

## Threats from Within

*By Dave Bilinsky<sup>1</sup>*

### Summary

Security most often focuses on protecting your system from outside threats, but what about the barbarians inside the gate? A significant number of security breaches come from disgruntled employees. Firm liability for unauthorized use of company equipment, such as employees running a side business off your server, can be enormous.

### Contents

1. [Introduction](#)
2. [Password issues](#)
3. [Laptops](#)
4. [File security](#)
5. [Portable storage devices — i.e., floppy disks](#)
6. [Temporary employees](#)
7. [Unauthorized software](#)
8. [Software copyright](#)
9. [Unauthorized use of company equipment](#)
10. [Email encryption](#)
11. [Offsite storage — encryption](#)
12. [Remote access issues](#)
13. [Application service providers \(ASPs\)](#)
14. [Personal digital assistants \(PDAs\)](#)
15. [Wireless access](#)
16. [Web sites of interest](#)
17. [Draft policy statements](#)

---

<sup>1</sup> This paper was presented initially at the 2002 ABA Techshow, held in Chicago in March 2002.

18. [Draft Confidentiality Agreement](#)
19. [Draft Internet and Email Use Policy](#)

## 1. Introduction

When most people think of computer security they tend to think of protecting themselves from “malicious hackers” seeking to invade their system via the internet. While that threat is very real, it overshadows a much more subliminal and oftentimes overlooked threat — that being from those people whom your organization trusts and admits past your security fence into your inner sanctum. Those individuals who already have a password and access privileges to your system can, deliberately or innocently, cause problems for your organization ranging from loss of equipment (and data) to breaches of client confidentiality to the loss of or damage to your entire system. When your organization is a law firm, these problems can mean loss of credibility and community trust, loss of face, loss of clients, media exposure, negligence suits and professional discipline proceedings before your regulatory body.

How large is this problem? Network Computing in an article dated November 27, 2000 (<http://www.networkcomputing.com/1123/1123f1.html>) stated that while 70 percent of all attacks on networks occurred via the internet, according to a FBI/CSI computer-crime report, more than 75 percent of all dollar losses came from internal intrusions. Network Computing went on to say: “The number of security incidents originating from external attacks is definitely on the rise, but the internal attacks are the real financial killers.”

Ethical and legal issues for lawyers and law firms arise in this area with respect to:

- meeting a reasonable standard to safeguard your client’s data,
- supervising and monitoring your employees’ and attorneys’ access to and use of all electronic resources, including property owned or leased by the firm and whether these resources are located at the firm or elsewhere,
- dealing with email communications including harassing, abusive, malicious, sexually explicit, threatening, inappropriate, illegal or offensive email, including cartoons or jokes or chain mail using the office’s email and internet resources,
- complying with all software copyright and licensing requirements,
- vicarious liability arising from someone using your email and internet resources in making postings to newsgroups and chat rooms or viewing inappropriate or illegal material on the web,
- storage and deletion of files on the office network relative to a client’s file, including email, electronic documents, data in evidence analysis programs and databases, email, accounting records, time and billing records, disbursement records, discovery and deposition evidence, data placed on ASPs (application service providers) and group work

## Threats from Within

spaces, data placed with third parties (including on-line storage and data backup resources),

- compliance with all federal and state law relative to legislation against terrorism, protection of privacy legislation, money laundering and proceeds of crime legislation.

Accordingly, this paper looks at the various areas where problems can develop and steps that a law firm can take to guard itself from these inner threats.

## 2. Password issues

There are a number of issues regarding passwords, ranging from the perennial problem of people writing their passwords on a 'sticky note' that is dangling from their monitor to writing all their passwords on a piece of paper that is filed in the desk drawer closest to their keyboard. Another situation has someone who duly records all their passwords in a file on his or her system (that is unprotected) entitled "Passwords.doc." The worst situation is when users have no password at all (they set their password to <enter>!!)

What are the issues regarding passwords?

- Use of someone else's password
- Use of a "guest" or default password
- Insecure passwords
- Non-expiring passwords
- Selecting good passwords
- Detection of inappropriate use of passwords

### 2.1 Use of someone else's password

Your password security is only as strong as your weakest link. When lawyers and staff write their passwords down on sticky notes, desk pads, in calendars, on sheets of paper stored in their desks, in rolodexes (usually under "passwords"), on their PDAs and the like, your system is easily compromised. The same is true with storing passwords in a Word or WordPerfect file on the computer (that is connected to the office network). Accordingly, it is important to set in writing a policy on passwords and how to keep them secure — which usually means stored only in a user's mind. What if you get the objection that today you have to remember SO many passwords that it is impossible to keep them all straight? The answer is a combination of having people choose good passwords (see "Selecting Good Passwords"), in having a password policy for your organization (see the draft Password Policy on the SANS Institute web site ([www.sans.org](http://www.sans.org)) and in having people in the organization take steps to not reveal their passwords or hint at their selection. In general, a good password selection will rely on a long string of upper

## Threats from Within

and lower case characters and non-alphabetic characters that are associated in a password phrase that is easily remembered.

If someone in your organization must grant access to a file then make it clear that the proper way to do this is to establish the user permissions on the file access — not by giving the person the rights to your computer or all files on the network.

Any password system can develop holes if the users are not forced to periodically change their passwords. This is usually done by having both a written policy and by having the system prompt users to reconfigure their passwords after the expiry of a fixed amount of time.

### 2.2 Use of a guest or default password

All organizations have staff that come and go — turnover is only natural and becomes more prevalent as the size of an organization increases. Furthermore, all law firms sooner or later employ temps — who must be granted access to the office system in order to work. In addition, most computer systems come pre-configured with a “default” or administrator password. All of these could lead to problems.

To avoid the problem of someone using another person’s password or a guest password, have your system “expire” all passwords after a set length of time. In this way, the protection is automatic by the ‘delisting’ of passwords on a regular schedule (if someone forgets to disable a guest password or a password assigned to a staff member who has left). Don’t use words such as “guest” or “visitor” for guest passwords!!

Default passwords are those that are ‘built-in’ to most operating systems (and routers and other devices...) at the outset. When I had a security system installed in my home, I was careful to change the password that our installer had set up for us as soon as he had left. Months later he was back to fix a problem and he walked up to the security keypad and disabled the system — while I stood there with a shocked look on my face — how had he managed to figure out our ‘new’ password at the first go? He noticed my surprise and told me, “All these systems have a default password for installers to use...” In other words, anyone with knowledge of the ‘default’ password could easily by-pass my new shiny security system!!! The same situation exists for computer systems — ensure that your IT people change every default password on the operating system and other devices such as routers (how many people realize that such devices contain passwords?).

### 2.3 Insecure passwords

Studies have shown that passwords are notoriously insecure — some contain 3 characters or less or are the user’s login name, the login name in reverse or the two in some combination. One writer has estimated that a cracker can expect to obtain access to between 8 to 30 percent of the accounts on a typical system. How? By trying the user’s login name, the login name in reverse or some combination of the two. Another writer has stated that by trying the 20 most common female names followed by a single digit, by trying a combo of the user’s first name and last

name, the user's login name and a list of 1,800 common first names, up to 50 percent of the passwords on any system can be cracked in 2-3 days. There are other software programs that can be downloaded from the internet that will try to crack passwords using similar algorithms, words from dictionaries and the like. There are also programs available on the internet that will test your password security (see useful web sites at the end of this article).

### 2.4 Non-expiring passwords

The longer any organization is in operation, the greater the number of passwords issued to users. In order to keep the password list roughly equal to the current list of users, have your system configured to invalidate all passwords on a regular schedule (say every 3 months). In this way, passwords connected to people who have left the organization, those who were granted user rights to a part of the system but who no longer need that access and guest and visitor passwords are all invalidated, thereby decreasing your risk of unauthorized password access. Make it part of your Password and Acceptable Use Policy that all users are to regularly change their passwords to secure passwords at least as often as requested (which should be prior to their expiry!).

### 2.5 Selecting good passwords (by David A. Curry, Systems Programmer)<sup>2</sup>

#### 2.5.1 Rationale

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you've chosen. This leaves him no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete.

#### 2.5.2 What not to use

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.

---

<sup>2</sup> Excerpt from: Curry, David A. 1990. "Improving the Security of Your UNIX System." Technical Report No. ITSTD-21-FR-90-21. SRI International, Menlo Park, CA. David Curry is presently with Merrill Lynch's Corporate Technology Group (Vice President and Information Protection Officer).

## Threats from Within

- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

### 2.5.3 *What to use*

- Do use a password with mixed-case alphabetic characters.
- Do use a password with nonalphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

### 2.5.4 *Method to choose secure and easy to remember passwords*

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree" becomes "IXdKKaspdd."
- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples include "routboo," "quadpop," and so on.
- Choose two short words and concatenate them together with a punctuation character between them. For example: "dog;rain," "book+mug," "kid?goat."

Another method to choose a good pass phrase is to think of a line from a song that includes a number (The Music Man said "76 Trombones led the Big Parade"!, for example — TMMs"76TltBP"!), and make the password an anagram from the first or second letter of each non-numeric word in the phrase, combined with the numeral for any numbers. Add punctuation marks to make the password even more difficult to crack.

## 2.6 **Detection of inappropriate use of passwords**

The first step is to look for bypassing of the use of any passwords at all (the <enter> password!) or inappropriate passwords. There are a number of tools that you can use (make sure you inform your users that you will be running a password check as part of your overall computer security system maintenance and get their written permission to do this in advance — for example, by having them read and sign your office Password Policy at the time of employment — see Draft Policy Statements (at [www.sans.org](http://www.sans.org)) or incorporate this into your Acceptable Use Policy).

## Threats from Within

- For Microsoft Windows NT and Microsoft Windows 2000:
  - LC3 — <http://www.atstake.com>: LC3 helps administrators secure Windows-authenticated networks through comprehensive auditing of Windows NT and Windows 2000 user account passwords. LC3 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.
  - Microsoft Personal Security Advisor, — Microsoft Windows NT and Microsoft Windows 2000, [www.microsoft.com/security/mpsa](http://www.microsoft.com/security/mpsa): Microsoft Personal Security Advisor (MPSA) is an easy to use web application that will help you secure your **Windows NT™ 4.0** or **Windows 2000™** personal computer system. Simply press the **Scan Now** button to receive a detailed report of your computer's security settings and recommendations for improvement.

MPSA will scan your system and build a customized report on items such as missing security patches, weak passwords, Internet Explorer and Outlook Express security settings, and Office macro protection settings. More details on the specific tests performed by MPSA are available by clicking on the “Features” menu option above.

For each weakness identified on your computer, MPSA provides easy to understand information on the security issue at hand, how to fix it, and links to additional information about the issue. Once you correct a reported deficiency, you can run the scan again and see the results of the change. Running MPSA on a regular basis will help ensure that your system stays up to date and secure.
- For UNIX:
  - Crack and CrackLib: <http://www.users.dircon.co.uk/~crypto>
  - John the Ripper — Unix, <http://www.openwall.com/john>: John the Ripper is a fast password cracker, currently available for many flavours of Unix (11 are officially supported, not counting different architectures), DOS, Win32, and BeOS. Its primary purpose is to detect weak Unix passwords, but a number of other hash types are supported as well.
- For Novell:
  - Pandora — Novell, <http://www.nmrc.org/pandora>: Pandora is a set of tools for hacking, intruding, and testing the security and insecurity of Novell Netware. It works on versions 4 and 5. Pandora consists of two distinct sets of programs — an “online” version and an “offline” version. Pandora Online is intended to be used for direct attack against a live Netware 4 or 5 server. Pandora Offline is intended to be used for password cracking after you have obtained copies of NDS (from Novell).

## 2.7 Biometrics

Biometrics is a growing area that may surpass password problems by placing a thumbprint or iris scan as the 'password' sign-on procedure. Thumbnail scanners are available for laptops where the threat of theft is particularly high.

For example, there is [www.biolinkusa.com](http://www.biolinkusa.com). BioLink develops, manufactures, and markets advanced fingerprint biometric products. Their solutions form the core of biometric user authentication systems for computer network resources, eCommerce platforms, and physical access solutions. Their products include:

- BioLink U-Match® Mouse — a patented fingerprint scanning methodology integrated into a standard two-button mouse.
- BioLink Authenteon Servers — a high-speed authentication server for LAN, WAN, and distributed networks that searches and matches fingerprint submissions against a large database of users.
- BioLink Software Development Kit (SDK) — a software toolkit that provides developers the ability to design integrated solutions that incorporate BioLink's authentication technology quickly and easily into new or existing software applications.
- BioLink Authentication Center — a secure desktop software application suite that provides logon security and prevents unauthorized access to the desktop, network and domain and is an integral component of their Authenteon solution.
- BioLink WebSDK — a software toolkit that provides web developers the ability to integrate BioLink's authentication technology into web based environments, such as eCommerce sites.

## 3. Laptops

Laptops offer particular problems from a security perspective — they are, by their nature, portable, they usually have dial-in or remote access ability, the files on the laptop are most probably not encrypted or secure (other than the sign-on password — see above), they can be used in non-office environments (such as at home where they are exposed to kids), they have modems or network cards that allow them to be connected to other networks, they have portable data output ability (floppy disks or CD burners), just to mention a few of the risks involved with these useful devices.

With laptops moving in and out of the office, it is most important for the organization to establish a written policy that sets out acceptable use standards (see the related article, *Running a Home Business on the Office Server* (and other Good Reasons to have a Technical Use Policy), which has a discussion and examples of acceptable use policies).

## Threats from Within

In particular, password security needs to be rigorous for laptops. Sensitive files on the laptop should be encrypted or otherwise protected so that if the laptop is stolen or lost, client confidentiality is not lost. Consider using the laptop as a ‘thin client’ — where all sensitive data is stored on the office servers and the laptop offers the ability for the user to work remotely — without any sensitive information being stored on the laptop.

Dial-in security must be of a high standard — consider having the system configured to call the user back at a pre-determined number to avoid the possibility of anyone trying to log directly onto your system.

Those with laptops can be tempted to connect to other networks — either through dial-in access (such as AOL) or by using any of the high-speed data access offered in hotels and meeting rooms. The danger here is that the user can download files with malicious code that compromises the overall system. Having a high-quality personal firewall that is properly configured and up-to-date anti-virus software installed will somewhat ameliorate this threat but not eliminate it. A particular threat is when the user has downloaded an executable file and runs that code on the system.

In the home environment, kids will be tempted to play on the laptop. A proper Acceptable Use policy would make it clear that office property is not to be placed at risk by allowing unauthorized persons such as kids to access the data and the software on the system. Furthermore, there is the risk that unauthorized software could be installed (that may or may not be licensed — in which case the law firm could be open to a copyright infringement problem) not to mention the potential of problems with the introduction of viruses, Trojan horses and other malicious code.

The fact that laptops have floppy drives or CD burners increases the potential for data to be taken off the laptop or downloaded off the system using remote access and distributed to unauthorized parties. Again, an acceptable use policy would cover off the copying and distribution of any data or software installed on the laptop.

Lastly, there is the possibility of theft — not only when the laptop is out of the office but also when it is in the office. Acquiring a laptop lock and cable reduces the risk that expensive equipment (and data) will just ‘develop legs’ in the office.

## 4. File security

There are many issues with regard to file security and internal threats. Sensitive files could be copied onto temporary media or sent via email outside the office — to either intended or unintended recipients. Internal users using someone else’s id and password could delete, copy or alter files, including firm intellectual property. Ex-employees could use undeleted remote access passwords to cause damage or data theft.

## Threats from Within

The unintended transmission of confidential files can be dealt with by having all electronic communications contain a confidentiality statement. The writer's own email contains this statement:

This electronic mail communication may contain privileged and confidential solicitor-client communications and/or lawyer work product. If you have received this communication in error or are not the intended recipient, please delete the communication without using, copying or otherwise disseminating it. Please notify the sender that you have received the message in error. Thank you.

The purpose of such a statement is to be able to maintain a lawyer's claim of confidentiality over the contents of the communication even if a transmission should occur to an unintended recipient.

The intended transmission of confidential information could be authorized or unauthorized. Authorized transmission could be to clients, experts, consultants — those people brought onto a file for the express purpose of assisting with the legal matter. Unauthorized transmission of a file can be dealt with in the Technical or Acceptable Use Policy (see related article — Running a Home Business on the Office Server) and by having all staff sign a Confidentiality Agreement (see Draft Confidentiality Agreement).

The modification of documents in the office can be tracked by having document management software such as WORLDDOX ([www.worlddox.com](http://www.worlddox.com)) installed on the network. Such software can track all modifications to documents and can maintain a "checked out — checked in" system for files, when they were modified and by whom.

An appropriate backup and restore system is warranted in any law office to allow for the restoration of any file that was accidentally or deliberately altered, deleted or modified.

### **5. Portable storage devices — i.e., floppy disks**

Floppy disks and other storage devices allow data and software to be removed from the firm as well as the introduction of software or malicious code into the office network. Data for a client's litigation file could be burned onto a CD-ROM and taken by a lawyer for working at home, at the cottage or at a client's office. It may be appropriate to have such data password protected as well as packaging the CD into a jewel case that states that it is the property of the firm, requests its return if found and maintains a claim of attorney privilege over the contents.

### **6. Temporary employees**

Temporary employees should be granted access rights to the system that are consistent with their duties. Passwords and access rights should be deleted on the termination of their engagement. Prior to being engaged, it is prudent to check to ensure that they have not worked for another lawyer or law firms that are known to be engaged on the other side of any ongoing matters.

Consider having the temporary employee sign a confidentiality agreement as well as the Acceptable Use Policy.

### **7. Unauthorized software**

Sooner or later a staff member may wish to install a game or other software application onto their computer. The firm may not know if the software is pirated or legitimate unless it was acquired using the proper purchasing protocol established by the law firm. Most operating systems such as Windows 2000 allow tiered levels of authorization that prevent all but administrators or “power users” from gaining the ability to install any new software applications. The law firm should carefully screen those granted ‘power user’ or administrator rights to avoid problems. Presumably these rights would only be granted where such rights would be consistent with the performance of the person’s duties for the law firm. Users should be made aware that downloaded software off the web may contain malicious code and attempting to install or run this software is not a permitted or authorized use of the system unless this software has been vetted and approved prior to installation.

### **8. Software copyright**

Every firm needs to maintain controls over software acquisition and licensing. While some packages limit the installation and use via software controls, others do not. The firm needs to maintain possession over the original software disks to prevent their unauthorized use. The firm also needs a software compliance system to track all software installed on the system, to ensure that the firm is complying with all copyright and software licenses. The firm must be able to establish a 1-1 correspondence between all software residing on the system and the licenses, users and permissions granted to the law firm. Mandating the compliance with all software copyright laws is normally part of a firm’s Acceptable Use Policy.

### **9. Unauthorized use of company equipment**

It is not unexpected that staff will make use of the office email system for occasional personal email in the same manner as they make use of the telephone system for occasional personal telephone calls. However, it is in the law firm’s interest to keep such personal use reasonable in duration, to ensure that it does not result in increased costs to the law firm and otherwise complies with the Acceptable Use Policy. Furthermore, staff should be made aware that such email is subject to monitoring and could be the subject of a court order.

### **10. Email encryption**

It is prudent and ethical for all lawyers to gauge the security used for an electronic transmission against the sensitivity of the contents of the communication. There are software tools that encrypt an email communication on the desktop and unencrypt the email on the desktop of the recipient. If the case or communication is sensitive enough, there is the possibility that transmitting an

email unwittingly using standard electronic email may result in it being intercepted, notwithstanding that the intentional unauthorized interception of such communications is most certainly illegal. Clients would not be comforted to know that their private and confidential email could have been read, even inadvertently, by the staff maintaining your ISP or by your internal IT staff.

### 11. Offsite storage — encryption

In January 2002, the following news report was released based on the publication in the Federal Register, Vol. 66, No. 235, Thursday, Dec. 6, 2001 at page 63369:

#### FEDS SELECT NEW ENCRYPTION STANDARD

The federal government has approved a new data encryption standard to safeguard sensitive information in federal computer systems, replacing the now obsolete standard adopted in 1977. The National Institute for Standards and Technology selected the Advanced Encryption Standard (AES), a new encryption technology. There was a four-year competition for the new standard in which experts around the globe attacked the candidate encryption codes to test their security. The winning standard, named Rijndael, was named after its co-creators, Joan Daemen and Vincent Rijmen, cryptographers from Belgium. Rijndael relies on an algorithm that encodes electronic communications by generating random numbers using 128, 192, or 256-bit encryption keys. The previous standard relied on a 56-bit key, which provided for approximately 10,000,000,000,000,000 different keys. By comparison, the new 128-bit keys provide a sextillion times greater number of possible keys (a number expressed by 340 followed by 36 zeros.) The earlier standard was cracked in the late 1990s after researchers developed machines that could recover a 56-bit key within a few hours. According to NIST, assuming that one could build a machine capable of recovering a 56-bit key in one second, it would take that same machine roughly 149 trillion years to crack a 128-bit AES key. Further information may be found at <http://csrc.nist.gov/encryption/aes/>.

Given that the 56 bit encryption has been broken back in the late 1990s, I suggest that any law firm that uses any off-site backup system where the data is hosted on a third-party server (such as ASP internet backup services) should investigate the encryption method (at least on the desktop prior to transmission) and length of the encryption key to ensure that they are complying with a reasonable standard to protect their client confidentiality.

### 12. Remote access issues

There are many issues relating to properly configuring and securing a system for off-site access. There are also many methods for allowing this to occur. For example, you may wish to grant a staff member dial-in access to the office network in order to work from home. You may wish to set up a VPN or frame-relay system (*“An extremely efficient data transmission technique used to send digital information such as voice, data, local area network (LAN), and wide area network*

## Threats from Within

(WAN) traffic quickly and cost-efficiently to many destinations from one port.”) Many software packages are now incorporating the ability for you to produce your own extranet to allow clients to have access to select portions of their file (ProLaw for example) and there are many third-party providers who will host your data for collaboration and group work (litigation preparation) such as CaseShare (see ASPs below). Each remote access ability raises the spectre of not only a hacker trying to “break into” such a system but also a current or ex-employee using a false or “should have been expired” password to breach the security of the system. As previously mentioned, laptops oftentimes have shortcuts for remote access right on the desktop, complete with long-distance charge numbers, PINs and passwords already stored and ready to roll. Remote access should be part of an Acceptable Use Policy.

There is a specific draft Remote Access Policy at [www.sans.org](http://www.sans.org).

### **13. Application service providers (ASPs)**

Application service providers are third-parties that will host your data on their servers and provide access to designated individuals or groups. They can be used in litigation files (to build an electronic ‘war room’ that can be accessed by attorneys, consultants, experts, trial preparation team members and the like), on transaction work (again to host documents that must be seen by a number of people such as in a big mergers and acquisitions file) and so forth. The problem here is not only the ability for an unauthorized person to gain access (a hacker) but also for a person who was granted access to exploit any vulnerabilities in the system. These vulnerabilities could arise from password problems such as staff members that have but no longer need access rights, by granting access rights to non-employees, a person using someone else’s password, or using a laptop or other means to cause damage or to copy files and information.

Like Remote Access Issues, ASPs should be dealt with in a specific ASP policy or dealt with in a comprehensive AUP policy (see specific ASP Draft Policy Statements at [www.sans.org](http://www.sans.org)).

### **14. Personal digital assistants (PDAs)**

Personal digital assistant issues are similar to laptop issues — except that people are somewhat more lax regarding PDA security as compared to laptop security. How many people do you know who utilize a PDA password? The problem can be compounded when a PDA is used to provide wireless access into an office system either via email or other means. Again the security approach is twofold — control the use of these devices to those who demonstrate a business need for them, establish a proper use policy and be vigilant in maintaining the security surrounding how access is granted, such as expiring passwords.

### **15. Wireless access**

Many office networks these days are run on a wireless basis — either for convenience or necessity (I know one firm that has its offices in a designated historic building — running network cabling through the building would be expensive at best. Their solution was to install a

## Threats from Within

wireless network that avoided the whole issue of cabling). I have read many news stories of people ‘cruising’ the downtown areas of New York and Toronto using a laptop equipped with a wireless network PCMCIA card (under \$80) and logging onto networks that do not enable the basic wireless security systems built into the wireless network system.

Even if the security is ‘turned on,’ however, researchers at the University of California at Berkeley have announced that they have broken the security of wireless LAN’s with “inexpensive off-the-shelf equipment.” This adds to the feeling of insecurity for wireless transmissions of all types — not just wireless networks. Specifically, the technology involved was the IEEE 802.11 standard — used by Apple Computer’s AirPort and Lucent Technologies’ wireless PC cards in home and office environments. Of more concern, this is the evolving default wireless protocol and should be in many laptops shortly. This security hole would allow hackers to decrypt an encrypted message or insert messages into the system.

However, Cisco has announced the development of a wireless network framework based on the IEEE 802.1x Extensible Authentication Protocol. This would allow the generation of single-user, single-session encryption keys, essentially producing a new user ID, authentication, key management, and accounting for anyone on a wireless LAN.

Assuming for the moment that you have utilized all the security built into your wireless network, you still face the issue of employees and staff, past and present, who know the security employed on your wireless network and who may access the information when they are not authorized to do so. The following web sites provide further information on security.

### 16. Web sites of interest

The following is a sampling of a few of the many web sites devoted to network security.

Center for Internet Security: <http://www.cisecurity.org>. Includes a scanner for the SANS/FBI “Top 20” security vulnerabilities list. This site offers benchmarking ability to gauge your security implementation. For the first time ever, a large group of user organizations, information security professionals and auditors have agreed upon an operational *prudent due care* security standard for computers connected to the internet.

<http://csrc.nist.gov/> — Computer Security Resource Center, hosted by the National Institute for Standards and Technology.

<http://www.cit.nih.gov/home.asp> — Center for Information Technology.

[http://www.cerias.purdue.edu/coast/archive/Archive\\_Indexing.html](http://www.cerias.purdue.edu/coast/archive/Archive_Indexing.html) — The COAST Security Archive contains several thousand tools and documents on all aspects of security. Searching and finding information in the archive isn’t always easy but they provide multiple ways of searching the database.

## Threats from Within

<http://ciac.llnl.gov/cgi-bin/index/documents> — CIAC Documents provide information on a wide variety of computer and information security topics, with an emphasis on issues of importance within the Department of Energy.

<http://www.alw.nih.gov/Security/security-www.html> — a large collection of links on all topics of computer security.

HFNetChk is a security-patch checker that lets administrators scan their servers — including remote ones — to ensure that they are up to date on all security patches for Windows NT 4.0, Windows 2000, IIS 4.0, IIS 5.0, IE and SQL Server. It is found at:

<http://support.microsoft.com/support/kb/articles/q303/2/15.asp?id=303215&sd=tech>

Microsoft Personal Security advisor. MPSA is a web application that will help you secure your Windows NT 4.0 and Windows 2000 computer system. Go to the MPSA site and press the Scan Now button to receive a detailed report of your computer's security settings and their recommendations for improvement. This is found at:

<http://www.microsoft.com/technet/mpsa/start.asp>

<http://catchup.cnet.com> — C|Net offers Catchup services — these services can not only scan your systems for the latest software updates but can also look for the latest security fixes. C|Net's Security Fixes identifies known vulnerabilities in your software applications and operating system and provides you with the information required to patch the security holes.

Operating system Benchmarks developed by members of The Center for Internet Security (CIS) can be found at: <http://www.cisecurity.org/>. These benchmarks are organized into different levels. Level 1 is stated to be the prudent level of minimum due care. Level 2 is prudent security beyond the minimum level.

Information on password protection may be found at:

[http://www.cert.org/tech\\_tips/passwd\\_file\\_protection.html](http://www.cert.org/tech_tips/passwd_file_protection.html).

Information on detecting intruder detection may be found at:

[http://www.cert.org/tech\\_tips/intruder\\_detection\\_checklist.html](http://www.cert.org/tech_tips/intruder_detection_checklist.html)

## 17. Draft policy statements

There are draft policy statements on the [www.sans.org](http://www.sans.org) web site. Their web site states as follows:

“There is no cost for using these resources. They were compiled to help the people attending SANS training programs, but security of the internet depends on vigilance by all participants, so we are making this resource available to the entire community.”

They are available in PDF and Word formats. The policy statements can be found at:

<http://www.sans.org/newlook/resources/policies/policies.htm>

## Threats from Within

These policies are samples, provided for reference purposes and not as model policies for law firms. These must be modified for any law firm setting to meet its particular needs, circumstances, clientele and practice. In particular, these policies should be considered in light of all relevant federal, state or provincial legislation, including any protection of privacy legislation.

### List of Sample Draft Policy Statements

- Acceptable Encryption Policy
- Acceptable Use Policy
- Analog/ISDN Line Policy
- Anti-Virus Process
- Application Service Provider Policy
- Application Service Provider Standards
- Acquisition Assessment Policy
- Audit Policy
- Automatically Forwarded Email Policy
- Database Credentials Coding Policy
- Dial-in Access Policy
- DMA Lab Security Policy
- Extranet Policy
- Information Sensitivity Policy
- Internal Lab Security Policy
- Internet DMZ Equipment Policy
- Lab Anti-Virus Policy
- Password Protection Policy
- Remote Access Policy
- Risk Assessment Policy
- Router Security Policy
- Server Security Policy
- The Third Party Network Connection Agreement

## Threats from Within

- VPN Security Policy
- Wireless Communication Policy

### **18. Draft Confidentiality Agreement**

This policy is intended as a sample, not a model. It does not and cannot purport to be the best of all possible policies, for the simple reason that any precedent must be modified to meet the needs of your firm, your clientele and your practice. In particular, this Internet and Email Use Policy should also be considered in light of all federal, state or provincial protection of privacy legislation that may at some point extend to law firms.

#### **Sample**

#### **[CONFIDENTIALITY AGREEMENT](#)**

(click on link above for sample policy)

### **19. Draft Internet and Email Use Policy (Acceptable Use Policy) — see also “Running a Home Business on the Office Server”**

#### **Sample**

#### **[INTERNET AND EMAIL USE POLICY](#)**

(click on link above for sample policy)