

First Steps in Security

Every firm takes their IT security seriously, but in such a fast changing environment this may not be enough. In large organisations, dedicated security personnel from both IT and the business can make sure that systems and policies are kept up to date with new risks and new working practices. In smaller organisations, including almost all law firms, staff have broader responsibilities. They therefore find it hard to spend as much time on security, which has no immediate or visible benefit, as they would like.

The result of this is that IT security arrangements change quite slowly, normally remaining the same for some period of time before being reviewed and overhauled at infrequent and possible long intervals. Like business in the modern world, to stay still is actually to move backwards. With IT security, new risks are occurring all the time. This may be caused by new forms of attack or methods of breaching security being found that need to be stopped. Just as often, changes to business practices open up new areas where security may be breached, or invalidate existing protection.

In this article we are going to look at three different areas where the cracks may be beginning to show. These are will not be the major problem areas for all firms, and will certainly not be the only areas that should be looked at, but they should be a useful starting point for any law firm.

Perimeter security

Fortress style security has been the starting point since someone first decided that protecting their network was a good idea. Making sure that the boundary cannot be breached provides much of the protection of any system and this is a principle that applies not just to IT.

The first review should look at three key changes in perimeter security:

- The perimeter has moved;
- The perimeter has already been breached;
- The perimeter has inherent weaknesses against new threats.

The advent of mobile working has moved the boundary of the IT network outside the physical building. Each laptop and Blackberry now represents a device that exists outside the traditional firewall, especially where they may be connected to public broadband internet connections. With the boundary now wrapping closely round these devices, the use of personal firewalls and other local security measures should be carefully considered.

Wireless networking has also moved the boundary. In many ways the solution to this is simple. As it is impossible to control where radio signals reach, the only real solution is pull

the security boundary in and address all wireless networks as outside the secure network. Once this is done, wireless can be a very useful new addition to your infrastructure.

In most networks, the core of the perimeter security is the firewall. This is not a complete barrier however (it would be more secure if you unplugged it and disconnected the internal network from the internet), and holes are opened up for specific purposes. As the internet is used for more and more purposes, a greater number of these openings in the firewall are created, leading in some cases to firewalls resembling a sieve more than anything else. As any new threat has to be compared against all the rules a firewall has, the simpler it can be set up the better. This is largely a case of balancing risk against business requirements, but a sensible approach to keeping the firewall configuration under control is to have a regular manual check of the rules, to see which are no longer required, which are now too risky or need to be tightened up. In addition, regular checks from the outside by a specialist company (penetration tests) should be standard to make sure everything is as secure as you think it is. At the end of the day, the only way to make sure a boat is watertight is to put it in the water and see if it leaks.

Because firewall rules and other security measures are put in place based on the environment that exists at the time, they may become a liability as that environment changes. A common example of this occurs where a firewall has been set up to allow through traffic that was considered safe at the time. Later this safe traffic may become a method that can be used for attack. Firms should reconsider areas where information flows in and out to see if current protection is still adequate. Many organisations will have allowed all web access from all internal PCs, in effect allowing them to communicate with any computer on the internet using HTTP. In the past, this represented an acceptable risk in most cases, but now this broad access can be used to breach security. Removing web access from users is unlikely to be acceptable to the business, so a change is needed in how this requirement is met. Putting in place a proxy server located in a neutral or isolated network (DMZ) will help. Choosing a proxy server that can scan content for viruses, trojans and other forms of attack will increase security further.

User identification

There are two aspects to user identification in IT security. Everyone is familiar with the concept of the system having to check a user ID using a password or other method of authentication. Many organisations forget that much of the security of this depends on the checks done before a user ID is issued. It does not matter how complex an IT system you put in place if a valid ID is given out to any temporary secretary or contract worker, one of whom turns out to work for a criminal gang or terrorist organisation. In law firms, confidentiality issues mean that problems can occur even with legal and honest staff if appropriate checks are not made.

When it does come to thinking about the authentication method, firms need to be aware that passwords are becoming less and less secure, as recent cases of identity theft have shown. Many firms also forget that additional non-computer based mechanisms may play a part in reducing risks in the office that do not apply for remote users. The standard difference is that in most smaller offices, visual identification by colleagues forms part of the IT security as well as the physical security, and strangers trying to log on in the office will be challenged. Remote users with laptops, or people trying to get in using remote access facilities will not be subject to this check, and simple passwords are unlikely to be a strong enough mechanism. With the advent of SMS based two factor/one time passcode systems, the costs of implementing better security are significantly lower than in the past, and there is little reason not to do so.

Storage

The big issue with storage is that there is now so much more of it, and that it is much more portable. The first point causes major problems with protecting data with backups and planning suitable recovery procedures. Unfortunately the cost of backups has not fallen to compensate for the growth in data, so adequate storage protection is now significantly more expensive than it was. One of the most important things a firm should do is make sure that the budget is still sufficient, and that they do not have IT staff unable to ensure data can be recovered as they have a lack of funds.

The other huge problem is that data is now very portable. When the risk of data theft was based on how many floppy disks someone could realistically carry out of the building, this was not a huge issue. Now they may regularly take a laptop with many Gigabytes of data on it, or load similar amounts of data onto an iPod. At the smaller end, enough data to be extremely damaging can be stored on a tiny USB memory stick. Loss of this data may be due to carelessness, theft or criminal intent, but all cases present a considerable risk that firms should be examining. Encryption of business data on approved devices is one step forward and is perfectly achievable, but also required is a firm policy on who can access and remove information, and what their responsibilities are.

Adam Westbrooke is the managing director of Firstcourt, a strategic IT solutions company specialising in helping professional services firms. For more information call Adam on 0870 350 3660 or see <http://www.firstcourt.co.uk>.