

Building Better Fences: Security for Small and Mid-size Law Firms

**By Sharon D. Nelson, Esq. and John W. Simek
© 2004 Sensei Enterprises, Inc.**

Robert Frost, in his famous poem “Mending Wall” noted that, “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 there is no question that some sort of 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 you do to secure your firm’s information in a similar way? A fence around your office won’t keep the “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 an IT staff that supports the computer and communications infrastructure, but how does the mid and small firm deal with securing their environment? Some of the answers are here. It is not that difficult to take rudimentary steps in securing your information and the costs are reasonable too.

The First Items on the List

Absolutely the first thing to do is install some sort of anti-virus software on the computers. Virus, worm and Trojan attacks have grown in epidemic proportions of late and protection is absolutely necessary. The choices in products depend on your 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 get the option that scans your e-mail server, if you have one on your network.

Symantec’s products are one of the most popular. The server suites come in two varieties depending on whether there is a mail server. The Symantec AntiVirus Corporate Edition is used for server environments where there is not a mail server 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 is scanning and centralized quarantine. A minimum purchase of ten licenses is required for the Symantec products. Budget around \$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 a year.

If you are running a peer-to-peer network or have stand-alone computers, then the personal edition of Symantec’s product is the proper version to purchase. The version costs \$40 and comes with a one-year subscription for updates and virus signatures.

Networking 101

It is absolutely necessary that today's computers have access to the Internet. Product updates, technical support, e-mail and research are all provisioned via the Internet. There are several choices in securing the connections to the wild, wild Internet.

If you connect to the Internet via a dial-up connection then you're at less risk of attacks and compromise versus those with persistent connections such as DSL, cable modem or fractional T-1 services. Your risk using dial-up is only when connected and goes away after you hang up the phone. However, don't think that you are immune to attack 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 will set you back \$40, but it is well worth the investment. If you are running Windows XP, then the personal firewall features of the operating system is also an option, however it doesn't have the flexibility or features that Zone Alarm has.

Don't use dial-up? Persistent Internet connections are better served through the installation of a router. The 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 is called NAT (Network Address Translation) and provides a simplified firewall by "hiding" your internal services. Traffic from the "inside" (Local Area Network) is allowed to exit, whereas unsolicited traffic from the "outside" is blocked from entering.

Higher end firewall products such as those from SonicWALL or Check Point are also available, but cost \$750 and up. They are filled with all sorts of 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.

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 regards to equipment location. Despite the cost and flexibility issues, wired networks are inherently more secure since you know where the two ends of the wire are. Wireless clouds bleed over into the air and may be viewable to the firm in the next office or building, not to mention "wardrivers" (wireless hackers) on the street in front of your building or in the parking lot.

If wireless is your choice, there are several items that should be addressed at an absolute minimum to protect your data and unauthorized access to it.

- Change the default SSID
- Change the default ID and password for management of the AP
- Enable encryption
- Disable the SSID broadcast
- Enable MAC filtration

What do all of the above bullets mean? The SSID (Service Set Identifier) is a unique set of characters that defines your wireless network. The Access Point (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.

It should be obvious that the default ID and password for the Access Points be changed, but you would be surprised to find out how many wireless clouds are still left at their default settings. The default values are well known and even posted on many Internet web sites.

Enable encryption for your wireless communication. Your devices may be able to encrypt via WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) and protect the data transmission from prying eyes. The encryption method is enabled by entering a passphrase. Make sure that the passphrase is complex and not easily guessed. You'll need to configure the passphrase for each device on your wireless network.

There are many free tools that 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 have the ability to limit connections through a process called MAC (Media Access Control) filtration. Each wireless device has a unique address (MAC), which acts as a type of hardware serial number. This provides the communication 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 jump onto your network. While this is all doable, let's face it – if you build a decent fence, you have built a deterrent, especially because there are so many unfenced networks to infiltrate. Why burgle a house with a security system when the house next door has none?

Simplified Logon and Access

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

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 in the least. The next time you get to the logon for Windows 98 just 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 that clunker machine and get Windows 2000 or XP.

On the subject of user IDs and passwords, make sure that you require them. In addition, change your password on a periodic basis and by all means 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 choice.

In the same vein, 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 screen saver password with a timeout. This will help keep your computer secure if you go to the bathroom or just run out to get something to eat. After all, you don't want someone walking up to your computer and sending an e-mail message out in your behalf, especially if contains inappropriate material.

Physical Security

If you are 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 up in a closet or in a room that can be secured. Disgruntled employees perform the vast majority of security breaches. Physically securing the server will help prevent unauthorized access and possible destruction of your data.

Besides securing any server, 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...That is the Question

Should you encrypt your files and/or electronic communications? The short answer is, it depends. Certainly you would 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. Probably the easiest place to start is by obtaining your own personal digital ID. You can obtain one from VeriSign (<http://www.verisign.com/products/class1/index.html>) for \$14.95 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 recipient. They will need your public key in order to decrypt any message you send them.

There are many choices for encrypting data on your computer or network. Let's start with the simple choices first. 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 view the contents. Reinstalling Windows with the same user ID does not provide access to the encrypted data so make sure you backup your private key. For Windows XP or 2000, right click on the file or folder and select properties. On the General tab, click on 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. Now that encryption is enabled, it would be a good time to backup the recovery key. View the Microsoft Knowledge Base Article – 241201 for instructions on exporting the private key.

PGP is probably one of the most familiar encryption products known. PGP Corporation is now a separate company and no longer associated with Network Associates. PGP Personal Desktop is \$50 and includes the ability to secure messaging and information storage. Those with servers or needing more advanced features would select the Workgroup (\$178) or Corporate (\$281) versions.

Data about Data

Metadata is data about data. When you create a document, spreadsheet, presentation, etc. 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 information. Perhaps you send your client a Word document for their review and modification. Using the "track changes" feature of Word would make it easy to see the modifications and approve or reject the changes. Certainly you wouldn't want the opposing counsel to see this data, yet how many times have you, probably unwittingly, provided an electronic version of a document that contains information that you wouldn't want shown?

Metadata Assistant© is a wonderful product by Payne Consulting and integrates with the 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. There are manual ways to reduce the amount of metadata, but the best approach is to convert the document to PDF (Portable Document Format) before transmitting.

Those Pesky Defaults

It is impossible to overemphasize the need to change any default values for 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 port
- SQL account

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 on to 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 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, there are a couple of other default values that should be changed. Exchange has the ability to remotely access a user's mailbox via a web browser. Outlook Web Access (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, worms and just plain bad guys. 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 and easy for 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 would look something like this <http://mail.yourdomain.com:9902/exchange>.

Pests, Bugs and other Nasty Web Elements

Virus protection is the number one item to install, but there is another form of prevention that is now becoming a requirement. Spyware and adware are invading our computers with increased regularity. The annoying pop-ups can merely 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, Internet search aids or by merely clicking on a link in a web page.

Products such as Pest Patrol and Ad-Aware are good for discovering and removing these pesky critters. Each will cost about \$40 and is a worthwhile investment. Note that Ad-Aware is free for non-commercial use only.

Finally, install the free Google toolbar (<http://toolbar.google.com/>) to augment the pest scanning products. We have found that the combination of Symantec's AntiVirus, Google toolbar and Pest Patrol's Corporate Edition have virtually eliminated the pop-ups and malicious code.

Update, Update, Update

Keep your operating system up to date by running the Windows Update on a periodic basis. 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 <http://www.securityfocus.com/newsletters>. Another good source of security notifications is SANS (SysAdmin, Audit, Network, Security). Subscription to their newsletters is at <http://www.sans.org/newsletters>.

Backup and Disaster Recovery

An entire article can be written about preserving your data through backups and devising disaster recovery plans, but a brief note is worthy here. Implement some sort of backup method for your critical and confidential data. External USB hard drives, CD/RW and tape are some of the options for backup. Make sure you take your backup data off-site.

Should you experience a security compromise, flood or just a general meltdown of hardware, your data can be restored.

Final Words

If you follow these protocols, you will have built a sturdy fence to secure your firm's data. Failure to do so gives the bad guys a "get out of jail free" card. 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!