For Your Information

Truth be told, it serves us right. For a long time, lawyers talked circles around business people by using strange terms and vague concepts like negligence, 10b-5 actions, parties of the first part, heretofores and my personal favorite, res ipsa loquitur.

Then the tables started to turn. Lawyers had to get used to the strange acronym speak from our friends in the IT group who bandied about terms like Corba, VPN, IP and IPSEC, and more recently VOIP. Now the tables are turning again.

"In the world of intellectual property, your rights can be severely impacted by electronic data and the associated systems that store that information," said Philip Burrus of the Burrus Intellectual Property Law Group. "A company that fails to maintain up-to-date technology and record-keeping does so at its peril."

An effective in-house counsel must not only be a legal whiz but thoroughly conversant and comfortable with technology. Back in the old days (oh, about 12 to 18 months ago), electronic information remained mostly the province of the IT Department. Now, counsel must recognize the importance of electronic data and be conversant with its myriad forms, in addition to understanding the legal issues relevant to each different type of datum.

"One of the biggest problems as a lawyer is an inability or unwillingness to effectively communicate with IT staff, both because of the lawyer's inability to understand IT people and because IT people don't understand the law," said Thomas Y. Allman, senior counsel for Mayer, Brown, Rowe & Maw in Chicago. "We have to make it our business to educate ourselves about the IT issues that will affect our companies."

Electronic-Document Discovery

At its most basic form, electronic-document discovery or "e-discovery" is just a new buzzword for the electronic version of an old problem – organizing and reviewing documents for discovery. However, dealing with electronic data increases the stakes and presents some new twists.

For starters, counsel must have an e-discovery plan before a suit is filed or a regulatory inquiry is commenced. A well-crafted discovery request will almost certainly include a broad demand for electronic documents, including e-mail. Without a plan already in place, you may be forced to settle a casejust to avoid the expensive process that e-discovery entails. Even worse, without a plan, your company may unwittingly delete relevant data as part of normal business processes, resulting in severe sanctions from the court.

The price for being unprepared is high. Zubulake v. UBS Warburg, a routine employment discrimination case, ultimately resulted in a verdict against the employer of $9 million – plus $20 million in punitive damages. Both the verdict and damage amount were arguably attributable to the defendant's conduct in discovery. Even more recent, Morgan

Stanley's discovery missteps (and misconduct) in Coleman Holdings v. Morgan Stanley resulted in a verdict of $604 million plus another $850 million in punitive damages – essentially without reaching the facts of the case!

Being prepared for e-discovery is challenging and time-consuming. The sheer volume of documents is staggering, as employees can create hundreds of new documents each day: e-mail messages; versions of pricing and forecasting spreadsheets; contract revisions; voicemail messages; instant messages; updates to customer and product databases; and changes to the web site, just to name a few. Some of this information may be printed, but most is stored – somewhere – electronically.

Determining where all this information is located is another significant challenge. Because e-discovery typically includes e-mail, voice messages, instant messages and databases, in addition to documents created in Word, Excel or other applications, finding all the information – and collecting it – is a difficult problem. Although the IT group may be your best ally in this task, it is your responsibility to manage. Once litigation strikes, counsel must be prepared to vouch for the fact that the information has been located, maintained and provided to the opposing party.

Some steps that can help you prepare for e-discovery include:

- Don't wait for litigation – craft and implement a document-retention policy that addresses litigation holds and other e-discovery issues. Many top law firms have specialized expertise to assist you.
- If you already have a policy, review it to ensure that it includes all electronic data in your company, not just e-mail. Include appropriate education and address e-discovery issues.
- Form a cross-functional team, including IT, to review the actual implementation of the policy. Don't forget to look closely at backup tapes and offline storage.
- Know the regulations that apply to your company's data. For example, there are specific regulations that apply to brokerages, SEC reporting companies and the insurance industry.

Some in-house counselors advise against relying too much on magnetic backup tapes. Some IT professionals are far too ready to use backup tapes as a "mini-archive," Allman said.

"Savvy counselors know that backup tapes are not efficient and should not be routinely accessed as an archive, but should be used for what they were originally intended, that is disaster recovery," Allman said.

Metadata

Metadata is another hot topic, largely because it is secret – involving electronic data that is hidden, or at least not readily apparent. After stripping away the buzz, however, metadata is simply "data about data." In a Word document, for example, metadata might include information on the location of the file on a server, the identity of the person who

initially created the file and the person who last opened the file. If configured in a certain way, metadata might also contain information on how the file was changed from its original format (a hidden "redlined" version).

It sounds boring – and most of the time, it is. But what if the metadata in the contract you just sent to your best customer hides a prior version with a better price (or better terms) for another customer? What if the metadata in that great new marketing presentation used by your sales force shows that the presentation actually belongs to your biggest competitor?

Fortunately, simply being aware that metadata exists is at least half of the battle. So, educate yourself and your employees. In addition, you may want to consider:

- Reconfiguring applications. For example, Word can be configured so that it does not create as much metadata. (Microsoft even provides a tool that permits you to manually strip metadata before it is sent outside the company.)
- Automated solutions. Other tools can automatically strip metadata when it is sent as e-mail. Nevertheless, keep in mind that metadata can be a valuable knowledge management tool, so how you handle metadata needs to be based on informed decisions.

Protection From The Internet

Just about everyone has implemented an appropriate Internet/web surfing policy, and that is a great first step in protecting your company from the dangers related to the Internet. But do you (or your IT department) have any tools to actually confirm that usage is consistent with your policy? When issues arise, is the policy routinely enforced?

The price for failing to effectively address Internet issues can be high. Obviously, employees lose valuable productivity if they are accessing non-work-related sites or instant messaging or using chat boards. In addition, workplace claims frequently arise from inappropriate e-mail use.

But a potential new threat starts from outside of the company. Many computer viruses can turn your company's computers into unwitting zombies, ordering them to "attack" other computers on their command. Now, let's say that those computers are used to target and shut down a top Internet site that handles a million dollars of business per day. If those computers are traced back to your company – and a negligent or poorly enforced Internet policy that allowed the virus or spyware to proliferate – you could find yourself the target of a suit for substantial business losses.

Some initial steps to address this threat are:

- Review your Internet policy with the IT group. Ask the tough questions: How do we know when the policy is being violated? What do we do? Every time? Executives too?
- Discuss the anti-spyware and anti-virus software that the company uses. Is the software automatically updated? Is it effective?

- Do you have a policy (or tools to prevent) the installation of unauthorized software on company PCs? How is it enforced?

Securing Sensitive Information

You might be wondering if we're straying far off the legal path. What could security possibly have to do with data and in-house counsel?

Consider all the important data that your company maintains – employee Social Security numbers, customer addresses, pricing, competitive information, trade secrets, formulas, financial data, etc. If you are not concerned about protecting the security of that data from a competitive standpoint – after all, who wants their customer list and pricing information posted on the Internet by hackers? – then maybe you are concerned because of HIPAA, Graham-Leach-Bliley, Sarbanes-Oxley or other federal or state privacy laws.

The news has been filled with recent stories of hackers improperly obtaining sensitive customer and employee data. Even though most of these cases involve a criminal element, companies are being held responsible for not having proper safeguards in place. Congressional hearings and even new legislation is in the works, and lawsuits are pending.

Although counsel certainly cannot be required to safeguard the data, it may be in the company's best interest to ensure that proper safeguards are in place. One simple safeguard many companies are considering is encrypting data before it is placed onto backup media, especially if that media is being transported off-site. A similar idea is to encrypt the data that resides in a database. That way, if the database is "hacked," the hackers will also have to obtain the key to read the data.

Remember that regular e-mail typically traverses the public Internet with as little security as a postcard in the mail. For extra credit, you may want to research encryption for your e-mail communication, especially any sensitive communications with outside counsel, financial advisers or auditors. A word of caution: Some counselors strongly disagree about whether encryption is useful.

"Encryption adds a layer of confusion and slows down the communication process," Allman said. "It may also be deciphered by clever hackers. It is better for counselors to rely on the traditional rule of client privilege."

To start getting a better handle on security:

- Get to know your business even better. You may need to speak with many business unit leaders to determine what type of sensitive customer data is being maintained. Human Resources and the Finance group will also be critical;
- Again, working well with your IT group is a key piece to the puzzle. The members of that team are in the best position to understand the systems that hold this sensitive data, how it is currently protected and how it can be better protected;

- Consider investing in some form of secure data transfer method for critical e-mail communication.

James D. Shook Esq. is the executive director of Special Counsel's Atlanta office. Jim holds a degree in computer science, has practiced law for more than 10 years and frequently writes and speaks on issues in which technology intersects the law. You can reach him at Jim.Shook@SpecialCounsel.com.