BY ERIC VAN BUSKIRK

Attorneys are often so busy attending to their clients' legal needs that they may not have noticed the growing importance of good information security practice. That importance stems from many causes.

First, Ethics Opinion 05-04 explains that lawyers have an ethical duty to take reasonable and competent measures to secure their clients' electronic files or communications against loss or inadvertent disclosure.[1] Second, in a stunning development, the United States Attorney General recently announced that the federal government is eavesdropping on the electronic communications between attorneys and clients.[2] Finally, as if that weren't enough, the news is replete with a never-ending stream of stories of hapless institutions whose shares or reputations have diminished in the wake of sloppy handling of their clients' electronic records.[3] Therefore, in the interest of protecting our clients, our reputations and our businesses, the time has finally come to understand and implement proper information security procedures.

If only it were so easy. The reality is that there are some attorneys who only recently have begun to use the Internet and cellular phones. Consequently, the enthusiasm level of some attorneys toward information security has on occasion been lukewarm or dismissive. In some cases, the prevailing attitude has been that, if we have lawyers who are still struggling to use a Web browser and e-mail, how can we expect them to understand firewalls, wireless network security or e-mail encryption?

Unfortunately, there is something appealing about this sentiment. For, conceptually speaking, it is obvious that one needs to know how to use a computer before possibly being able to understand its weaknesses and security requirements. The urge to accept this reasoning should be resisted. Indeed, this attitude is contrary to the Rules of Professional Responsibility, adverse to the interests of our clients and a threat to our reputations and businesses. Moreover, even if an attorney is not yet proficient using technology, it is a safe assumption that his or her partners, subordinates and assistants are using technology to the point that they need responsible guidance or supervision.

This article aims to help Arizona attorneys understand the risks to their clients' electronic files and communications. Toward that end, it sets forth recent legal, political and business developments that should compel Arizona lawyers to improve their commitment to and practice of information security. Having made the case for information security, the article sets forth a brief synopsis of important practices necessary to protect our clients' confidences.

The Landscape

Wiretapping

The need to protect our clients' electronic files and communications derives in part from the activities of our government.

In the name of rooting out terrorists, we have been told the government must covertly, and without warrant, listen to the electronic communications of American citizens, including those between attorney and client. In March 2006, U.S. Attorney General Alberto Gonzales shocked many in the American legal community when he revealed the extent of the government's wiretapping. He said, "Although the [national wiretapping] program does not specifically target the communications of attorneys or physicians, calls from such sources would not be categorically excluded from interception."[4]

The ways in which the government may be listening to attorney/client electronic communications are multifaceted. Communications passing through telecommunication satellites and deep-sea communications cables, including telephone calls, cellular calls, and Internet communications, are subject to interception by Echelon,[5] the global eavesdropping program operated by the National Security Agency. It scans millions of messages daily against key criteria such as telephone numbers, voice patterns and keywords.[6] In addition, leading telecommunications providers have been sued for giving the government direct access to customer databases of communications records.[7] Furthermore, the FBI has proposed "sweeping legislation that would require Internet service providers to create wiretapping hubs for police surveillance and force makers of networking gear to build in backdoors for eavesdropping."[8]

Attorneys who are inclined toward indifference to the government's warrantless activities should understand that locating Osama bin Laden's cave is not the only objective of such wiretapping. For instance, major news outlets have reported that Echelon is used to help certain American companies compete abroad.[9] Moreover, in light of the fact that researchers have identified the drug trade, forgery, fraud, kidnapping, extortion[10] and even copyright infringement[11] as activities supporting terrorism, the universe of attorneys who should be concerned is quite large.

In addition to holding a license to practice law in Arizona, **Eric Van Buskirk** is a Certified Information Systems Security Professional. He has authored numerous articles on computer forensics, digital evidence, electronic discovery and information security. His professional passions include criminal law and estate planning/asset protection. He can be reached at evb@azbar.org.

This article grew out of a continuing legal education seminar presented to the Sole Practitioner & Small Firms Section of the State Bar of Arizona on September 9, 2005.

Information Security 101

Protecting Yourself and Your Clients

Ethics Opinion

In addition to wiretapping programs with global reach, there are also more local reasons to practice good information security. Attorneys can look to Arizona Ethics Opinion 05-04 (the "Opinion") for inspiration and guidance.[12] There, the issue put before the Ethics Committee concerned the nature and scope of a lawyer's duty to protect clients' electronic files and communications from loss or inadvertent disclosure.[13]

In analyzing this issue, the Committee succinctly summarized the rule as required by the Rules of Professional Responsibility (the "Rules"): "To comply with these ethical rules as they relate to the client's electronic files or communications, an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence."[14]

So what are the competent and reasonable steps that attorneys must take in order to comply with the Rules?

The Opinion does not say exactly. It does mention steps that might satisfy the Rules, such as firewalls, passwords, encryption, anti-virus and anti-spyware programs. However, the decision is left to the context and the attorney: "Precisely which of these software and hardware systems should be chosen—and the extent to which they must be employed—is beyond the scope and competence of the Committee. This is the kind of thing each attorney must assess."[15]

For those attorneys whose practices are in need of expertise that cannot be obtained in-house, the Ethics Committee recommends retaining the services of an expert consultant.[16]

Business Missteps

In addition to legal/political reasons to practice good information security, there are important business reasons, as well. To illustrate, several years ago a television news sta-

tion in Portland, Oregon, aired a relevant piece. A local computer forensics company had commissioned the station news team to purchase used computers from several local charities. The news team then turned these computers over to the computer forensics company to see what sensitive data were inadvertently left on the associated hard disk drives. The point of the project was to promote a new data removal software product the computer forensics company had recently released.

The news team's cooperation in the promotion paid off. As anticipated by the computer forensics company, one of the purchased computers formerly belonged to a Portland attorney. Because the attorney had not used proper data removal methods prior to donation, the company discovered a large trove of confidential client information. Although this attorney claimed he had "deleted" all client information from the hard disk drive, the company had no problem "un-deleting" this data. Portland viewers learned how remorseful this attorney was when he appeared on camera, his identity obscured in shadows, professing his belief that the client data was truly gone.

Fortunately for that attorney, the news team did not reveal his identity. Furthermore, the computer forensics company was kind enough to ensure the all client data were permanently removed before returning the computers to the local charities.

It is interesting to ponder, however, how fast that attorney would have lost his clients—and perhaps his license to practice law—had his identity and mistake been revealed to hundreds of thousands of Portland television viewers.

The Practice of Information Security

By now it should be clear that the practice of information security has at least three important purposes: client protection, reputation protection and compliance with the Rules.

"Information security" is a technical term. It has three subcomponents:

- *confidentiality* of information
- *integrity* of information
- *availability* of information.[17]

The confidentiality part of information security is easy enough to understand: information should not flow to unauthorized persons. The integrity part of information security demands procedures that ensure sensitive information is not corrupted or tampered with. The availability part of information security demands that information is accessible to authorized persons at the appropriate times.

Attorneys should seek to ensure the confidentiality, integrity and availability of client data wherever it flows. The same data set can exist in many places at the same time. It usually makes no sense to encrypt a sensitive client file on the server while later sending it as an unencrypted e-mail attachment, or later copying it in unencrypted form to a portable hard disk drive. These truths demonstrate that careful and consistent attorneys who care about their clients and reputations will strive to achieve information security for sensitive data wherever it travels.

What follows is a basic introduction to some important ways to help attorneys safeguard their clients' information.

Firewalls

Every computer facing the Internet should have a firewall. A firewall is a software or hardware device that controls access to network ports on an Internet Protocol ("IP") address of a computer. An *IP address* is analogous to a telephone number; when computers want to talk to each other, they locate each other using IP addresses. Using that analogy, a *port* is akin to a telephone extension. However, an IP address has many thousands of ports. When a service, such as a Web server or e-mail server, is running and listening for connections, it must attach to an available port to perform its function.

An open port presents a security risk. Hackers will randomly scan thousands of IP addresses for services ready and waiting to receive connections. If the port scan reveals an active service on an open port, the hacker may attempt to exploit it. An open port thus presents an opportunity for mischief. At the same time, the opening of some ports can be necessary to provide services users need. Firewalls should be installed and configured so that only necessary ports are open.

Readers who are interested in gaining a better understanding of network ports, as well as testing the configuration of their own firewall, are encouraged to use the "Shield's Up" service available at www.grc.com. However, be aware that Shield's Up only tests the security of the most common network ports; it does not test the security of all ports. To determine the security status of all ports, a complete port scan must be performed.

What makes a good firewall? In part, a good firewall will monitor and control both incoming and outgoing network traffic. The firewall that comes with Windows XP Service Pack 2 is considered by some to be inferior because it does not monitor or control outgoing network traffic.

A good firewall must be properly configured. On more than one occasion, friends or clients have installed and configured firewalls that were so horribly misconfigured that they provided no protection at all. The Shield's Up service can help attorneys begin to understand whether their firewall is properly configured.

Although not technically a firewall function, some firewalls today come with an additional feature sometimes called "behavior anomaly detection" ("BAD"). Generally, the purpose of BAD is to prevent unauthorized programs from covertly accessing the Internet. For instance, if a spyware program tries to "phone home," BAD technology should ask for your explicit permission before granting Internet access to that program. BAD thus gives users the ability to subvert the malicious activities of certain programs. To determine whether your firewall has BAD, try a tool called Leaktest.[18]

Remote Access

Nowadays, it is not uncommon for attorneys to work from home or while traveling. What makes this possible, in part, is the ability to remotely log in to an office computer from a hotel lobby, a home computer or an Internet café.

There are various technologies that allow remote login. Attorneys who have a choice of remote login products should opt for ones that encrypt network traffic rather than those that do not. They also should prefer remote login products that do not require an open port. Use care when entering your remote login credentials from untrusted computers, such as those in hotel lobbies or in Internet cafés. Attorneys who are concerned about having their remote login credentials secretly captured by a "key logger" can mitigate this risk by using the Microsoft On-Screen Keyboard ("OSK").[19]

Key Loggers

These are a hacker favorite. A key logger is a hardware or software device used covertly to capture personal information, such as

user names and passwords, by watching for physical typing (keystrokes) on a keyboard. To mitigate the key logger threat, attorneys can use their mice to enter user names and passwords using the OSK. The OSK will subvert most known key loggers.

Anti-Virus & Anti-Spyware Program

These are a well known part of information security. Make sure these programs are configured properly and have frequently updated definitions.

Metadata

In practical terms, metadata are data in or about a file that get you in trouble or subject you to embarrassment.[20] For example, in some cases WordPerfect files can keep track of deleted text. Were this kind of file disclosed to opposing counsel, text thought to be deleted could actually be recovered by your opponent. Metadata occurs in many kinds of files, although WordPerfect and Word files are typically the most relevant to lawyers.

To minimize the metadata threat in WordPerfect files, for starters, attorneys should ensure the "Undo/Redo" as well as the "Document Revision Annotations" features have been disabled.[21] To minimize the threat in MS Word, users should disable "Track Changes," disable "Fast Saves," and use the "Word 2003 Redaction Add-in" or the "Remove Hidden Data" tool.[22]

File System Security

One advantage of using modern Microsoft operating systems like Windows 2000 and Windows XP Professional is that they can use either of two kinds of file systems: FAT32 or NTFS. Attorneys who are concerned about information security will want to implement the NTFS file system because it can allow them to control the ability of others to read or make changes to sensitive files. This is because the NTFS file system has a security feature called *file permissions.* Attorneys who use file permissions properly can control the ability of others to read, change or copy sensitive files without authorization.[23]

Wireless Networks

Certain kinds of wireless local area networks are known for weak encryption. In some cases, this makes it easier for hackers to steal data during network transmission. Although there are a few patches and meth-

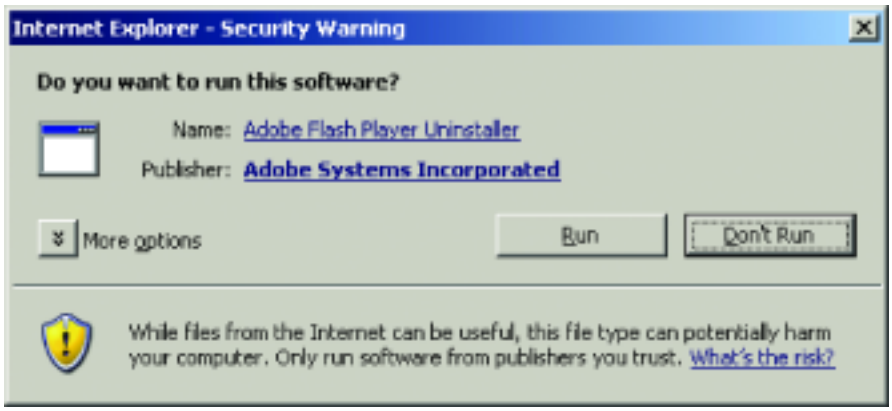


FIG. 1: ActiveX Control dialog box

ods that can increase wireless security to some degree, many of these patches and solutions have their own weaknesses.

The better approach is to avoid patchwork solutions to wireless network security. Attorneys interested in solid, cost-effective wireless network security should consider implementing a wireless network based on *802.11g with RADIUS and Active Directory integration using client certificates.* Although it sounds like a mouthful, in appropriate situations it is one of the most secure and hassle-free wireless networking technologies available today.

■ ActiveX

Many a user has suffered from an Internet browser toolbar that serves up unwanted advertisements or changes the default homepage. Often these toolbars are installed without proper user understanding through something called an "ActiveX control."

Figure 1 contains an example demonstrating the appearance of an ActiveX control.

The bottom line with ActiveX controls is that users should choose to "Run" an ActiveX control if: (1) the control itself is wanted, and (2) the publisher of the control is trusted. To assess trustworthiness, research the name of the publisher and/or control using Google or Yahoo!. If trustworthiness cannot be determined, users should not run the ActiveX control.

■ Hard Drive Security

There are many important things to know about hard drive security, only some of which can be discussed briefly here.

"Hard drive security" broadly refers to ensuring the security of sensitive information stored on internal hard drives, external hard drives, USB tokens, CDs, DVDs, media cards and so on. The general concern for all these devices is that if the device came into the wrong hands, sensitive information might be inadvertently disclosed. Even if a client's file is encrypted on disk, for example, a prior version of that file may exist in "deleted" form somewhere else on the disk. In this example, one purpose of hard drive security is to ensure such "deleted" data are permanently gone. Thus, even if the disk is lost, stolen, discarded or donated, the attorney and client are protected.

To achieve hard drive security, users should begin by regularly deleting the contents of their cache directory. The cache directory is a place where Windows stores temporary copies of documents and Web pages.[24]

Second, even though a file is deleted, it still can be recovered in many cases. To ensure deleted data truly is gone, attorneys should use the *cipher* program, which works on Windows 2000 and Windows XP machines.[25]

Third, most attorneys do not realize that many modern photocopiers and fax machines also have hard drives: When a user feeds a client paper document into such a device, a copy of that document is made on the device's hard drive. When the device is subsequently sold, discarded or stolen, client data may go along for the ride. Thus, when selling or discarding these devices, attorneys should consider taking steps to protect sensitive information.

■ Mobile Devices

Attorneys who own mobile devices also have information security challenges, especially when these devices are lost, stolen, sold or discarded. Users have been burned, for example, by selling their Blackberry device on eBay without first ensuring all data are permanently removed.[26] Those who want to dispose of or sell their Blackberry should take the necessary steps to remove all sensitive data from the device.[27]

■ Bluetooth

Many new mobile devices now come with a feature called Bluetooth. Bluetooth "provides a way to connect and exchange information between devices like personal digital assistants…, mobile phones, laptops, PCs, printers, digital cameras and video game consoles."[28]

Bluetooth may be enabled by default or by choice on the majority of new mobile devices. In some case, this may be a problem, as has been reported: "Serious flaws discovered in Bluetooth technology used in mobile phones can let an attacker remotely download contact information from victims' address books, read their calendar appointments or peruse text messages on their phones to conduct corporate espionage."[29]

To avert these risks, attorneys can set their Bluetooth device to "discoverable" or "invisible" mode. This protection is not complete, however, because some models can be attacked even if set to invisible mode.[30] Attorneys with such exceptional devices might consider disabling Bluetooth altogether.

■ Encrypted E-Mail

In some cases, attorneys communicating with their clients via e-mail may want to consider protecting the communication content with e-mail encryption. One of the easiest ways to facilitate the exchange of encrypted e-mail between attorney and client is to set up each person with a free e-mail account from Hushmail.com.

As long as the two Hushmail accounts are used for e-mail communication, by default the e-mail exchange will be encrypted and confidential as against government eavesdropping and hacker malevolence. Attorneys with more sophisticated clientele may want to use e-mail encryption products like Pretty Good Privacy or S/MIME. In certain cases, attorneys may want to consider whether client disclosure and consent is needed before using non-encrypted communications.

■ Phones

Former Senator Newt Gingrich found out the hard way about the importance of cellular phone security.[31] Attorneys interested in such security should begin by understanding that modern phones, including dual-band and tri-band models, can still transmit with no encryption whatsoever while in roaming

mode or while dialing for emergency services. Attorneys interested in maximum protection of all telephone and cellular calls need to transition to specialized encryption products.

Phishing

Phishing is the "attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication."[32] Although often the subject of media hysteria, the large majority of phishing attacks can easily be prevented if users simply refuse to use HTML e-mail and learn to read Uniform Resource Locators, or URLs.

How phishing works can be demonstrated by viewing an e-mail message in two different ways, as shown on page 40. First, it is displayed with HTML formatting enabled (Figure 2); next, it is displayed with HTML formatting disabled (Figure 3). The illustrations make clear how phishers use HTML e-mail to perpetuate fraud.

Figure 2 is an HTML-formatted e-mail with a hyperlinked URL leading to a sign-in page, apparently within the eBay.com domain. (The hyperlinked URL is boxed in red near the bottom.)

Figure 3 shows the same e-mail viewed without HTML formatting. The apparent (but false) URL is boxed in red near the bottom, whereas the real destination is boxed in black below the red box.

Viewed in this manner, the true destination page is revealed to be within the fairwindsmthorses.com domain (wherever that is).

The lesson: By disabling HTML formatting and reading URLs, the fraud is revealed. To disable HTML e-mail in Outlook 2003, go to Tools > Options > Preferences. Click E-mail Options, and then select the check box labeled "Read all standard mail in plain text."

Users who are interested in further protection from phishers may want to try the anti-phishing toolbar, free from Netcraft.[33]

Data Backup/Restoration

Some are surprised to learn that data backup and restoration are a part of information security. Because lost data are not *available*, and data that are corrupted when restored do not have integrity, data backup/restoration is an important part of information security.

Data backup and restoration are not easy

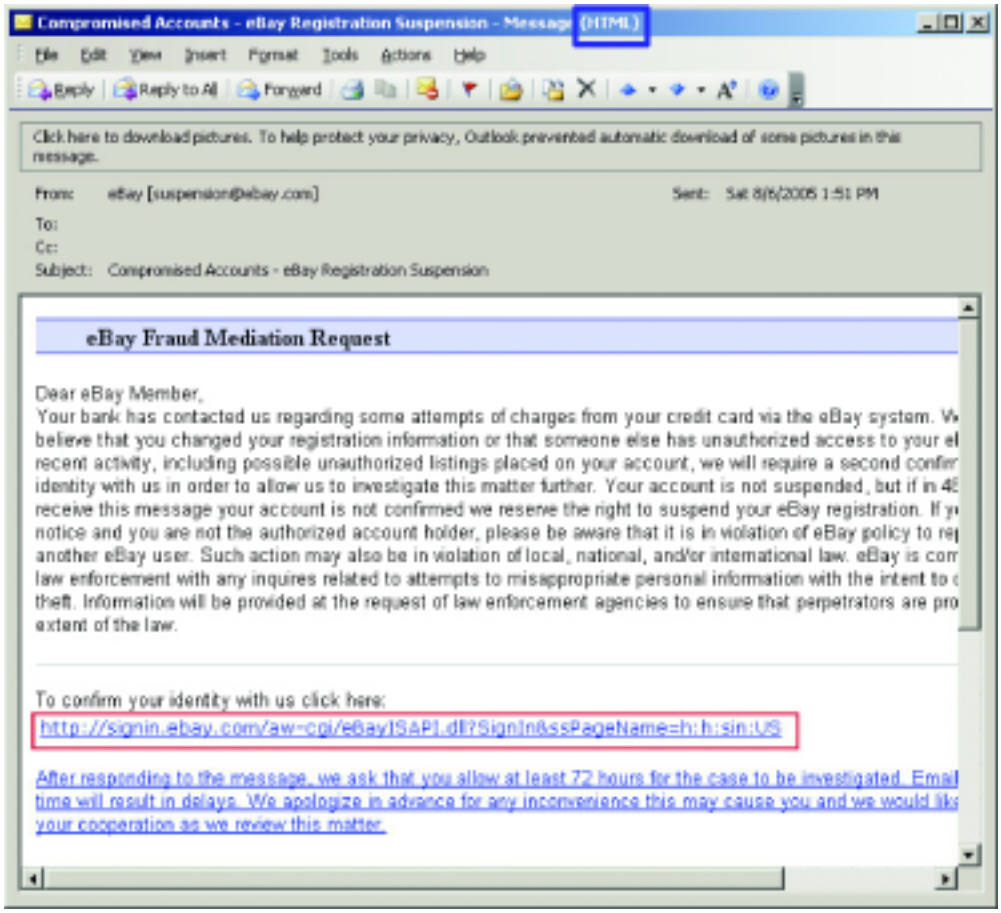


FIG. 2:
E-mail with HTML formatting enabled

to do correctly. Those who disagree simply have not considered the issues carefully. Data backup cannot be given proper treatment in a small section, but here are a few pointers:

- Daily data backups are a must.
- Backup tape technology is declining in popularity.
- Attorneys should ensure their backup data can actually be restored by periodically performing "mini-practice-restores."
- Online backup services are too expensive in many cases.
- Offsite copies of backup data are essential.
- Consider encrypting data backups.

Paper Shredding

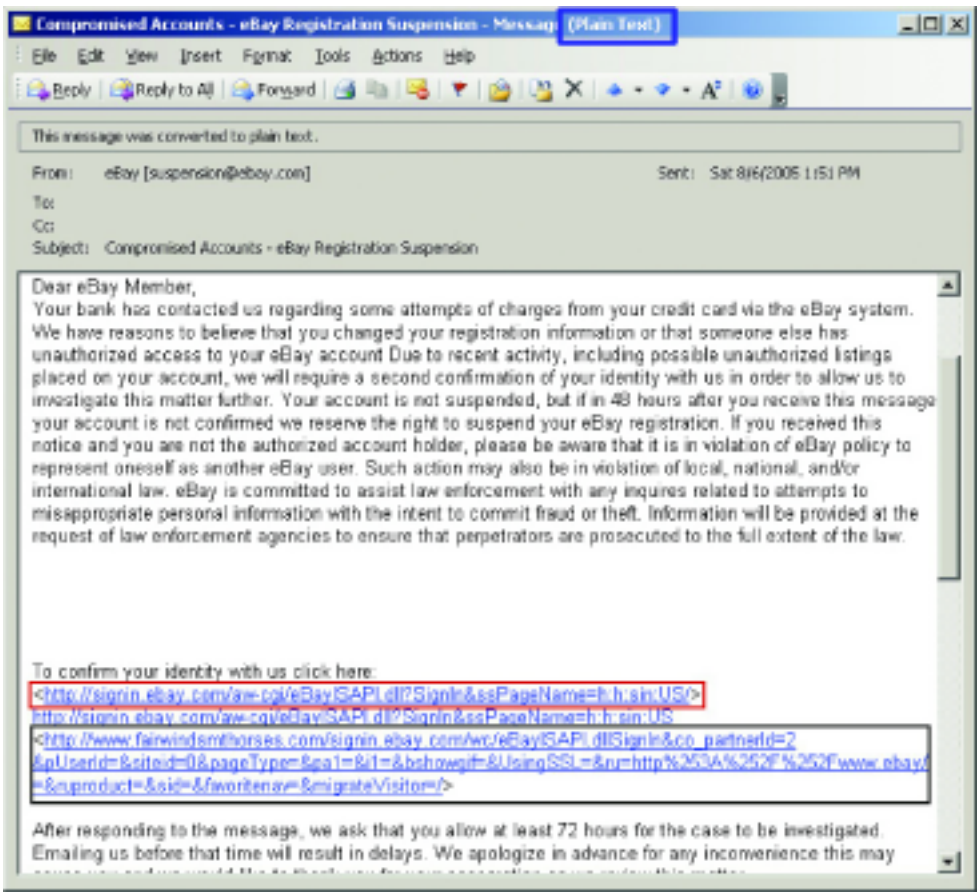
Attorneys should always shred sensitive documents before disposal. The Arizona Center for the Blind and Visually Impaired offers a reasonably priced paper shredding service.[34]

Conclusion

The security measures discussed in this article are meant to be introductory in nature; by no means do they represent a comprehensive list of measures to be taken to protect client data against loss or inadvertent disclosure. Whichever information security steps are taken, however, it is clear that the political, legal and business environment has progressed to the point that attorneys should take special care of their clients' electronic information. AZ AT

endnotes

1. Arizona Ethics Op. No. 05-04 (July 2005).
2. Michael Ratner & Sara Miles, *Above the Law*, SALON (Mar. 2006), available at www.salon.com/opinion/feature/2006/03/31/wiretapping/index_np.html.
3. Privacy Rights Clearninghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident* (Apr. 20, 2005), available at www.privacyrights.org/ar/ChronDataBreaches.htm.
4. Ratner & Miles, *supra* note 2.
5. Niall McKay, *Lawmakers Raise Questions About International Spy Network*, N.Y. TIMES, May 27, 1999, *available at*



After responding to the message, we ask that you allow at least 72 hours for the case to be investigated. Emailing us before that time will result in delays. We apologize in advance for any inconvenience this may

FIG. 3: E-mail with HTML formatting disabled

www.nytimes.com/library/tech/99/05/cyber/articles/27network.html; *see also* Wikipedia, *Echelon*, http://en.wikipedia.org/wiki/ECHELON (last visited July 21, 2006).

6. *Id.*
7. John Leyden, *AT&T Sued Over NSA Warrantless Wiretapping*, THE REGISTER (Feb. 1, 2006), available at www.theregister.com/2006/02/01/atandt_wiretap_assistance_suit/.
8. Declan McCullagh, *FBI Plans New Net-Tapping Push*, C-NET NEWS (July 7, 2006), available at http://news.com.com/2100-1028_3-6091942.html.
9. Robert Windrem, *U.S. Spies On Corruption Overseas*, MSNBC (July 21, 2000), available at www.msnbc.com/news/434065.asp?cp1=1.
10. David R. LaRivee, *Attacking the Financial Roots of Terrorism*, www.acdis.uiuc.edu/Research/S&Ps/2002-Su/S&P-Su2002/financial_roots.html.
11. Declan McCullagh, *Terrorist Link To Copyright Piracy Alleged*, C-NET NEWS (May 27, 2005), available at http://news.com.com/Terrorist+link+to+copyright+piracy+alleged/2100-1028_3-5722835.html.
12. Arizona Ethics Op. No. 05-04.
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. Wikipedia, *Information Security*, http://en.wikipedia.org/wiki/Information_security (last visited July 21, 2006).
18. Leaktest, www.grc.com/lt/leaktest.htm (free software tool available for download).
19. The OSK can be accessed on a Windows XP machine by going to Start > All Programs > Accessories > Accessibility > On-Screen Keyboard.
20. Richard M. Smith, *Microsoft Word Bytes Tony Blair in the Butt*, ComputerBytesMan (July 30, 2003), www.computerbytesman.com/privacy/blair.htm.
21. Richard C. Belthoff, Jr., *WordPerfect Metadata: Removing the Garbage from Your Documents*, LAW OFFICE COMPUTING, Apr./May 2005.
22. Donna Payne, *Control Metadata In Your Legal Documents*, http://office.microsoft.com/en-us/assistance/HA01140034103.aspx (last visited July 22, 2006); *id.*
23. Willis et al., *NTFS Permissions*, WINDOWSITPRO, Dec. 2000, *available at* www.windowsitlibrary.com/Content/592/1.html.
24. To delete the cache directory contents, first open the My Computer desktop icon, right-click on "C:," choose "Properties," and then choose "Disk Cleanup." Then delete as many files as possible.
25. To use *cipher*, navigate to Start > Run and type "cipher /w:X:", where "X" represents the drive to be cleansed. Attorneys who want to maximize their information security will eschew *cipher*, instead opting for Eraser 5.7 (free for download), *available at* www.heidi.ie/eraser/download.php. When running Eraser 5.7, be sure to choose the option to erase "cluster tips."
26. Kim Zetter, *Blackberry Reveals Bank Secrets*, WIRED NEWS, Aug. 25, 2003, www.wired.com/news/business/0,1367,60052,00.html.
27. To remove personal data from a Blackberry, choose one of two options. First, choose Settings/Options > Security; then, using the Trackwheel, select "Wipe Handheld." Alternatively, on older devices, choose Tools > Settings > Security and enable password protection; then lock the Blackberry, then enter an incorrect password ten (10) times.
28. Wikipedia, *Bluetooth,* http://en.wikipedia.org/wiki/Bluetooth (last visited July 22, 2006).
28. Kim Zetter, *Security Cavities Ail Bluetooth*, WIRED NEWS, Aug. 8, 2004, www.wired.com/news/privacy/1,64463-0.html.
30. *Id.*
31. Kathleen Kirby, *Wiretapped Conversations*, COMMUNICATOR (Feb. 2000), *available at* www.rtnda.org/foi/wtc.html.
32. Wikipedia, *Phishing,* http://en.wikipedia.org/wiki/Phishing (last visited July 22, 2006).
33. Netcraft Anti-Phishing Toolbar, http://toolbar.netcraft.com (software tool available for download).
34. For more information, visit www.azcenterfortheblind.com/.