

Building Better

Fences



Legal administrators in small and mid-size law firms should take several rudimentary yet vital steps to ensure effective technological security.

In his famous poem "Mending Wall," Robert Frost wrote, "Before I built a wall, I'd ask to know what I was walling in and walling out." It was clear that he didn't agree with his unthinking neighbor's refrain that "Good fences make good neighbors."

In the world of data security, it is indeed important to know what you are walling in and walling out, but it's also apparent that some barriers are needed to protect the confidentiality of law firm data. Fences separate areas so that something (or someone) is kept inside and/or something (or someone) is kept outside.

What can legal administrators do to help secure their firms' information in similar ways? A fence around your office won't keep "hackers" from attacking your data, but if the fence is well constructed, they may rattle the fence posts ineffectually and turn their attention to less-protected data elsewhere.

The "big boys" have IT staffs that support their computer and communications infrastructures, but how can small and mid-size law firms secure their business environments? Some of the answers are providers here. Ultimately, it is not that difficult to take rudimentary steps in securing your information – and the costs are reasonable, too.

STOPPING COMPUTER VIRUSES

First and foremost, you must install anti-virus software on your firm's computers. Virus, worm and Trojan attacks have increased

exponentially in recent years, and protection is absolutely necessary. Your product choices depend on your working environment. If you have a server or servers, then you should choose products that protect the central devices and manage the connected workstations. Don't forget to select the option that scans your e-mail server, if you have one on your network.

Symantec's anti-virus products are among the most popular, and the server suites come in two versions. The Symantec AntiVirus Corporate Edition is used for server environments where no mail server is present. In contrast, the Symantec AntiVirus Enterprise Edition includes Symantec's Mail Security for those with e-mail servers. Both products install to a central server and manage the connected clients. Virus signature updates are automated, as are scanning and centralized quarantine. Symantec requires a minimum purchase of 10 licenses. Budget approximately \$50 per license for the Corporate Edition and around \$75 per seat for the Enterprise Edition. Both costs include access to technical support and updates for one year. You can also purchase three-packs for \$90.00.

If you are running a peer-to-peer network or have stand-alone computers, then you should purchase the personal edition of Symantec's product. This \$40 version includes a one-year subscription for updates and virus signatures.

SHORTCUT

Legal administrators and others in today's small and mid-size law firms face significant challenges when it comes to technology and ensuring the safety and confidentiality of critical data. In this article, learn several essential yet easy-to-execute steps to maximize tech security in your firm.

NETWORKING 101

Internet connections are essential to all of today's computers – for e-mail correspondence and research as well as software product updates and technical support. If you connect to the Internet via a dial-up connection, you have slower functionality, but you're also at less risk of attacks and compromise than those with persistent connections such as DSL, cable modem or fractional T-1 services. Your risk using dial-up is only when you're connected and goes away after you hang up the phone.

Don't think that you are immune to attack, however, just because you use a modem to connect. A personal firewall is the appropriate line of defense for a dial-up connection. One of the highest rated is Zone Alarm by Zone Labs. The base-level Zone Alarm Pro costs \$40, but it is well worth the investment. If you are running Windows XP with Service Pack 2, then the personal firewall feature of the operating system is also an option, but it doesn't have Zone Alarm's flexibility or other special features.

Don't use dial-up? Persistent Internet connections are better served through the installation of a router. Products from Linksys, Netgear and D-Link are very popular for small office installations. The router will translate the IP address from the outside world to a private address for your internal network. This process, called Network Address Translation (NAT), provides a simplified firewall by "hiding" your internal services. Traffic from the "inside" (a Local Area Network, or LAN) is allowed to exit and return, whereas unsolicited "outside" traffic is blocked.

Higher-end firewall products such as those from SonicWALL or Check Point are also available at costs of \$750 and up. These have all sorts of extra features and are generally deployed for larger networks. The configurations are getting easier; however, a high degree of networking knowledge is needed to take full advantage of the robust features. As a result, these high-end firewall appliances are better left to those firms that have an internal IT staff or outside consultants to assist with installation and implementation.

WIRED OR WIRELESS?

Confidentiality of information is paramount for any network. Should you jump on the wireless bandwagon or "hard wire" your machines together? Wired networks are generally more expensive to install and are not as flexible, particularly with regard to equipment location. Despite the cost and flexibility issues, wired networks are inherently more secure because you know where the two ends of the wire are. Wireless clouds extend into the air and may be viewable to the firm in the next office or building, not to mention wireless hackers on the street in front of your firm's building or in the parking lot.

If you prefer a wireless connection, several critical items should be addressed to protect your data and unauthorized access to it.

- Change the default Service Set Identifier (SSID).
- Change the default identification (ID) and password for management of the Access Point (AP).
- Enable encryption.
- Disable the SSID broadcast.
- Enable Media Access Control (MAC) filtration.

The SSID is a unique set of characters that defines your wireless network. The AP and wireless network cards must have the same SSID in order to connect. Change the default SSID to make it harder for someone to discover your network and establish an authorized connection.

And while it should be obvious that the default ID and password for APs be changed for security reasons, you would be surprised to find out how many wireless clouds are left at their default settings. The default values are well known and posted on many Web sites, so you don't want to retain them.

Enabling encryption for your wireless communication is also critical. Your devices may be able to encrypt via Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) and protect data transmission from prying eyes. The encryption method is enabled by entering a "pass phrase." Make sure that the pass phrase is complex and not easily guessed.

You'll need to configure the pass phrase for each device on your wireless network.

Many free tools allow for "sniffing" of wireless traffic. As previously mentioned, the SSID is the "name" of your network and makes it easy for devices to connect. This means that your neighbor in the next office can "see" your network if you broadcast the SSID. Disabling the broadcast makes it more difficult to find your network and keeps it hidden from those free sniffing tools. After all, you are the one installing the network and know what you called the wireless cloud. If you insist on broadcasting the SSID, why not just hang a sign on your office door telling people that you offer free wireless access?

Most wireless APs can limit connections through a process called MAC filtration. Each wireless device has a unique MAC address, which acts as a type of hardware serial number. This provides the layer necessary to communicate with the appropriate device. You can greatly improve security by configuring the APs to accept communication only from specific devices. MAC spoofing is fairly easy in the wireless world, but a would-be hacker would have to know the SSID, administration values to configure the AP, WEP/WPA key and the targeted MAC address in order to access your network.

While this is all doable, let's face it – if you build a decent fence, you have created a deterrent, especially because there are so many other "unfenced" networks to infiltrate. Why burgle a house with a security system when the house next door has none?

SIMPLIFIED LOG ON AND ACCESS

Do you need a password or user ID for your computer? Can't remember your ID? Totally confused by the massive amounts of passwords to remember? Well, you are not alone. Human beings like to keep things simple. It is a lot easier to just turn on your computer and have it immediately go to the desktop with instant access to all of your information and applications. Remember: It may be easy for you when you power up in the morning, but it is equally as easy for the evening cleaning crew or other guests in your office.

If you are running Windows 98 as your operating system, don't! Wait a minute. You have a user ID and password for your Windows 98 system. Doesn't that make it secure? Not at all. The next time you get to the log-on screen for Windows 98, press the

escape <Esc> key and watch how easy it is to gain access to your computer. Now would be a good time to replace the old system and get Windows 2000 or XP.

Make sure that you require user IDs and passwords. In addition, change your password on a periodic basis – and don't write it on a sticky pad and affix it to your monitor! Turn off the "auto complete" feature of Windows and don't save your password for any application access, such as e-mail retrieval. The auto complete option is accessible by selecting the Content tab in the Internet Options for Internet Explorer under the Tools menu.

Also, don't save your password for e-mail access. Configure your e-mail so that you are prompted for the password whenever you need access to the messages. Use a screensaver password with a "timeout." This will help keep your computer secure if you leave to go to the bathroom or just run out to get lunch. After all, you don't want someone walking up to your computer and sending an e-mail message on your behalf, especially if contains inappropriate material.

PHYSICAL SECURITY

If you work in a small office and have a peer-to-peer network, you can't physically secure the main computer that holds your data. However, if you have a server where the data is centralized, it should be physically secured. This means locking it in a closet or in a room that can be secured. Disgruntled employees are responsible for most security breaches. Physically securing the server will help prevent unauthorized access and possible destruction of your data.

And don't forget about the telecommunications equipment. It is best to have your telephone and data communication equipment under your own control and located in your office space. If your equipment must be installed in a common communications closet, consider installing a locked cabinet (with proper ventilation) to prevent unauthorized access.

TO ENCRYPT OR NOT ENCRYPT

Should you encrypt your files and/or electronic communications? The short answer: It depends. You definitely want to encrypt any sensitive data such as patent documents. Electronic communications are generally not encrypted unless they are very sensitive or encryption is required by your client.

E-mail encryption is fairly simple to achieve. The easiest place to start is by obtaining your own personal digital ID. You can get one from VeriSign (www.verisign.com/products/class1/index.html) for \$19.95 a year. The installation is fairly straightforward and integrates with your browser and e-mail client. Once you've installed your digital ID, you will be able to digitally sign and/or encrypt message contents and attachments. To begin communicating in an encrypted form, you must send your public key to your intended recipients. They will need your public key in order to decrypt any messages you send them.

Many choices exist for encrypting data on your computer or network. Windows 2000 and XP Professional have a built-in encryption method that is very simple to implement. The Encrypted File System (EFS) will encrypt data so that nobody – other than the Windows user that encrypted the file – can

Universal or Command Line Products. Visit the PGP Web site (www.pgp.com) to learn more about its products and their costs.

UNDERSTANDING METADATA

Metadata are data about data. When you create a document, spreadsheet or presentation, certain information about the file is contained within the file itself. This could include such information as the author, number of words, version number, tracked changes and a wealth of other data.

Consider, for example, when you send a client a Microsoft Word document for review and modification. Using the "track changes" feature of Word would make it easy to see the modifications and approve or reject the changes. You certainly wouldn't want the opposing counsel to see this data, yet how many times have you, perhaps unknowingly, provided

A fence around your office won't keep "hackers" from attacking your data, but if the fence is well constructed, they may rattle the fence posts ineffectually and turn their attention to less-protected data elsewhere.

view the contents. Reinstalling Windows with the same user ID does not provide access to the encrypted data, so make sure you back up your private key. For Windows XP or 2000, right-click on the file or folder and select properties. On the General tab, click the Advanced button. Check the box for "Encrypt contents to secure data" and click OK. That's all there is to it. If you encrypt a folder, all files placed in the folder will be encrypted. Once encryption is enabled, it's a good time to back up the recovery key. View the Microsoft Knowledge Base Article – 241201 for instructions on exporting the private key.

PGP Corporation also offers a popular encryption product. PGP Desktop Home costs \$99 and includes the ability to secure messaging and information storage. If you need full click encryption, you should purchase PGP Desktop Professional for \$199.00. Those with servers or needing more advanced features can select PGP

an electronic version of a document that contains information that you wouldn't want shown to someone outside your firm?

Metadata Assistant is a wonderful product from Payne Consulting that integrates with Microsoft Office products. When sending an e-mail message from Outlook that contains an attachment, Metadata Assistant will prompt you to clean the data before transmitting. Of course, you can change the default action to prompt, but it is better left as a reminder, lest you release unwanted data from your firm. Metadata Assistant will clean the metadata from Word, Excel and PowerPoint files.

WordPerfect also saves metadata within its documents. Manual methods exist to reduce the amount of metadata, but the best approach is to convert the document to Adobe's familiar Portable Document Format (PDF) before transmitting.

THOSE PESKY DEFAULTS

One cannot overemphasize the need to change default values for any software or hardware in your environment. We've already identified the default items for wireless APs. Here are a few other places to consider changing the defaults.

- Administrator account name
- Domain name
- Workgroup name
- Outlook Web Access (OWA) port

In the Windows world, the default administrator ID is administrator. Change the default name to something the rest of the world doesn't know. Fortunately, with the advent of Windows 2000 Server, there is no longer a default domain name. In Windows NT 4 Server, the default domain name is domain. However, Microsoft has still held onto defining default workgroup names. The default workgroup name can be WORKGROUP, or you may see MSHOME as the default. Workgroups are used to connect computers in a peer-to-peer environment. Change the default workgroup name to something less well known, especially if you are in a shared office location and interconnect with other computers. As with the SSID for wireless, all computers must have the same workgroup definition in order to see each other and share files or resources.

To change or specify the workgroup for Windows XP, go to Control Panel and then System. If you don't see System, then select Performance and Maintenance, and then select System. Click on the Computer Name tab, and then click Change. Enter the desired workgroup name. Remember that this has to be done on all computers in your peer-to-peer network. To change the workgroup in Windows 2000, go to Control Panel and then System. Click the Network Identification tab, and then select Properties. Enter the desired workgroup name in the workgroup box. For Windows ME or 98, go to Control Panel and then select the Network icon. Click on the Identification tab and enter the desired name in the workgroup box.

If you are running an Exchange server or have installed Microsoft's Small Business Server, some other default values should be changed. Exchange has the ability to remotely access a user's mailbox via a Web browser. OWA uses the default TCP/IP port 80, just like most Web sites. This means that

you have to allow port 80 to pass through your firewall in order to gain access to your e-mail on the Exchange server.

Unfortunately, port 80 is one of the most exploited ports by viruses and worms. The default port for OWA is the same as the default Web site on your Windows server. From the server, go to the Administrator Tools and select the Internet Services Manager. Right-click on the default Web site and select properties. Change the TCP Port value to something other than 80 that's easy for your employees (and *only* your employees) to remember. A ZIP code or last four digits of a fax number are good choices. The firewall will have to be changed to allow the port that you configured for OWA. Assuming that you changed the port number to 9902, you would gain access to your e-mail by entering a URL in your browser that looks something like this: <http://mail.yourdomain.com:9902/exchange>.

SPYWARE AND OTHER PESTS

Virus protection is still the No. 1 item to install, but another form of prevention is quickly becoming the No. 2 requirement. Spyware and adware are invading our computers with increased regularity. The annoying pop-ups can produce merchandise advertising or offensive pornographic images or, worse yet, send personal information from the computer to an external source. These nasty bits of program code can come from the installation of free software such as screen savers and Internet search aids or by merely clicking on a link in a Web page.

Products such as Spy Sweeper and Ad-Aware (about \$40 each) are good for discovering and removing these problems. Note that Ad-Aware is free for non-commercial use only. Enterprise versions are also available for those with server installations.

Finally, install the free Google toolbar (<http://toolbar.google.com>) to augment the pest-scanning products. The combination of Symantec's AntiVirus, Google toolbar and Spy Sweeper's Enterprise Edition will virtually eliminate pop-ups and malicious code.

UPDATE, UPDATE, UPDATE

Keep your operating system up to date by running the Windows Update periodically. This will help with performance issues, but also will patch the operating system for known security vulnerabilities. In addition,

you may want to subscribe to newsletters at Security Focus. You can register to receive weekly notices of security issues by subscribing at www.securityfocus.com/newsletters. Another good source of security notifications is SANS (SysAdmin, Audit, Network, Security). Subscribe to SANS newsletters at www.sans.org/newsletters.

BACKUP AND DISASTER RECOVERY

Finally, whatever you do to improve security for your firm and its technologies, you must also implement some sort of backup method for your critical and confidential data. External USB hard drives, CD/RW and tape are excellent options. Also, make sure you take your backup data offsite. Should you experience a security compromise, flood or just a general meltdown of hardware, your data can be restored. (For more about disaster recovery strategies, see "Ready

for The Worst" in the January/February 2006 issue of *Legal Management*.)

If you follow the protocols cited in this article, you will have ultimately built a sturdy fence to secure your firm's data. Stay ahead of those who might infiltrate your technology by keeping abreast of security developments and periodically reviewing your defenses for needed upgrades. Safe computing requires constant vigilance! ✱

about the authors

Sharon D. Nelson and **John W. Simek** are President and Vice President, respectively, of Sensei Enterprises Inc., a legal technology and computer forensics company based in Fairfax, Virginia. Contact them at sensei@senseient.com, and learn more about the company at www.senseient.com.

LEARN MORE

ALA Resources

These titles are available through ALA's Web site, www.alanet.org/education/mrc/index.asp.

- *E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication*, by Nancy Flynn and Randolph Kahn
- *Minimize Risk: How to Structure Law Firm Internal Controls*, by Joan W. Gleich, updated by Rosemary Shiels
- *The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies*, by Nancy Flynn

The following articles are available in the *ALA Management Encyclopedia (ALAME)*, www.alanet.org/alame.

- "Improve Computer and Network Security Now"
- "Wireless Networks: Are They Right for You?"
- "VPNs (Virtual Private Networks): The Current Standard For Remote Access"

The following articles are accessible via ALA's Legal Management Resource Center, <http://thesource.alanet.org>.

- "Security for Telecommuting and Broadband Communications," by the National Institute of Standards and Technology – Type in keywords "firewalls and network security" in the search engine
- "Protect Your Business Against Disruptions and Disasters," by the International Legal Technology Association – Type in keywords "firewalls and network security" in the search engine

- "Securing the Surf: Do You Know What Your Employees are E-mailing?" by Kevin O'Connor, Brian Klein and Jeanne Coglianesi – Type in keywords "firewalls and network security" in the search engine

On the Web

- *SmallBusinessComputing.com*, "Sensible IT Security for Small Businesses" – www.smallbusinesscomputing.com/webmaster/article.php/3490406
- *eWeek.com*, "Symantec Firewall Appliance Targets Midsize Firms" – www.eweek.com/article2/0,1895,1679912,00.asp
- KnowledgeLeader, "BCM Options for Large and Small Firms" – www.knowledgeleader.com/iafreeweb/site.nsf/content/BusinessContinuityManagementBCMOptionsforLargeandSmallFirms!OpenDocument
- Cisco Systems, "Security in Midsized Firms" – www.cisco.com/web/about/ac123/iqmagazine/archives/q2_2005/midsized_firms.html

On the Shelf

The following titles are available for purchase or download through many online retailers, including www.amazon.com.

- *Firewalls: Jumpstart for Network and Systems Administrators*, by John R. Vacca and Scott Ellis
- *Computer Security Handbook*, by Seymour Bosworth and Michel E. Kabay (Editors)
- *Network Security: The Complete Reference*, by Mark Rhodes-Ousley, et al
- *Physical Security for IT*, by Michael Erbschloe