



INTERNET SECURITY FOR BUSINESS

Bart Swisher, Data Manager Discusses the 5 Step Plan

Operating a business today requires an Internet connection to the outside world; but as just about anyone can tell you, that essential connection also exposes your company to many security problems, liability risks and productivity distractions.

Utilizing the power of the Internet may be a critical process in your company, but without proper planning and understanding, it can cause costly and catastrophic problems for your organization.

Designing a solid plan

No matter the size of your business, the main components for securing your Internet remain the same — only the type and size of the solutions may vary. Always deal with a trusted, reputable reseller who can talk with you about your company and help you find the solutions that best suit your needs. Follow this five-step plan for securing your Internet:

1. **Set a Strong Internet-Use Policy** — A strong and effective Internet-Use policy lets employees know what their responsibilities are when it comes to online activities on company time. You have to determine a company-wide policy that clearly states what constitutes acceptable usage. Educating your employees about security risks via the Internet is important.

Content filtering software lets you control where your employees go on the Web. You might want to filter out hate and pornography sites or online shopping sites. Doing so covers liability issues and creates a more secure, productive environment.

Of course, being able to customize the filter is important because employees must be able to get the information they need to perform their jobs. This can be a daunting task given the broad realm of businesses today and what information they may need to find. For example, an attorney may need to find information regarding a client's online activity in order to gather information related to an offense. Content filtering may block the website or newsgroup that has the evidence needed.

2. **Install Centrally Managed Anti-virus Software** — Anti-virus software that's managed from a single point (i.e., a server) ensures that every PC in the company is automatically scanned for viruses, worms and Trojans, and that they receive regularly scheduled security updates.

Small business owners may run into a dilemma, do they have the staff available that can manage a complex anti-virus solution? A centralized solution is only valuable if you can verify that it is in fact working.

An option would be to locate a reseller that can offer a managed solution that includes monitoring. Many service providers can offer these services on a 24x7 basis and have the ability to maintain the latest tools and techniques

3. **A Firewall with Intrusion Detection Capability** — Hackers have become increasingly crafty when it comes to attacking networks. A firewall is much like a door with a deadbolt, it is only effective when it's locked. Many businesses have either no

firewall in place or a firewall that is not configured correctly. If a virus attempts to open ports in order to allow a hacker access to your network, the firewall detects that this is not authorized and can block the attempt and notify the system administrator.

That's why you want to have a firewall that has intrusion detection capability, it will help the firewall recognize and deflect external threats such as worms and other well-disguised intrusions from gaining access to your network.

4. **Install Host-Based Intrusion Detection** — While intrusion detection at the firewall keeps worms from entering the network, host-based software — intrusion software you install on individual desktops — protects your network from attacks launched *inside* of your network.

If an attack comes from within the network the firewall won't help — it's strictly for defending against external threats. Installing intrusion detection software on individual workstations will help protect your network. Major anti-virus companies — Trend Micro, Symantec and McAfee — offer intrusion detection in the latest versions of their software.

5. **Digital Signatures** — Digital signatures are used to encrypt data between locations or across the Web. They're especially important for companies that need to meet Federal regulations such as HIPAA.

For example, if you're a doctor and you need to communicate via e-mail with a specialist about a particular patient, you can use a digital signature to secure the patient's data so that no one but the specialist can access it."

Digital signatures are more costly than the other four steps mentioned here. They require people to manage the encryption keys, but small businesses without the in-house resources can outsource the task to a third-party company like Verisign.