

# Securing Client Information: Problems and Solutions

*Toby Brown*

With the ethical duty lawyers have for holding client information securely, lawyers should be utilizing computer security a bit above the norm. Yet many lawyers coast along with what they perceive to be “adequate” security. For lawyers to address this situation, they should gain a deeper understanding of the security threats that exist and the possible approaches to minimizing the risk of breach. This does not mean you need to have a deep understanding of the technology. On the contrary, lawyers should focus on the practice of law and leave the technology to technology professionals. However, as a fiduciary you should have in place policies that drive the appropriate level of technical security. Clearer understandings of the risks of data exposure will help you make better decisions at the policy level.

## Security Defined

To start off, we will break security down into three main components: Physical, Human and Technical. Physical security is defined essentially as the building security for your computer equipment. Is your server in a locked room or cabinet? Who can access it? Are any desktop computers easily accessible by outsiders? Do you have adequate heating and AC ventilation where the servers reside?

Human security is the most often overlooked, but typically the biggest threat. Most security breaches come from insiders. Some of these are malicious and some are innocent mistakes. From the policy side of human security, a good approach to have when terminating employees is to have their computer access removed while the termination is occurring. Too often, fired employees walk back to their workstations and can start deleting information. It is a good idea to have comprehensive employee policies that address client information security.

The third aspect of security, technology, is the focus of this paper. Technical security encompasses a number of issues, but generally is focused on securing stored and transmitted data.

The Internet poses many risks to electronic information. So in order to understand the risks, it is good to understand how the Internet operates. The basic design of the Internet was created for the national defense interests. And as such was designed to deal with significant system failures. This means a big piece of the Internet can crash and information will flow around the damaged segments.

To help illustrate this approach, we will apply a traditional transmission method with how the Internet works. If regular US Postal mail were handled the way e-mail travels the following would occur. First, the carrier would stop in your building and pick

up your outgoing mail. The carrier would then proceed to the next building. On this segment of the journey, the mail is secure. This is the e-mail traveling from your computer to your Internet Service Provider (ISP).

When the carrier reaches the next building, they drop your mail there. At this building a copy of your mail is made, since it is printed on numbered postcards and not in an envelope. These copies may sit there for only a moment or for some period of time. The copies are held by the owner of the building (and not the US Postal Service). The building then sends copies of the mail to the other buildings on its block. In this way the various postcards may travel different routes, but will end up at the same destination. Moving forward the postcards bounce from building to building, and find their way to the recipients ISP. From here a 'secure' carrier delivers the postcards to the intended recipient. This approach might seem a bit odd, until you consider what happens when a building is destroyed. Information merely flows around it, still completing its journey.

With this approach there are obviously many opportunities for others to access the content of your messages. And they can take copies without the sender or recipient ever knowing.

This method is obviously not secure. The US Postal Service offers an end-to-end secure transport system. Whereas the Internet is a web of privately owned "buildings" that pass data.

An obvious question to ask is how often do thefts of data occur in this environment? The answer: we don't know... which highlights the problem and need to secure electronic client information.

We have explored how information travels across the Internet, but will now turn to protecting stored information from Internet attacks.

## Technical Security Components

### *Firewalls*

The first and most obvious security tool is a firewall. Firewalls act like a big wall with a whole bunch of windows (which geeks call ports). When data flows out to or in from the Internet, various windows open up and allow the data to pass through. Strong firewalls have windows that only allow the right kind of data to pass through. Hackers basically have tools that allow them to check each window to see if it is open or able to be opened. Most hackers are just kids that go online and find the software programs that will check all of the windows. Serious hackers are the ones who actually write the programs.

Firewalls can be just software or a hardware/software solutions. Networks usually employ the stronger hardware based ones, whereas software firewalls are mostly meant for desktop and laptop computers. I run a firewall called ZoneAlarm on my laptop

as a second line of defense, since I connect to a variety of networks and Internet connections with varying degrees of firewall protection.

On a policy level, you should have the logs of your firewall checked regularly. These logs tell you how often and what types of attacks are occurring on your system. This can be extremely useful information, as it tells you how you should be adjusting your security to meet these known attacks. This is like having a guard at the gate to watch for people picking the lock.

Again we can ask; what is the likelihood that your network is being attack? A recent interview with a high-profile hacker addresses this question. When asked if he targeted any companies or firms for attack he said “No.” He thought it took the fun out of hacking. Instead he would just surf for vulnerable networks and poke around once he got inside. So even though you think your law firm isn’t a target, if it’s connected to the Internet, it is. Food for thought: recently the Utah State Bar logged 800 attacks on its systems in one day’s time.

### *Virus Protection*

The next obvious piece of security is virus protection. Viruses, once insider your system, can act as tools for opening hacker access to your network as well as tools for crashing it. Virus software has two components: the engine and the virus list. Most virus software companies offer online updates to help you keep the list of detectable viruses up-to-date. As well you can automate the update so it happens regularly. I do mine every 5 days, but also do a manual update whenever I get a virus alert.

One side note is to watch for virus hoaxes. I have seen two types of theses. First is a hoax alert that asks the user to send notice of a potential virus to everyone in their e-mail address book. This approach is kind of humorous, since it tricks the humans into doing what the virus warns against. The second type of hoax is the one that gets the user to delete a “malicious” file which happens to be something useful. The most common is the Teddy Bear virus which asks you to delete a file called “jdbgmgr.exe.” When you get a virus notice you should go to the web site of your software provider and check the web site for information about the virus. It will tell you whether it is real or not and how to deal with it (even if you accidentally deleted the non-virus file). This brings up another policy note. You should have employees notify the IT staff whenever they receive any virus or virus notification to insure that the correct reaction occurs.

Another security hole occurs through Operating Systems (OS). The most obvious here is Windows. Even with a good firewall and virus protection program in place, security holes in Windows can create problems. From a policy perspective, you should have staff regularly update the OS based on security notices. An out-of-date OS can present significant problems.

On top of the OS are growing Software Application security issues. Just this week I loaded an application that kept requesting access to my e-mail address book.

Although this was somewhat legitimate for the application, it made me very nervous. This situation could create a back door hack risk into my e-mail program. Consequently, I uninstalled the software.

Microsoft recently announced that security is taking priority over functionality for its OS and applications. This is good news but will probably take 3 to 5 years to be fully in place. So for now, be diligent about ensuring that any security holes are plugged.

### *Disaster Recovery*

I prefer to refer to Disaster Recovery (DR) as business continuation. Since continuing your business operations after a disaster is your main goal. If you look at it from this perspective, it may well change your approach. DR has traditionally been creating back-ups of files. Most offices have regular tape back ups, with hopefully an offsite rotation that always keeps a copy somewhere else. Policy Point: How often is your back up tested? Retrieving files from magnetic tape is a very slow process. How much will it cost to have your office down for a day? A conservative estimate is that you will lose \$900 per day per attorney in revenue from lost billables while you are down. This highlights the point about business continuation.

Fortunately new options are emerging for DR. Two examples. First is an online backup solution. In this scenario, data is back-up securely over the Internet to a secure data center. Of course you need to do some homework about the security of this approach. But with this in place, you can access your back-ups quickly from any Internet access point. A provider of this service is AmeriVault ([www.amerivault.com](http://www.amerivault.com)).

At the top end of DR is real-time back up systems. These services create back ups of files immediately after they are saved or changed. Again think of business continuation. How much will it cost to lose a day or week of work if a disaster occurs just prior to the back up? A provider of this service is MiraLink ([www.miralink.com](http://www.miralink.com)).

An emerging method for dealing with DR is to make it someone else's problem. As a lawyer you may not want to be or employ security experts. An alternative is to store your documents on an outside, secure server. Of course you need to ask the provider some tough questions about how they manage security and ensure back ups. It is very possible that the outside technology provider will have better security practices since that should be one of their core functions. An example of a provider like this is NetDocuments ([www.netdocuments.com](http://www.netdocuments.com)). Their servers reside inside a bank's data center which is extremely secure.

To summarize and reiterate, as a lawyer you should have policies in place that dictate your back up procedures and require regular testing to make sure the back ups are working properly.

## Document Security

A new security issue that is emerging is that of document security. MS Word has a 'feature' that embeds information in all Word documents. Some of this information is 'metadata' which tells you who created a document and when. Some of the information may be deleted content. Lawyers should be very careful about inadvertently passing this client information that may be hidden in the document. The metadata might reveal an original source of a document that exposes a client confidence. The deleted data could expose a host of client confidences and seriously harm a client's interest. Imagine having terms from a former deal revealed to the current deal opposing party?

There are software programs available for "cleansing" Word documents of this data. There are two poor man's approaches you might want to try. First is saving a file in .pdf format. This eliminates both types of data but results in a much larger file size. The second approach is to save in .rtf file format. This cleanses and leaves a much smaller file format. As well .rtf documents can be read by WordPerfect.

## Ethics – the Moving Target

This discussion brings us around to the ethical landscape. The MDP debate taught us that Client Confidentiality is one of the three pillars of the profession. This is for good reason.

Most ethics rules or opinions on securing electronic client data to date have focused on the transmission of electronic data. The presumption is that stored data will be subject to the same protections as stored paper. Hopefully the discussion above has illustrated that there are unique concerns for protecting stored electronic information. What I expect is that once a breach becomes public through discipline, standards of care will evolve. My suggestion is that you put protections in place now to avoid becoming that precedence setting lawyer.

On the transmission side of things a number of bars have spoken out, but the voices have not been entirely consistent. Additionally the ABA issued Ethics Opinion 99-413 which essentially states that e-mail is like mail and therefore it is reasonable to expect that communications sent through e-mail will be secure. Given the description above about how information travels across the Internet, I personally do not believe there is a reasonable expectation of security and privacy for e-mail. Even though it is illegal to intercept e-mail (as the opinion points out) it is so much easier to intercept than mail that the presumption of privacy is weak. Again, I suggest you take steps to avoid being the test case for this issue. You should check with your own state bar for current ethics rules or opinions on this subject.

## Special Financial Practice Highlight

The federal Graham-Leach-Bliley Act (GLBA) was directed at banks. The intent of this law was to require financial institutions to inform their customers on an annual

basis about their privacy policies. These policies typically come in the mail in the summer. As well, the banks are required to properly secure any electronic customer data they hold. For what is privacy without security?

The SEC has preliminarily ruled that lawyers who have a “financial” practice will need to comply with GLBA. It is my understanding that the ABA and the New York State Bar promptly appealed this ruling on the grounds that lawyers already have a higher duty to secure client data and that it could put undue burdens on legal services organizations that might have to comply with the notice provisions.

The jury is still out on this issue. However, if you have a financial practice you should be aware of this issue and become knowledgeable on the security guidelines being develop for GLBA. Check with the SEC for updates ([www.sec.gov](http://www.sec.gov)).

In closing on the ethics issues, the standards of care will continue to evolve. As lawyers you should keep in mind your ethical duties and takes steps to insure the security of your clients’ information.

### Protecting the Goods

There are a variety of tools available for protecting e-mail communications. And there are two basic approaches for addressing this. First is to encrypt your e-mail. Outlook includes some options for encrypting or “digitally signing” messages. However, if the recipient uses another program, they might not be able to read the message. In this case, you can try a test message with a client to ascertain compatibility.

Next is a tool called PGP, which stands for pretty good privacy. It is actually very good privacy. With PGP you will need to share a password with the recipient. This can be cumbersome if there are many clients involved. Finally, there are providers emerging with point-and-click solutions for encrypting e-mail. You should check the Internet for these as many are starting to appear.

Following on our ethics discussion, you may not need to encrypt all communications. My suggestion is to use your judgment and apply a level of security that matches the sensitivity of the information being sent.

The other method for securing e-mail is to not use e-mail. There are vendors that provide secure relay tools and services. In this scenario the lawyer securely uploads a document or message to a secure site. Then the client establishes a separate secure connection to the same site and downloads the document. A number of online legal sites are starting to offer this service.

Again the watch word for lawyers is; Policy. Smart policies for managing your electronic communications will go a long way towards reducing the risk of exposing client data to third parties.

## Conclusions

There exists a higher duty for lawyers to protect and secure client information. Following from that, lawyers should take steps to understand and manage electronic client information in a thoughtful fashion.

The Internet is an inherently insecure medium. Numerous threats exist for stored and transmitted data. Additionally data can be compromised without the lawyer ever knowing. This situation demands that lawyers put in place policies and procedures to effectively secure electronic information.

Fortunately many tools exist and more are entering the market each day. Look to your bar association for new tools and education on the topic.