

Make the Most of Your Money

Five Security Tips

Does social networking breach the walls of your network security? As social media permeate the business world, the need to defend against data leakage and malware grows more urgent.

Good security should not be bad for the budget.

How can your business safeguard its assets—including customer data—at a low cost of ownership? Cisco customer experiences answer the question.

1. Get It Together: Integrate

Combining different security technologies into one system is good for business.

Integrated security can reduce expenses, improve protection, and increase productivity. The 45-employee [Delta View Habilitation Centre](#) got all these results from its end-to-end wireless network security solution.

What needs to be combined? Multilayer network security tools; you may also want to integrate physical security tools.

- A very basic system may combine virtual private networking (VPN), antivirus and antispyware, firewall, and video surveillance tools.
- Stronger systems include tools for encryption and intrusion prevention.

All security tools require management software to install, control, and update them. With a single integrated system that can be managed remotely over the web, you increase control, simplify tasks, and reduce labor costs; you can also outsource the management.

An integrated system protects your investment as your company changes or grows. At [Brown Bear Car Wash](#), the IT manager says, "With our previous system, it was extremely difficult to forecast whether we could add a new project or system to the network. With our current system, we have the confidence that we can add whatever we need, whenever we need it, and it's easy."

2. Simplify Processes for Your People

Good security is more than products. It also addresses social engineering vulnerabilities. How you or your IT staff communicate your security policies to employees, set up and use the security tools, and manage compliance determines the degree of security that your business can attain. A key to success: Keep it simple.

- **Automate.** The 17 employees at [3Marketeers](#) now use built-in Cisco VPN "tunnel" technology to help ensure that files going to and from clients are always protected. This restricts file access to only the individuals authorized to see the file, and enables them to access it whenever they need it, wherever they are.
- **Simplify tool installation and use.** The three-employee [Skye Cosmetic Dental Center](#) chose Cisco video surveillance cameras that feature support for Power over Ethernet. The business owner simply plugged in the cameras with computer cable. Employees now easily monitor the cameras' output from any computer in the office. A simple glance at the computer screen tells them if anyone is in the lobby, and who is coming into or out of offices.

3. Stay Vigilant 24/7

Cybercrime is unrelenting. Don't let your security system fall asleep. Ensure that it is doing all that it can to protect your business.

- **Install the latest security software updates.** This is one of the fastest ways to increase protection. Establish a system, ideally automated by patch management software or a service, that ensures prompt downloading and installation of updates on your laptops, desktops, and IP phones, as well as your network equipment and servers.
- **Use your system to monitor and log events.** Its management software can let you see and record activities. It can also send alarms.
- **Test your security.** Conducting an internal audit, and doing so regularly, tells you where your business is protected and where it's not. A vulnerability scanner can also discover weak points in your network and web applications.

4. Consider the Value of Reliability

Investing in security solutions involves weighing product attributes against cost. An attribute that some buyers tend to overlook is product reliability; later, however, they can incur the costs of system failures.

Brown Bear Car Wash uses Cisco network security for credit card transactions, data reporting, and video surveillance. The chief financial officer discovered that the system's reliability:

- Increased the productivity and morale of employees
- Improved customer care
- Reduced expenses

What are the costs to your business of a security solution that fails? Do you have IT staff with the skills and time required to restore service? Does the vendor provide the online and in-person phone support that offers the help you need? What is the service contract? What is the product warranty?

5. Manage Your Cash Flow with Financing

While investigating how much a security solution will cost from various vendors, look into what financing they offer. Some vendors will let you use their funds to protect your cash flow while you're improving your security.

Next Steps

- [Learn more about Cisco security solutions.](#)
- [Get the security solution you need today with 0% financing.](#)
- [Find an experienced local Cisco value-added reseller.](#)

Questions about Cisco Small and Medium Business Solutions?
Visit www.cisco.com/uk/smb for more details or call Cisco on 0800 015 3003 or 1800 556 670 from Ireland.