Technological foundations of an efficient, reliable law office network

Prepared by Brian Mauch for the Trial Lawyers Association of BC conference
"Maximize Your Personal Injury Practice: 20 Ways to Get Smart Fast"
February 9, 2007

Table of Contents

1) Infrastructure

A network's infrastructure is often overlooked, but it is just as important the selection of appropriate computer hardware and software to the reliable operation of a law office. A reliable infrastructure consists of three elements: (1) modern network cabling, (2) sufficient electrical power, and (3) an internet connection.

Network cabling

Even before new computer equipment is purchased, a law office should ensure that modern network cabling is in place and has been tested for cabling faults.

Electrical power

Sufficient electrical power is also an important of a law firm's network infrastructure. Law firms should consult an electrician to make sure that an office's electrical circuits are able to supply any new computer-related device with appropriate levels of voltage.

Internet connection

A final infrastructure component is the internet connection. The two primary options for fast (aka. broadband) access are ADSL and cable. ADSL is provided over a telephone line, whereas cable is supplied by television providers. Both have their pros and cons. Business internet accounts are generally more reliable, and a more expensive account that provides a "static IP address" will give you increased remote access and email hosting options.

2) Hardware

Server

A reliable law office network should be designed around the use of a primary computer called a server. The server acts as repository for all of the firm's data, and shares it out to user's workstation computers. As a firm grows, it may be necessary to add multiple servers to handle increasingly complex duties. With the exception of very small offices with limited computer needs, a server should be a dedicated computer – that is to say, it sits in a back room and is not used as anyone's regular workstation.

Workstations

The computers that sit on lawyers' and staffs' desks are called workstations. Workstations have the productivity applications (such as word processors and email applications) installed, and access their data from the server.

Printers

Law offices have considerable printing requirements. I generally recommend name-brand laser printers, to be shared by clusters of users. A law office would also benefit from a network copier. Network copiers not only copy, but they act as high-speed printers, as well as network scanners. In fact, digital copiers are the best solution for law office scanning, because they are easily accessible by everyone and are not tied to a specific computer.

Brand-name hardware

I recommend that a law office use only brand-name hardware. I have found that the brand-name computers break down less often, and when there is a problem, the warranty service is superior to

that of clone manufacturers. There was a time when I used clone hardware, but I've found that the minimal savings in cost is not worth the tradeoff in reliability.

Business class equipment

All computer manufacturers have two lines of equipment. One line is targeted at home consumers, and these computers are sold at retail stores. However, you won't find the line of equipment targeted at businesses in the retail stores, as they are special-order only. Generally speaking, the consumer class equipment includes cheaper components, but many bells and whistles, and includes software that is not designed for office networks. An example is that most consumer class computers come preloaded with Windows XP Home, whereas the more expensive Windows XP Professional is required to connect to a Windows server-based network. I strongly recommend that law offices purchase business class computers, because their hardware and included software are more reliable.

Three-year warranty

I always purchase a three-year warranty on computers. All computers are subject to operational wear and tear, just as in a car, because they contain moving parts. A computer will be most efficient during the first three years of its life, and if a component prematurely breaks down during that three-year period (which does occasionally happen with name-brand computers, although far less than with clone computers) you will want to have that component replaced under warranty.

Note that computer warranties do not cover user-generated software problems. Unfortunately, most computer problems fall into that category. When you take a computer of its box, it usually has Windows loaded, but not much else. It isn't much use to the average law office user without installing software. However, as soon as you install and configure software, manufacturers treat the software as being modified. The situation is analogous to that of an auto manufacturer refusing to warrant a car that had been extensively modified by a car hobbyist. Manufacturers can only guarantee a product that is maintained in its original operating condition, and within reasonable use guidelines. Therefore, the safest way to keep a computer in good working order is to limit the software that is installed or downloaded to only what is required for work purposes, and nothing more. Most parents have experienced frustration when their children have installed file-sharing programs or games that crash or otherwise disable a home computer.

4-5 years expected useful life

After the initial three-year period, a computer will likely start to seem slow to its user. However, the hardware itself is no slower than it was when originally purchased. The primary reason that older computers begin to feel slow is that the software has likely been upgraded at some point over the initial three years. For example, a law office may have upgraded their legal accounting software, or installed newer antivirus software. A general rule is that each new version of software has more features, but requires more horsepower to run at the same speed. Therefore, if the hardware remains constant after a software upgrade, then the software is going to run more slowly.

If software is kept to a reasonable minimum, and the hardware remains in good working order, the expected useful life of a law office computer is 4-5 years. Beyond that point, a computer is

no longer efficient at running the latest software. Law offices should budget for new hardware every 4-5 years.

3) Software

When it comes to software, compatibility is of utmost importance for law firms. Due to the now-frequent exchange of data with clients and other law firms, deviation from established standards will only result in conversion frustration.

Microsoft Windows and Office

Almost all law firms use Microsoft Windows-based PCs, and Windows computers are also used by the majority of business and home users. Apple-based computers have found niches in some industries, and are currently enjoying increased popularity in the home, but they are generally not compatible with most law office software.

Microsoft has also established its Office suite of applications (Word, Excel, Powerpoint, etc.) as the business standard. Regardless of how you feel about the relative merits of Wordperfect vs. Word, or Microsoft's software monopoly, your firm will be at a disadvantage if you don't use Microsoft Office. Compatibility is key to efficiency, and you want your office to be compatible with the established standards.

Legal accounting

Every law firm should have a computerized accounting system. There are a variety of legal accounting packages, each with their own strengths and weaknesses. The best choice of accounting software is probably the one that your bookkeeper is most familiar with, since they will be the primary user. Legal accounting software can also allow lawyers and staff to input their time directly, which increases efficiency.

Practice management

Practice management software can manage all of a law firm's information and activities from critical deadlines, to email, documents, research, billing and client and matter information. This kind of software can increase the efficiency of any law firm, but due to the unfortunately high cost of this software, many firms do without. I recommend that every firm consider the practice management packages available, because the initial cost will soon by eclipsed by the additional billings generated by increased efficiency.

4) Remote access

Law firms are increasingly using various remote access methods to stay in touch, even while out of the office. Remote access can permit lawyers to work from home when required, and can allow part-time staff to work from their own homes, which reduces overhead.

Home computers and laptops

Depending on the type of network that is installed, there are generally two types of remote access from remote computers (including laptops as well as home computers): (1) email only, and (2) remote control.

The most basic type of remote access is limited to email. Users with appropriate permissions can send and receive emails from a remote computer, and perhaps also access other information in an organizer program such as Microsoft Outlook.

More advanced remote access is known as remote control, and allows a user to work as if he or she was in the office. This can be done by connecting to the user's office computer, or by using a single remote server that can host a number of users at once.

Handheld devices and cell phones

Some lawyers may also benefit by carrying a mobile remote access device, often built in to a cell phone. These devices are either Palm, Windows, or Blackberry-based. Each variety has its strengths and weaknesses. Generally, Blackberries are the most reliable, and best for email. Palm devices are preferred by those who are familiar with the Palm interface. Windows devices have a similar interface to full-size computers, and incorporate advanced multimedia functionality.

5) Security

A law office should be concerned about the security of its network. Confidential client information and accounting data should be protected from prying eyes. Viruses, spyware, and spam can reduce the efficiency of computers and users, and even render a network unusable.

Hardware firewall

A business-class hardware firewall should be used to protect your internal network from your internet connection, and should be configured to only allow legitimate internet traffic.

Gateway anti-spam and anti-virus

Most law firms are heavy users of email, and email-borne viruses and spam is a significant problem. This problem can be effectively reduced by utilizing gateway anti-virus and anti-spam services. "Gateway" refers to the fact that these services are operated by your internet provider, and help to prevent viruses and spam from reaching your office computers. The advantage to having an internet provider managing these services is that you don't have to do it yourself.

Workstation anti-virus

Not all viruses travel by email. Viruses can also be spread by disk or portable drive, or can be downloaded. To supplement a gateway antivirus system, every computer on a network should run antivirus software.

Physical security

The physical security of your computer network should not be overlooked. The theft of a computer workstation, or even worse, of a server, can be more disruptive than a computer crash. In particular, laptops or mobile devices should be locked up when not in use.

Acceptable use and password policies

Finally, I recommend that every firm develop and enforce an acceptable computer use policy. More computer downtime is caused by users downloading and installing non-work related software, than any other work-related cause or hardware malfunction. A password policy should also be developed and enforced.

6) Backup

Last on this list, but certainly not the least, is a backup system. With recent tragedies in New York and New Orleans, the business world has been made painfully aware of the importance of backing up computer systems. In the event of catastrophe, having proper backup procedures in place can make the difference between a business surviving and carrying on, or having to permanently close its doors.

In a law firm setting, proper backup procedures involve: (1) keeping all data on a server; (2) using rotating, removable backup media; and (3) using offsite storage.

Keep all data on server

All computer data should be kept in a central location, typically on a server. This not only makes it easy for users to find the data they need, but also simplifies the backup process. Users should not keep any important data on their personal computer workstations. Workstations break down more often than servers, and if all the data is kept on the server, a workstation can be repaired or replaced without any loss of data.

Rotating, removable media

Using multiple backup media on a rotating basis, be it tapes or CD/DVDs, allows for multiple versions of data to be restored. For example, if only one backup tape was over-written and re-used every night, you would only be able to restore a file from yesterday. However, if multiple tapes were used, you could restore a file that existed a few days ago, but has since been accidentally deleted from the network. The more tapes that are used, the further "back in time" that the restore can reach.

Offsite storage

Offsite storage should be used in case of fire, flood or worse. If all of the backup tapes are kept in your office, then you would not have any recourse if the entire building was to go up in flames. It is therefore a good idea to keep at least one copy of the backup somewhere offsite.

7) Conclusion

If your law office gives due attention to the six foundations of a reliable network (infrastructure, hardware, software, remote access, security and backup), you will enjoy the benefits of having an efficient and reliable network. These benefits include increased lawyer and staff efficiency, which will result higher billings for your firm.