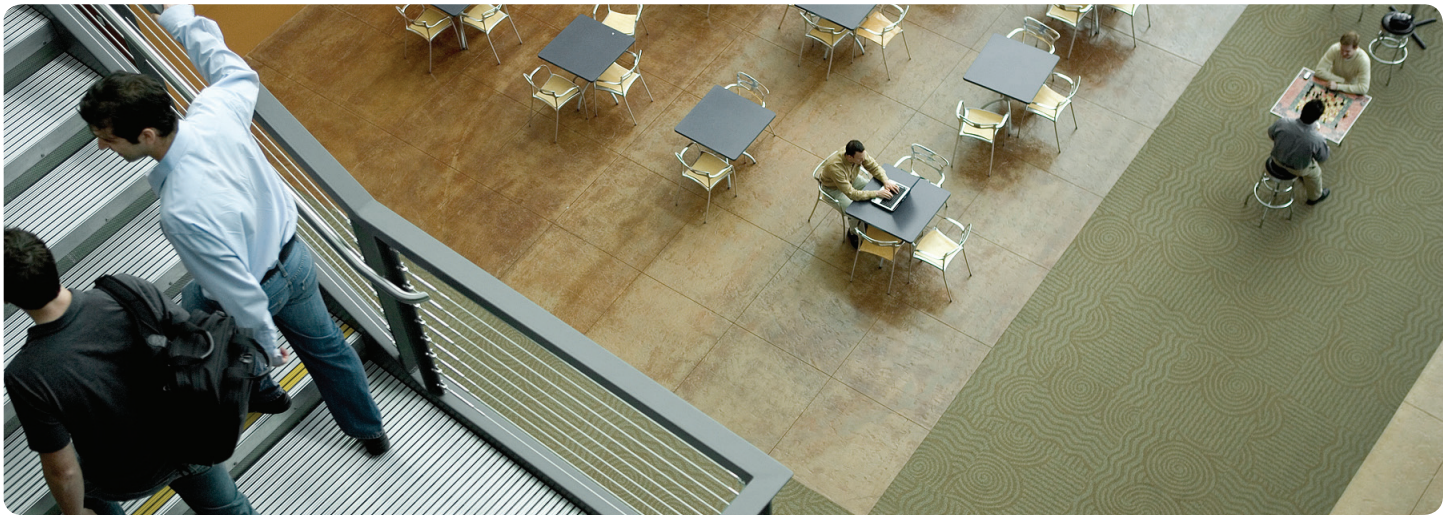
Availability

Provide employees, customers, and business partners with reliable and timely access to the business resources they're authorized to use.

Technologies for protecting availability include:

- **Video surveillance** to guard against the misuse or theft of property. For example, you can monitor your workspaces by using a web browser and affordable Cisco IP video surveillance cameras.
- **Intrusion prevention system (IPS)** to detect and stop malware—including zero-hour attacks—before it does harm. A variety of Cisco security appliances and routers offer IPS.
- **Spam filtering** to remove garbage email before it gets to your network.
- **Secure wireless network** to control access by employees, guests, and passersby who use Wi-Fi devices. For example, Cisco Small Business wireless routers and access points use technologies such as encryption to help keep a wireless network just as secure as a wired one.

CIA technologies—working together—cost-effectively deliver the multi-layer digital security that a business requires.



What You Can Do Now to Protect Your Business

Now that you've learned the basics of business-class security, here are tips to help you decide which security technologies you need:

- Identify the value of the assets in your business (their impact on operations costs and sales, as well as their replacement cost).
- For each high-value asset, assess its CIA vulnerabilities. Now you can prioritize the protection that your business needs most.
- Inventory the security capabilities your business already has, then focus on the gaps.
- Choose solutions that work together; integration improves performance and security, and the productivity of technical staff.

We're ready to help. Cisco Small Business technology can help protect your business with affordable layered security hardware and software solutions that fit your unique needs.

Choose Cisco for technology you can trust to help your business succeed. Count on us for:

- **Business-class products.** Find your Cisco Small Business security solutions online or tap the expertise of a local Cisco Certified Partner or service provider to help identify the right solution.
- **A worry-free investment.** We offer strong product warranties and an extensive product portfolio that can grow with your business. We also frequently offer financing, including leasing.
- **The technical support your business needs.** We provide a full range of support specifically for small businesses.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C02-654570-00

