Network Security: An Oxymoron?

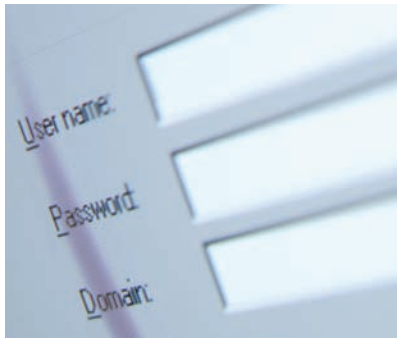
Preparation Is Pivotal to Ensure Your Firm's Survival

BY ED POLL

"Disaster" for any law firm is not a question of "if," but rather of "when." The only unknowns are the type of disaster, when it will occur, and how disruptive it will be. Whether it's a hurricane, a fire, a broken water pipe, or a more subtle danger, the real issue is ensuring the firm's survival.

While some disasters cannot be prevented, others can – such as the loss of data network capability. Failure to reasonably anticipate and be prepared to service clients in the wake of a disaster that jeopardizes your data network is arguably a failure both in the overall duty to act competently and in clients' best interests. Network survival and firm survival are thus one in the same.

Famous UCLA basketball coach John Wooden once said, "Failing to plan is planning to fail." Keeping your data network secure is an issue that goes far beyond firewalls, encryption, and passwords. Network security should be conceived and carried out in the context of a comprehensive plan that addresses every aspect of keeping that network functioning: technology safeguards, disaster planning, organizational development, modernization program, and more. In that spirit, let me suggest 10 areas on which every law firm manager should focus in order to ensure network security and survival, and the firm's security and survival.



Keeping your data network secure is an issue that goes far beyond firewalls, encryption, and passwords.

1. CYBER CRIME

If your system was compromised by a hacker, or otherwise threatened by criminal activity, it would certainly qualify as a disaster for any firm – and it happens far more often than most firms want to admit. An annual survey of businesses and professional organizations conducted by the FBI and the Computer Security Institute revealed that 90 percent of survey participants had suffered computer security breaches, with average losses totaling hundreds of thousands of dollars.

The two biggest sources of financial loss from computer security breaches are viruses and unauthorized access. Therefore, all of the standard protection tools, from antivirus software to encryption, are valid and necessary.

2. CYBER INSURANCE

Computer security risks, and the disasters that can result from them, are fundamentally unprotected by traditional property, fidelity, and professional liability insurance. The only effective insurance protection against a computer disaster is cyber insurance – a specialized form of computer insurance coverage that insurance organizations such as American International Group, Chubb, and Lloyd's of London have offered since the late 1990s. Such policies are highly specialized, but definitely worth investigating.

Ed Poll, *Principal*, LAWBIZ MANAGEMENT

If a disaster occurs, you may have members of the firm working at remote locations for an extended period of time. Telecommuting ... is an excellent dry run for setting up the logistics of a remote network.

3. DOCUMENT LIFE CYCLE

Every record of information in a law firm – every brief, pleading, contract, and form prepared for each specific matter – has a life cycle that encompasses creation, distribution, maintenance (electronic and physical), retention, and preservation. If you don't have a systematic approach to managing this process, you will have no idea what you have and what you've lost if disaster strikes.

4. KNOWLEDGE MANAGEMENT CULTURE

Knowledge management is the systematic organization of the firm's entire work product, prepared for all of its clients, so that the collective research and advice of all lawyers are available to each lawyer. Best practices require every firm, whether one lawyer or one thousand, to create a standard classification system for each lawyer's electronic work, and to keep it updated for every matter. This classification system may vary by practice area, but should not be left to the whims of individual attorneys. Systematic organization eliminates haphazard attempts to keep track of information, and thus makes it more secure.

5. REMOTE BACKUPS

Most firms know to back up all computer data and to store data backup and important records and documents off-site. But think of this – what if your "secure" site is just a few miles from your office, and your city is hit by a disaster the magnitude of Hurricane Katrina? Consider arranging for offsite backup in a location as far removed from your own as is physically and financially possible.

6. TELECOMMUTING

What does telecommuting have to do with data security? If a disaster occurs, you may have members of the firm working at remote locations for an extended period of time. Telecommuting, where feasible under normal working conditions, is an excellent dry run for setting up the logistics of a remote network, and it can give you remote and functioning information centers in the event of a disaster at your central office location.

If you are a single-office law firm, you may want to consider a "buddy system" with another law firm, locating your independent (and "locked") server at its premises, outside of your extended geographic location. Or, arrange with an independent resource such as West to house your duplicate server.

7. ALTERNATIVE TECHNOLOGY LOGISTICS

Know where you can get replacement computers and infrastructure in a hurry. Consider the example of 200-lawyer firm Thacher Proffitt. Three-quarters of its attorneys and staff worked at Two World Trade Center. Miraculously, not one person was lost in the September 11, 2001, terrorist attacks. However, every firm computer was gone. On September 12, the firm already had a truck on its way to Dell Computer Corporation in Texas to pick up 300 new PCs. *That's* security planning.

8. KNOW WHOM TO CONTACT

Every firm should have physical and electronic communication lists with firm members, clients, vendors, courts, and others who make its practice work. A good communication plan must be in place before a disaster occurs. It should include a standing list of building managers and real estate agents whom you can contact to set up temporary space, including furnishings, computers, and phones. It should also have full contact info for service providers who can help re-establish your practice utilities, data security, and Internet services, and legal specialists such as Lexis/Nexis and West, etc.

9. FINANCIAL PLAN FOR TECHNOLOGY INVESTMENT

An old and inefficient network is more prone to disaster, and even to internal failures. While many

firms replace computers and related technology before the end of a three-year cycle, the burden for small firms is challenging because they can be overwhelmed by the high up-front expense, resulting in upgrade cycles of up to six years. One survey recently found that 37 percent of firms spend from 4 percent to 7 percent of expenses on technology; however, about 50 percent spend less than 4 percent. Given the variety of lease, manufacturer, and bank loan financing options available, it makes no sense to delay so long and leave your security more vulnerable.

10. COMPREHENSIVE DISASTER RECOVERY PLAN

The bottom line summary of all of these security tips is to have an effective, detailed disaster recovery plan that you constantly review, practice, and update. The plan should include a risk assessment, identify responsibilities for a disaster recovery team, create an emergency communication network, and include security procedures to protect your network against disgruntled employees, unhappy clients, and deranged strangers. Your energy on such efforts will be priceless when needed – and a good investment to maintain your network security and business continuity.

Keep in mind, too, that technology is only one element for a disaster recovery and business continuity plan. Your *people* represent the most important element, followed by the *nature of your practice*, or practice areas. Each area of practice must consider the critical elements of the given practice area needed to survive a disaster (segmented by down time and time needed to recover). Then, apply to technology needed to expedite the required elements to get the practice operational once again. ❄

about the author

Ed Poll is the principal of LawBiz Management and an internationally recognized coach, law firm management consultant, and author. Author of the legal business blog at *www.lawbizblog.com*, Poll is a regular columnist in *Legal Management*. Contact him at *edpoll@lawbiz.com*.