



ILLINOIS STATE
BAR ASSOCIATION

STANDING COMMITTEE ON LEGAL TECHNOLOGY

The newsletter of the ISBA's Standing Committee on Legal Technology

From the Chair

By Nerino J. Petro, Chair

Time and technology are constantly moving forward and with the passing of the past 12 months, I find myself coming to the end of my term as chairman of the Illinois State Bar's Committee on Legal Technology (CoLT). It's been an interesting year with numerous new software releases including Microsoft Windows Vista, Microsoft Office 2007 and online software as a service (SaaS) with new online applications from Google; technology hardware manufacturers have also been busy to share with Apple making a big splash with its soon to be released iPhone, new BlackBerry models from Research and Motion, new models of the Treo from Palm and more. CoLT member Trent Bush takes us through the decision-making process for his firm in selecting a new smart phone and his experience with the BlackBerry. Adam Nelson of CoLT, addresses data security for the solo and small firm in his article later in this newsletter which is very timely in light of continued security breaches resulting in the theft and/or loss of confidential

and personal information for hundreds of thousands of people throughout the United States. This past spring has also demonstrated that Mother Nature is a force to be reckoned with as demonstrated by the destruction of not only homes, but businesses as well. These and other disasters around our country, continue to drive home the absolute need to backup your all too critical data on a regular basis. In the August 2006 edition of this news letter, I addressed the basics of backup from a perspective which included different types of backup sets, various software choices and other information, but that article did not include a specific example of a backup procedure that you could follow. I intend to remedy that in the balance of this article.

There are a wide variety of backup methodologies and schedules from the extremely simple to the incredibly complex. The sample that I set below is just one suggestion and is by no means the only way to create a backup methodology and schedule. The sample plan below is intended for single computers, computers that are in a peer-to-peer environment or are using strictly Windows XP for networking including operating the server. True networks can use a modification of this plan, but it would require different software. However, this sample backup plan provides a reasonable balance between rotating backup media, preparing for a catastrophic loss that does not destroy your office as well as securing your absolutely critical data offsite. I've also tried to take into consideration the complexity, cost and time involved in preparing this sample backup plan.

**Get the electronic
version of this
newsletter**

**Go to www.isba.org/newsletters
for details**

While it seems that there are as many backup recommendations as there are individuals, I take the view that you should be able restore your entire system meaning not just your data, but all of the programs and software in the event disaster strikes. Many people take the position that they have the backup disks and can simply just reload from those and therefore, there is no need to back up the operating system and all of your programs. While this may be true, think of how much time it will take you to locate all of the disks for each of your programs, install them on your computer, download and install all of your program updates; if you're lucky, you're only talking a matter of hours, but it could be several days. And while your computer system or systems are down, much of your practice will be at a standstill. While my suggested backup plan may leave a small gap between complete backups, it is much easier to download and install updates for a one-week period than it is if you've never made a backup of your entire hard drive at all.

Taking into consideration the points I make above, this generally results in a three-tiered backup approach that includes A) an image of your entire hard drive; B) backups of the data that has changed since the last full backup; and C) online backup of only your data and critical files.

I suggest the following:

1. Purchase a copy of Acronis True Image 10 home for each computer. Ideally, if you have more than one computer, all data is centralized

IN THIS ISSUE

- From the Chair 1
- To BlackBerry or not to BlackBerry? 3
- Information Security for the Solo and Small Firm Attorney 4

on one of them as it makes backing up much easier. You will also need a minimum of two external hard drives (three is better). You can usually find the hard drives on sale at Best Buy or similar stores every weekend for around \$130 for 300 Gigabyte Drives (or larger) and you can check there for the software also. If using full-size external hard drives, I recommend that you stick with similar hard drives as you will be able to keep one power adapter at the office and one at home; usually come each manufacturer provides a different power supply for their full-size external hard drives. Another option would be to use a smaller notebook-sized external hard drives which generally only require a USB cable to provide their power. The downside to the smaller external drives is the capacity and their speed which will result in a longer backup duration.

2. Install the Acronis True Image software on your computer and make a complete image of your hard drive using the wizard found in the software to one of the external drives. If you have multiple computers, you'll want to make a backup of each and save it to an external drive. This is where the third external hard drive can come in handy as you can back up all of your images to that drive. I also recommend you burn this initial image to a DVD or, if you don't have a writable DVD, then to CD-ROM. Place the disks in a fireproof and secure location. In the event of a disaster, at a minimum, you can restore back to this original complete disk image. Then on a regular basis, such as quarterly or even after you install new programs, create a new complete image so that you can always back up to that point without having to reinstall all of your programs, operating system and data.
3. On Monday and Wednesday, run a differential backup with a full backup once again on Friday. I recommend a differential, rather than an incremental, backup as a differential back-up backs up all information from the time of the last full back-up through the date of the differential backup; while an incremental backup only backs up the information from the last

incremental backup not the last full backup. What this means is the difference between requiring the last full backup and one (the most recent) differential backup to restore your data versus your last full backup and every incremental backup since that full backup to restore your data. For simplicity, I would swap external hard drives out after you make the complete backup on Friday and take the drive with the most current information home with you.

4. Sign up for a free Mozy online backup account at www.Mozy.com. There are numerous other online backup services, but Mozy is simple and provides a free account or a paid unlimited storage account. Mozy will not back up system or program files, and due to the bandwidth limitations, even just backing up your critical data files will take some time. Schedule this to backup only your data files on Tuesdays, Thursdays and Saturdays over the Internet. When you set up your free, 2 GB account (which should be enough to get you started), I also recommend that you use your own encryption password as this will prevent anyone at Mozy or anyone else for that matter, from looking at your data.

IMPORTANT NOTE: YOU MUST MAINTAIN YOUR PASSWORD AS IF YOU LOSE IT, MOZY WILL BE UNABLE TO PROVIDE YOU WITH YOUR PASSWORD SINCE IT IS YOURS AND YOURS ALONE. IF YOU'RE UNCOMFORTABLE WITH THIS, YOU MAY USE THEIR ENCRYPTION, BUT YOU DO RUN THE RISK OF INFORMATION BEING TURNED OVER PURSUANT TO A SUBPOENA OR OTHER ACTION AS SET OUT IN THEIR PRIVACY POLICY.

5. Finally, perform a sample or test restore to ensure that your data is actually being backed up. Murphy's Law of backups provides that your backup will fail when you need it most. One method of doing this is to select several critical files and data types such as your time and billing data and word processing files, renaming several of these files and then doing test restores from the backup data stored on the external hard drive as well as from the online backup service and see

if the files will open and if the data appears to be current and correct. Initially, you want to test this with the first backup and then at least biweekly for the first two months. Thereafter, I would recommend doing a test restore at least monthly.

If you add a third external hard drive to this plan, it would become the primary backup for a monthly full backup and then on successive months, each of the hard drives would be rotated through so that at any one time you have a monthly full backup and a weekly full back. This translates into the greatest period of time that you could potentially lose data for would be one week or in the worst case scenario, one month. However, with the online backup of critical data, your data should always be within one or two days of being up-to-date at all times.

For offices using true network operating systems such as Microsoft Server or Microsoft Small Business Server, Acronis makes a product suitable for use on these servers and this procedure can be adapted using such a product. In this event, I would also strongly suggest that each workstation also have a copy of Acronis True Image software installed on it with regular images being made of these systems on a quarterly or semiannual basis or at least when major software is upgraded. You can also use a more traditional backup product such as EMC Retrospect (server version) which still allows for disaster recovery as well as including the ability to backup connected workstation computers that are connected to the network.

You must weigh your own needs against the potential risks of different backup intervals and what the backup to come up with your own backup plan. However, you need to do some type of backup, even if that's just a backup of your critical data: you can always reinstall your software, but you can't replace your data.

Nerino Petro is a former Illinois Solo and Chair of CoLT. In addition to his years as a lawyer, he has been a legal technology consultant for over 11 years and holds certifications on a number of legal software packages. He is currently the Practice Management Advisor for the State Bar of Wisconsin's Practice411™ Law Office Management Assistance Program and serves on the ABA GP|Solo Technology Committee.

To BlackBerry or not to BlackBerry?

By Trent L. Bush

That is the question our firm recently faced as our mobile phone contracts were about to expire. Below, I detail some of the factors we considered in making that decision and my initial impressions as a new BlackBerry user (some may say future addict).

Our firm has 19 attorneys in two offices and we practice in Northwest Illinois. Our two-year commitment with Verizon was set to expire in March. With our old phones dropping like flies, we began to investigate our options. At that time, we all carried our run-of-the-mill phones. While BlackBerry and so-called “smartphone” devices may be quite prevalent in the metro area, only a handful of attorneys had made the leap to such devices in our area. Several of us had used PDAs for some time and were interested in exploring this option for our new contract.

Options, options, options. When shopping for new phones, we considered many options that fell into three general categories: regular phones, smartphones, and BlackBerry devices.

Phones. If you’ve been in the wireless market lately or watch any TV, you know there are many phones to choose from. These phones can come with a variety of features, including camera, video, speakerphone, instant messaging, picture messaging, video messaging, web access, Bluetooth, and music capabilities. The prices of these phones range from free to over \$300, depending on the model and the nearly ubiquitous rebate that may happen to apply at any given time.

Smartphones. The smartphone category includes such brand names as the Motorola Q and Treo. Physically, these phones are a little larger than the regular phones, have larger color screens, and typically have built-in keyboards. These devices are essentially mini-computers in that they have operating systems (generally either Microsoft or Palm based), internal memory, and processors. In addition to some of the features available on the regular phones, these phones incorporate the features of a tra-

ditional PDA device (e.g., calendar and contacts) plus e-mail. Depending on the device, the phone may also enable you to open and even edit e-mail attachments with such programs as Word, Excel, PowerPoint, and PDF. These phones can synchronize your calendar and contacts with your computer so that entries made on your computer will appear on the device and vice versa. You can also access the Internet, albeit in a different (and far less-convenient) manner than you are accustomed to on your computer.

BlackBerry. Finally, we also considered BlackBerry devices. BlackBerry devices—developed by Research In Motion (RIM)—contain many of the features of the smartphones, less some of the program and multi-media applications. Physically, these devices are roughly the same size as the smartphones. The devices are high-speed wireless broadband capable and can be used as a modem when tethered to your laptop. The devices run on a proprietary operating system and can be integrated into an existing e-mail system with the installation of a software package called BlackBerry Enterprise Server (BES).

Making Our Decision. Ultimately, only five attorneys decided they were interested in a smartphone or BlackBerry handheld. The primary factors we considered in deciding whether to purchase the devices were cost and functionality with our existing system.

1. Cost. The first factor we considered was the cost of having these devices. The additional cost hits you at several levels. First, just as with a regular phone, the devices must be purchased from the service provider. The cost of the units themselves is significantly higher than the regular phones—even with a two-year commitment and the typical rebates. The initial purchase price can be anywhere in the range of \$100 to \$500.

Second, in order to take advantage of the wireless capabilities of the devices, you have to purchase not only a voice package but also an additional

data package, which can be another \$50 per month. Thus, you can be looking at an additional \$600 per year per device. When you multiply this by several devices, you’re starting to talk about real money!

Third, there may be some cost associated with the software or associated licenses, although I got the feeling there are regular deals that include the software with a contract. Finally, there may be some cost in getting the devices to actually work, which gets me to the next factor.

2. Functionality. Aside from cost, we also considered whether the devices would actually work with our system. We run Outlook on a Microsoft Exchange server version 2000. After numerous discussions with our dealer and a meeting with the technical support person, we were assured that the devices would work with our system. We were told that if things didn’t work out we could return the devices within fifteen days and choose a different product.

After we felt reasonably certain that the devices would work and that the cost was justified (at least in our heads), we had to choose between going with one of the smartphones or a BlackBerry. Initially, we were drawn to the Treo for the ability to open and edit attachments with the various programs. However, the Treo came with a higher list price (around \$400) than the BlackBerry devices and we did not need the multimedia capabilities of the Treo. Also, our local sales rep personally carried a BlackBerry and told us he really liked it. Ultimately, we felt that the BlackBerry would be a better device for beginners.

Taking the Leap. We considered and ultimately purchased two different BlackBerry models—the 7130e and the 8703e. The 7130e is a slightly slimmer model than the 8703e with reduced-key QWERTY keyboard (i.e., the keyboard is laid out like your typical computer keyboard). In other words, there is more than one letter on each key. BlackBerry has developed something called SureType technology that does a pretty good job of figuring out the word

you are intending to type.

The devices are fairly intuitive, even for some of the less technologically savvy of our attorneys. A trackwheel with a clicking function (like that on your computer's mouse) is the primary method of navigating the system. The "home" screen displays such basic things as the date, time, signal strength, and Bluetooth status. In addition, there are icons for messages, phone, address book, calendar, Internet browser, pictures, search, profiles, tools, applications, settings, Bluetooth, keyboard lock, and power. Rolling the trackwheel highlights the various applications, which you can then enter by clicking. You can then backup by clicking a little button called the escape button right below the trackwheel.

On the technical side, we turned to our firm administrator and our IT consultant to integrate the devices with our system by utilizing the BES software. BES essentially automatically relays e-mail to the device. The software monitors your inbox, contacts, and calendar so when a new item arrives, it is automatically "pushed" or relayed to the BlackBerry device. The information is automatically synchronized so the items appear the same on your device and computer.

We were provided a link to download the BES software upon purchasing the software. What we were not provided before our purchase that would have been useful were instructions or system requirements. Our initial attempt did not successfully integrate the devices with the system. In order to talk to BlackBerry technical support, we had to first go through Verizon technical

support. It took nearly a week before we were able to discuss the matter with BlackBerry support.

Once we were able to contact BlackBerry, the tech person was able to assist in getting our system and the devices to synchronize. However, there were still various small features that still were not working correctly. For example, the calendar on one of the devices did not synchronize at all. On the other devices, appointments made on the devices would not appear on our Outlook calendars and the messages on the devices were not reconciling with the Outlook inbox. Our administrator estimates that he and the IT consultant spent 12-16 hours installing the software and ironing out the wrinkles.

Review. We have now had our devices for a couple weeks and the reviews to date are positive. Like any other new technology, there is a bit of a learning curve and we have not figured out how to effectively utilize all of the features of the devices. However, for anyone who has had a PDA or feels comfortable with their computer, the transition will likely be a smooth one. Stay tuned in the upcoming issues for a more comprehensive review of the pros and cons of our BlackBerry experiment.

Trent L. Bush
Ward, Murray, Pace & Johnson, P.C.
202 E. Fifth St.
P.O. Box 400
Sterling, IL 61081
ph: 815.625.8200
fax: 815.625.8363
web: www.wmpj.com
e-mail: bush@wmpj.com

Information Security for the Solo and Small Firm Attorney

By Adam C. Nelson and Benjamin Gerber

It has become increasingly important for practicing attorneys to address information security and privacy requirements in their offices. This is especially true around the various types of sensitive data in their possession. This data can include sensitive

client data—anything from financial records, health information, and real estate records, to secret formulas, trade secrets, and business strategies.

The main business drivers for the attorneys to address their information security and privacy requirements are

Legal Technology

Published at least four times per year.

Annual subscription rate for ISBA members: \$20.

To subscribe, visit www.isba.org or call (217)525-1760

Office

Illinois Bar Center
424 S. 2nd Street
Springfield, IL 62701
Phones: (217) 525-1760 OR 800-252-8908

Web site: www.isba.org

Editor

Bryan M. Sims
1001 E. Chicago Ave., #111
Naperville, IL 60540

Managing Editor/Production

Katie Underwood
kunderwood@isba.org

Standing Committee on Legal Technology

Nerino J. Petro, Chair
Peter V. Mierzwa, Vice-Chair
David Yavitz, Secretary
David M. Clark, Ex-Officio
Trent L. Bush
Todd H. Flaming
Jay Jung
Peter M. LaSorsa
Mark A. Lichtenwalter
Mark B. Moran
Robert G. Moss
Adam C. Nelson
William L. Niro
Enid K. Olsen
Alan R. Press
Meredith E. Ritchie
Bryan M. Sims
Carl R. Draper, Board Liaison
Doug Barringer, Staff Liaison
Steven L. Dunn, Staff Liaison

Disclaimer: This newsletter is for subscribers' personal use only; redistribution is prohibited. Copyright Illinois State Bar Association. Statements or expressions of opinion appearing herein are those of the authors and not necessarily those of the Association or Editors, and likewise the publication of any advertisement is not to be construed as an endorsement of the product or service offered unless it is specifically stated in the ad that there is such approval or endorsement.

Articles are prepared as an educational service to members of ISBA. They should not be relied upon as a substitute for individual legal research.

The articles in this newsletter are not intended to be used and may not be relied on for penalty avoidance.

Postmaster: Please send address changes to the Illinois State Bar Association, 424 S. 2nd St., Springfield, IL 62701-1779.

their legal obligations as well as their reputation and image. Perhaps even your “brand.” For many attorneys their reputation and image coalesces into their brand and this is an important factor to understand.

There is also an increasing amount of legislation at the state, federal, and international levels mandating security and privacy policy, practices, and controls; and even outside of mandated compliance, a sensitive information breach can be devastating to future business prospects. Knowledgeable clients often take their business to attorneys who can be discrete, this is true not only for their particular matter, but also for all their information associated with, and resulting from their matter.

All security controls, including policy, must be relevant to the risks your firm faces. Risk is determined by understanding the various threats, identifying vulnerabilities, and devising controls to mitigate these threats and the exploit of vulnerabilities.

Determining risk and associated controls is not a one time operation; controls, including policy, must be reviewed and updated on a regular basis. At a minimum, an annual review and update should be conducted. This includes reviewing compliance requirements and ensuring controls support compliance goals.

Today, your information assets take the form of paper files, data on laptops and office desktops, and on several central office servers. These are the assets we are interested in protecting. Your controls must then address the risks of loss or inappropriate disclosure of these assets. We also understand that you may outsource some, if not all, of your IT needs. Security controls can also help address the needs of this outsourcing.

Putting aside all of the various compliance requirements that attorneys must follow,¹ we will focus on the most relevant and important practical controls your firm can implement to address risk and establish a basic level of information security. The controls we recommend implementing follow.

Policy

Ultimately protection is achieved through the establishment and adherence to information security and privacy policy, standards and controls. Policy defines what objectives your firm will

achieve or require; standards state how the objectives are to be met, while controls, both procedural and technical, are in place to support policy.

We recommend starting out with the creation of a single overall policy and controls document that can be used as a roadmap for your firm’s implementation and ongoing support of information security and privacy objectives. In many organizations, creation of policy, followed by standards and supporting documents is often a requisite first step. However, you may find that policy creation can be tackled as security controls discussed below are themselves being implemented.

There also may be a need to create an additional high level public information security and privacy policy document, or perhaps two separate policy statements—one addressing information security and another addressing privacy—that would be written specifically for your clients’ consumption. These policies, intended for consumer audiences, are the type you typically encounter on consumer web sites, when renting a car, or visiting your doctor’s office.

Various information security frameworks exist that offer starting points and best practices for developing an information security program. Selection of a standards framework will be based on the industries you primarily cover, type of business performed, and culture of a firm. The most widely leveraged framework—both for use by organizations’ security programs and by those developing compliance requirements, is the ISO/IEC 17799 Code of Practice for Information Security Management.² This is also the framework found to be most applicable to the typical business activities of attorneys. Other security frameworks to consider include COBIT (Control Objectives for Information and Related Technology) and the NIST (National Institute of Standards and Technology) 800 Series.

ISO/IEC 17799 defines what areas should be addressed in the context of information security and will provide you with a guide when developing your information security policy. The eleven major control areas will act as a check list of items that when considered you may find applicable to your firm’s requirements.

Hiring Employees

Ensure that employees, contractors

and third parties are suitable for the jobs they are considered for and understand their responsibilities. Do background checks, ask for references, and review their resumes closely. Have a fully featured termination policy which includes removing access to facilities, software, hardware (keys, keycards, passwords, locks), and notifying clients when appropriate. Remember, employees and contractors will have access to your clients sensitive data.

Education, Training, and Awareness

Conduct annual training on how to handle sensitive data; this includes security, privacy and compliance issues and responsibilities. Your internal security policy and controls document will be the basis of this security training program. Topics should include how to handle sensitive information and what controls are in place to protect it and how to use these controls. Training should ensure awareness of social engineering techniques, and how to avoid viruses, and other potential attack vectors. Make it a requirement that employees must acknowledge that they have had this training.

Vendor Management

Evaluate your vendors. Ask for a copy of their data handling practices; make sure they comply with their practices. Ensure they care for your data and information. Ask for the right to audit their practices. If you use temporary employees, ensure that the agency follows proper hiring practices. Basically, require of them what you would do for your own hiring, including background checks.

Physical Security

The physical space of your firm should be protected. It is important to prevent unauthorized physical access, interference and damage to the organization’s information and premises. Some basic suggestions include placing cameras at entry and exit points, keeping printers and fax machines which may receive sensitive information in a secured area, locking down offices, computers, cabinets and printers. File cabinets containing sensitive information should not be left unlocked at night or throughout the day and if small cabinets must be secured to the floor

or wall to increase the time and difficulty of their removal. Paper files and media should not be left in public or common areas unattended.

Centralize Information

A solid strategy that should be used in order to mitigate risk is to get away from keeping important and sensitive data on workstations, laptops and desktops, and utilizing centralized servers as repositories of such information. Servers are not only easier to secure, but offer a centralized place from which to retrieve and backup up-to-date information. Sensitive information stored on laptops should be limited to what is needed for immediate business purpose. Secure remote access can be employed for retrieving records when out of the office when deemed necessary as well as for access to e-mail and intra-office communication.

Referencing Individuals Information

Review the method in which the firm refers to clients and other individual's records. Are you falling into the trap of utilizing social-security-numbers or other externally referenceable personally identifiable information? Utilize unique identifiers that do not have a meaning outside of your firm—clients and employees should have a client or employee number by which various records can be tied together, referenced, or retrieved.

Anti-virus

Ensure anti-virus software is installed and functioning on all workstations. The software must be configured to:

- Update signatures, which are indications of a virus' presence, at least once per week. The application can be configured to do update automatically.
- Perform automatic file protection when certain events occur—such as executing or loading a file—that would cause harm. If the file is infected, the anti-virus software will intervene and either cleanse or delete the malicious software.
- Many anti-virus software packages include the ability to plug into popular e-mail systems, consider utilizing these features as well.
- These programs often have an application that searches for spyware. Spyware is software that is often downloaded inadvertently from the

Internet. It runs in the background, slows your computer down and has the ability to send messages about every Web site you are visiting to someone who might be tracking your activities.

Enterprise editions of anti-virus software allow for centralized control and updating of the software—this can be a time saver when many workstations require management.

Firewalls

There are two types of firewalls you must use. Office and/or home office Internet connections should go through a router-firewall device—not just a hub device. A combination router-firewall will provide the ability to connect multiple computers to the same connection, as well as protect against some types of attacks from the Internet—do not use high speed internet connections without one. These devices may also come with built in wireless network functionality.

“Personal firewalls” or firewall software that runs on laptops and desktops offer additional critical protection. They prevent network attacks, as well as rogue applications communicating to the Internet. Many offer additional functionality such as cookie privacy management, spy-ware detection, e-mail security and personal data management. Firewalls for laptops and desktops are particularly important while traveling and using public or hotel Internet connections.

Wireless

If you use wireless in the office or home office—ensure the latest security functionality is being used. This will require entering in passwords or keys on every computer that uses the wireless connection—but it is well worth the effort. This will prevent outside users from utilizing your connection and gaining access to your network, as well as prevent the monitoring of users' activity and the use of various exploits against the computer. WEP is an older and flawed wireless security protocol and should not be used; newer equipment will offer better options—preferably WPA2. Additionally the default password for configuring the wireless device should be changed, the network name or SSID should be changed and broadcasting of the SSID can also be disabled. Optionally MAC addresses of

legitimate computers can be added to the wireless device's list of permitted devices.

Operating System and Software Updates

Update/patch your operating system and any software packages you use—be aware of security patches as they are announced—most exploits occur w/ known vulnerabilities on un-patched systems. Once again, Windows XP and Vista can be configured to automatically install updates.

Whole-Disk Hard-Disk Encryption

Laptops will be stolen, desktops will be misplaced, and server hard-drives may be inadvertently disposed of during an upgrade. While whole disk encryption of hard-drives will not protect against intentional dissemination of sensitive information—it greatly reduces the risks involved with unintentional loss. Data from stolen laptops on which whole disk encryption has been applied can not be easily recovered and will in many cases not result in any breach of data.

There are several software packages available today with varying ease of use. Some may be configured to prevent unencrypted data from being moved to portable media. Other desirable features may include the use of a master key for recovery of data by authorized persons other than the primary user.

File Level Encryption

It will at various times be necessary to convey data to third-parties as well as protect data files at a finer-grain level than offered by whole-disk encryption. Software and hardware choices for achieving this are wide, including a handful of high-quality freely available applications. Utilizing software from the same vendor that you choose for whole-disk encryption will offer familiar interfaces and integrated functionality.

Workstation Lockdown

While it is convenient to have administrative powers on laptops and desktops—it is most often not necessary for most users. Locking down access to operating system functionality—such as the ability to install additional applications or install optional hardware devices—can mitigate a user's risk of installing viruses, and Trojan horses and

reduce the ease with which data can be moved to portable media. Also consider if CD or DVD burners are a necessary tool for some users jobs, or a data breach waiting to happen.

Research your Purchases

Research, research, research. All attorneys research the law as the outcome is obviously very important, but we need to use our skills when purchasing new equipment. This should be fairly obvious. Subscribe to PC World, attend ABA Techshow, and attend ISBA Tech Offerings. As you become better educated regarding technology, you will feel much more comfortable about purchasing it and using it in your practice

Event Management and Incident Response

Prepare through planning and practice. Every firm should establish consistent practices and procedures outlining activities and responsibilities to plan for, detect, respond to, recover from, and report out of the ordinary activity. This includes the loss of control over or integrity of, or purposeful or inadvertent misuse of sensitive data, resulting in a security and privacy incident. The practices and procedures must be documented in a response plan, and the plan should be periodically tested, practiced, an updated as appropriate.

Backups

Backup centralized servers and store the backup media offsite with a vendor who specializes in secure storage of data records. Traditionally full backups are performed regularly, once per week, once per month; with incremental backups performed on a daily basis. However, with today's high-speed, high volume, and inexpensive optical media (e.g. DVD-R) and magnetic media (e.g. tapes), a daily full backup of your firms critical data is well within reach.

Remember that this data is no doubt sensitive—both from a privacy and competitive perspective—encryption must be applied; the data must be encrypted as part of the backup procedure. Many software packages that facilitate archiving and backup offer such a feature, and better still, many dedicated backup media recorders offer built into their hardware encryption on the fly, as the data is recorded to the media.

Disposal Procedures

The Federal Trade Commission has indicated that they are going to start evaluating companies' disposal procedures. Do not dump documents containing personal information directly into a dumpster. The storage medium containing this data has to be completely destroyed. This means shredding for paper or CDs and magnetically wiping or destroying hard drives. Please, please do not sell your old hard drives on eBay. If you donate or sell your old workstations, remove the hard drives.

Cell Phones and Personal Digital Assistants (PDA)

Attention must be paid to the data stored on cell phones and PDAs. For many uses, PDAs and smart-phones in particular, should be treated as laptops—though they are easier to steal. Anti-virus software is available for Windows Mobile devices, various encryption options exist for storage and access to e-mail. Almost all smart portable devices have the capability to remotely wipe their memory before a device is disabled by the service provider, though unless encryption is applied data can still be recovered by a motivated thief. Functionality for remotely removing data can be provided by your service provider or third-party software. It is often possible to have service providers remotely wipe out stored phone numbers and call histories on even basic cell phones. There may be features you have to activate in advanced, do not wait until a device is lost or stolen to discover the options.

You may want to evaluate the use of portable music players in the office. A 40 MB iPod can store a large amount of your data and it is relatively easy to use an iPod as a storage device. As with hard-drives—do not sell or donate old smart-phones that at one time may have contained non-encrypted sensitive data.

Conclusion

Implementing the controls discussed will help alleviate a large amount of risk around the loss and inadvertent disclosure of data. You still may have to address the particular requirements of your practice. Although these are basic controls, many firms do not take the time to address them, you will find that following these suggestions will provide guidance toward achieving your information protection responsibilities.

Adam C. Nelson, Esq., is a member of the Technology Committee of the Illinois State Bar Association and is on the Board of Editors of the Privacy & Data Security Law Journal. He is a Managing Consultant in the Security and Privacy Practice at IBM. Benjamin Gerber, CISSP, CISA, CPP, CIPP/G, is a Managing Consultant and Architect with IBM Security and Privacy Practice. The authors can be reached at anelson@us.ibm.com and bgerber@us.ibm.com, respectively.

1. ARDC, GLBA, ethics mandates.
2. This Standard was published by the Information Standards Organization and was revised in 2005. The official name is Information technology - Security techniques - Code of practice for information security management. It is due to be renamed to ISO/IEC 27002 later this year.

Target your message!

- Reach the exact practice area you need with no wasted circulation
- Ads cost less
- ISBA newsletter readers ranked their newsletters 2nd highest of all Illinois legal publications in terms of usefulness. (Illinois Bar Journal was ranked 1st)
- 72% of newsletter subscribers either save or route each issue, so your ad will have staying power.

For more information contact:
Nancy Vonnahmen
Advertising Sales Coordinator
Illinois State Bar Association
800-252-8908 or 217-747-1437



ILLINOIS STATE
BAR ASSOCIATION

Do yourself a favor

Say goodbye to paper and get this newsletter electronically

Why?

You'll get it faster. Opt for the electronic version and bypass the ISBA print shop and post office. We'll send you an e-mail message with a link to the latest issue as soon as it's posted on the Web, which means you'll get it days, even weeks, earlier than you would in print.

You'll save space. Because newsletters are archived on the ISBA Web site, you needn't worry about storing back issues.

You'll help keep section fees low. At \$20/year, section membership is a tremendous value. But paper and postage costs continue to rise. By choosing the electronic over the paper version, you help keep our costs—and yours—down.

How?

Just go to <<http://www.isba.org/newsletters/enewsletters.html>>. Submit an easy-to-complete form and have any newsletter—such as the next issue of *Legal Technology*—delivered to your inbox.



Non-Profit Org.
U.S. POSTAGE
PAID
Springfield, Ill.
Permit No. 820

Legal Technology
Illinois Bar Center
Springfield, Illinois 62701-1779
June 2007
Vol. 14 No. 5