WHITE PAPER

Preventing security threats and stopping unwanted activities

How much security is enough?

When it comes to security, there's no such thing as "enough"— it's usually a matter of how much protection you can afford. But remember, security threats are constantly changing, and you may have new security needs as your business grows. Security threats include malware attacks, phishing and spam. There are a number of ways these could occur; all of which can be prevented.

In this guide, we list the security steps every small business should consider.

Related guides:

Protecting your data

Managing data storage

Maintaining compliance

ECSEC confronts security vulnerabilities head on — and secures success

OBJECTIVE

- Prevent network downtime caused by botnet
- Fix numerous other network and server vulnerabilities
- Fill in data backup gaps
- Block spam

SOLUTION

- Enlisted professional help
- Comprehensive technology audit
- Managed security service, including backup, recovery and protection software bundles

RESULT

- An estimated 25% leap in productivity
- Ability to complete project with full capability and resources
- 99.9% of spam eliminated
- Alleviated risks from virus threats, malware and other security issues

For the full story, please see the
Preventing security threats and stopping unwanted activities brochure.

CenturyLink™ Business

How can I start preventing security threats?

The right security strategy for your business will naturally depend on your resources and budget as well as your technology. For instance, if you don't have a website, you won't need to think about outsourced hosting at the moment. In any case, proper security requires layers of protection, not a single-point solution. Follow these steps to minimize security vulnerabilities and prevent unwanted activities.

Step 1: Identify your vulnerabilities

Vulnerabilities may include computer hardware (work stations and laptops), data storage devices, your network, mobile working habits (potentially exposing your business information on a public network), and users who have access to sensitive information.

Step 2: Install anti-virus/anti-spyware solutions on your computers to prevent malware attacks

Network-based solution providers may include Cisco and ISS Realsecure, but software packages are the more typical solution for small businesses, such as Norton, Symantec Security Suite, McAfee, and Adaware. Also, many Internet service providers include these solutions in their packages.

Step 3: Install perimeter security solutions (such as a firewall) to protect your network

There are three types of network perimeter security: a firewall, which prevents unauthorized Internet users from accessing your private network (intranet), via the Internet; intrusion detection system, which will monitor and report on threats to your network; and intrusion prevention programs, which attempt to stop threats as well as report on them.

Installing a firewall can usually be accomplished without professional assistance. McAfee, SonicWall and Norton are some of the companies that offer options geared to small businesses. Also, many Internet service providers include these solutions in their packages.

The more stringent intrusion detection and prevention solutions typically require in-house or third-party IT expertise; check with your Internet service provider for options.

Step 4: Use a spam filter (email firewall) to block unwanted emails

You can either install spam filtering software on your computer or network server, buy a dedicated appliance or outsource spam filtering to an online service provider. Online services such as Barracuda and Postini prevent spam from reaching email inboxes. Software applications like McAfee and Norton will alert you to spam messages that have come through. The software option is typically more budget-friendly, but online services may be more effective and suitable for higher volumes. Also, check with your Internet service provider for options.

When choosing a spam filter, look for a vendor or provider that consistently offers new features and updates to keep up with changes in threats. Buy the best service or product you can afford.

Step 5: Back up your important data regularly and keep it in a safe place

Identify the vital data you need to protect — accounting information, business plans, customer databases, vendor information, marketing documents, etc. Choose from offline and online data backup solutions to ensure the security and availability of your critical business information.

Set a backup schedule and test your solutions regularly.

(See the *Protecting your data* brochure and white paper for more guidance).

> **More new malicious code vulnerabilities were introduced in 2008 than in the previous 20 years combined. That number was surpassed again in just the first half of 2009, with a new threat signature appearing every eight seconds.**
>
> *— Government Computer News, 2009*[1]

CenturyLink™ Business

Step 6: Encrypt your files, hard drives and backup disks

Encryption solutions encode data in transit or data at rest. Data at rest includes information on your hard drive, file servers and backup media. Data in transit includes any information sent over the Internet, including credit card or other payment information.

Encrypt laptop hard drives as well as any desktop work stations.

When choosing an encryption solution, check that it is based on open security standards and read industry reviews of the product. RSA and TrueCrypt are two options to consider.

Remember to secure and encrypt your backups. Otherwise, you're essentially leaving your weakest links open.

Step 7: To make mobile working more secure, set up a virtual private network (VPN)

If your team tends to work from home or on the road using public networks (via Wi-Fi), they're potentially exposing your private network to security threats. Set up and ask them to log in to a VPN, "which is a dedicated communications network that only certain users can access…[It] controls traffic to and from the network rendering it a private rather than a public access."[2]

Many VPNs include laptop monitors that allow users to make only certain approved actions when connected.

SNAP VPN, Untangle, Microsoft and Cisco are some of the vendors that offer VPN options appropriate for small businesses.

Step 8: Automate updates for your applications and security software

Automating updates makes it easier to stay protected as new threats emerge. Typically, you can set automation alerts within security programs as a preference.

Step 9: Use an online website hosting service instead of hosting your business website on your own servers

The hosting service will take care of your website's security needs and provide redundancy, meaning your website can be properly restored if attacked.

Don't be shy about reviewing security and service level agreements before choosing your provider.

You can also ask for their 20 Critical Controls score as a benchmark of their security. (See the "Know your 20 Critical Controls" section in this white paper for more details.)

Put professionals on your side

Managing security needs for a small business can feel overwhelming if you don't have in-house IT resources. And bringing in third-party assistance can actually save you time, money and worry. It's more costly to find out you invested in the wrong solutions (especially if a breach occurs), or you remained vulnerable because you couldn't keep up with security updates.

- **Seek recommendations** for providers trusted by businesses like yours. If you belong to a professional association, ask other members who they use, or do research in online communities related to your business.
- **Ask providers whether they will give you monthly reports** on how many viruses and intrusions have been prevented from entering your systems. Although a third party takes the main burden of security management off your shoulders, they should be accountable to you for results.
- **Check references:** Once you've shortlisted providers, contact other businesses that have used them to ask if they've been exposed to any attacks and whether they're happy with the service and support levels.

[2] Computers designed to process requests and deliver data to other (client) computers over a local network or the Internet.

CenturyLink™ Business

Step 10: Restrict access to your sensitive data to help prevent internal sabotage

Identify the people you trust to access and use critical and confidential information.

Protect sensitive files and databases with passwords that only your key people will know.

Step 11: Draft a security policy and educate your team about security dos and don'ts

Spell out what actions your people should and shouldn't take online and when managing emails.

Step 12: Monitor Internet use

Programs like Untangle allow you to see who's visiting which sites and which of your computers they're using.

Step 13: Review your security methods every few months

Stay aware of fresh security threats and improved solutions by visiting your security software/service vendor websites.

Also, be aware that as your business grows you may need to take new security measures. Include security needs and allocate resources for it in your ongoing business plan.

Know your 20 Critical Controls

It can be difficult to stay aware of all the concerns and tasks that go with preventing threats and unwanted activities. That's where the 20 Critical Controls checklist can help. It outlines and explains "what vulnerabilities…attackers [are] exploiting today, what controls are effective against those attacks, and how you can validate those controls with automated means."[3]

It's also a great benchmark to use if you're considering cloud-based services (online Web hosting or business applications accessed online). Ask providers to share their scores on the 20 Critical Controls as part of your procurement process.

Trends to watch

- **Small-to-midsize business (SMB) security awareness is up:** A survey sponsored by McAfee, for example, found that one out of every five SMBs thought an attack could put them out of business.[4]
- **But SMB security action is low:** Three-quarters of SMBs spend five or fewer hours per week on security, and one-quarter of SMBs spend an hour or less.[5]
- **Social challenges:** Malware attacks via social networks and Web 2.0 applications are set to pose a high risk to information security.

20 Critical Controls checklist

Below are interactive tools that can be used for your security activities:

□ Inventory of devices

□ Inventory of software

□ Hardware and software configurations

□ Network device configurations

□ Boundary defense

□ Maintenance and monitoring analysis

□ Application software security

□ Administrative privileges

□ Need-to-know access

□ Continuous assessment

□ Account monitoring and control

□ Malware defenses

□ Limitation and control

□ Wireless device control

□ Data loss prevention

□ Secure network engineering

□ Penetration tests

□ Incident response

□ Data recovery

□ Skills assessment and training

For more detailed definitions of the 20 Critical Controls, see the user-friendly interactive tool at http://www.sans.org/critical-security-controls/interactive.php

[3] "Cloud computing: Is it secure enough?" Alan Joch. Federal Computer Week. June 18, 2009. http://fcw.com/articles/2009/06/22/tech-cloud-security.aspx

[4] Dark Reading, http://www.darkreading.com

[5] Ibid.

CenturyLink™
Business

> **Almost 80% of small and midsize businesses rank detection and prevention as their top concern, above compliance and reporting, according to a SANS Institute and RAS survey released in 2010.**
>
> *— CSO, 2010*[6]

Need more? We’re with you.

Your community representative is always happy to help. You can count on them as a resource for compliance solutions to consider that fit your specific business needs, budget and level of expertise, as well as advice and resources on a range of small business technology issues.

Visit **http://centurylink.com/smb-resources** to contact your community representative, and learn more about how technology can boost your business. You’ll find information sheets, videos, case studies and more.

[6] “Data Protection: SIEM use grows in mid-sized orgs, surveys say.” Bill Brenner, Senior Editor, CSO, June 2, 2010. http://www.csoonline.com/article/595787/Data_Protection_SIEM_use_grows_in_mid_sized_orgs_surveys_say

Service not available in all areas. Contact CenturyLink for details.

CenturyLink™
Business