

Security

Security is bit like drains: important, but not very exciting, so no one really wants to take responsibility for it. It is however vital that it is done correctly because if it goes wrong, as with drains, you will end up with a very unpleasant situation that everyone will know about.

Knowing what to do about security at management level is no longer a complete mystery. Since the publication of the ISO guidelines on information security (ISO 17799) a good, standard reference has existed that can be used as a starting point. The problem with a universally accepted set of guidelines for those people trying to ignore the issue is that they quickly get used as a definition by others who need to make sure your business is not a high risk. Insurers, regulators and even clients will more and more start to expect this as a minimum standard. Some may even require your firm to be certified that it meets the much more detailed British Standard (BS7799), and one or two firms such as Kennedys have pre-empted this by gaining that certification.

So, according to best practice, what should firms be looking at to demonstrate that they are effective in looking after their own and their clients' information?

Business continuity planning

This is not about having a disaster recovery plan written ten years ago that no one knows about, although an up to date plan is an essential part. Business continuity is also about ensuring that small failures of systems do not affect day to day business. Many firms are seriously exposed in this area as they procedures have not caught up with the rapid growth in the use of IT and the amount of information stored. Where once a failed mail server could have been restored from tape in an hour or two, and few people would have noticed, a large modern server may take more than a day to recover from tape, and clients and partners will be screaming after about five minutes.

To address this problem, each system needs to be looked at and a decision made as to how long it could be out of action for in the event of an isolated problem (as opposed to a major disaster where clients will give you more leeway). Then you need to plan how you can recover the system within that timescale. In some cases this may be simple, but critical components such as the firewall or the document management system may prove hard and costly to bring to this level.

Access control

The traditional view in law firms has always been that the staff can be trusted and information should be available to all. Definitions of confidential information tend to refer only to internal partnership and staffing information and not to information held on behalf of a client. The guidelines expect information access to be restricted to those who require it do their job. There is an additional requirement that access is logged and the audit trail is checked in order to detect misuse of information.

In law firms a particular difficulty here is the relationship between a secretary and their partner. It is essential that the access granted reflects the different positions and requirements, and that an assumption is not made that it should be equal. Even more importantly from an audit point of view is that the identification of the user on the system must be unique to the individual. Allowing secretaries access to systems under a partner's identity is a very high risk strategy and open to abuse with little chance of detection or sanction.

Development and maintenance

While most firms do not do large scale development, almost every firm has some in house software from Word macros upwards. The guidelines expect security and prevention of data corruption or loss to be an integral part of this, but how many firms have sent any of their developers or IT staff on any form of security training?

In industry at large, the most common serious security failure in software is not from the much derided Microsoft, but applications written in house, and in particular those presented to the outside world as extranets. It is very common to find elementary mistakes in the design of these systems that allows the security and authentication mechanisms to be bypassed. What makes this worse is that such security breaches are often undetectable as the systems are also missing the necessary audit records and checks that would have identified them.

Physical security

This is normally completely ignored in IT security plans, but can prevent some of the most damaging incidents that can occur. The obvious physical security elements concern prevention of theft. Central server rooms should not only be protected by checks on people coming into the office, but they should also be physically secured against unauthorised staff internally. It is probably true for larger firms that not all IT staff should be authorised either.

While malicious damage may be rare, disgruntled former employees or even clients can cause a lot of damage very simply. Central power and telephone connections are often

located outside the traditional security perimeter, especially in a shared office, but disruption to either will prove catastrophic to any law firm.

A more recent but growing threat is the physical theft of data. Catching someone walking out with a key document on a floppy disk has always been difficult, but now vast amounts of information can be downloaded onto a tiny USB memory stick and removed from the firm. With the widespread adoption of hard drive based music players like the iPod, and even some mobile phones having huge storage capacities, the potential for very simple theft of enough information to ruin the reputation of a firm if it made public is not something that can be ignored.

Compliance

The compliance requirement for law firms in the area of IT security is a very topical issue, but no one is any doubt that it is growing. Increased regulation and an increased understanding of the risks will lead to much greater controls being placed on IT departments and firms' overall policies. Data retention policies are likely to become tighter.

An important change in this area will be as firms move away from using a paper file as the main client record and start to have totally electronic matter files. The technology to do this now exists in a practical and cost effective manner, but the barrier holding back the adoption of this is that these electronic files will then fall clearly under the Law Society's regulations. This will have a significant impact on the IT systems used and the way they are managed.

Personnel security

The legal sector has become much more familiar with the concept of 'know your client' recently. While there may be complaints about the extra administration most people understand that you need to know who you are doing business with. The same checks should be applied to staff, both temporary and permanent.

According to xx the number one threat over the next year will be fraud and information theft by internal staff, either employees or contract staff. By far the easiest way for a less than scrupulous company to obtain an edge in litigation or commercially sensitive transactions would be to get someone in the opposing side's law firm as a temporary secretary or in the post room. Few firms conduct their own checks on temps, relying on the agencies, and even then these checks are likely to be limited to taking a copy of a passport. Extra special care needs to be taken with IT staff who have much wider access coupled with the knowledge of how to use it.

Even at a basic level, what checks are made when recruiting support staff from another firm that there is no conflict of clients with the possibility of confidential information being disclosed, even if accidentally.

The other aspect of security relating to staffing is the procedures for staff joining and leaving. You can have the best procedures in the world, but if you do not tell new staff about them they are not worth the paper they are written on. Just as importantly for leavers do you have the mechanisms in place to ensure they have returned all their equipment and returned or deleted any data they may have? Do you even have any way of knowing what data they do have, especially if they have been a trusted employee for many years?

Security organisation

The objectives of this section are:

- (a) To manage information security within the Company;
- (b) To maintain the security of organizational information processing facilities and information assets accessed by third parties.
- (c) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Network Management

The objectives of this section are:

- (a) To ensure the correct and secure operation of information processing facilities;
- (b) To minimise the risk of systems failures;
- (c) To protect the integrity of software and information;
- (d) To maintain the integrity and availability of information processing and communication;
- (e) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- (f) To prevent damage to assets and interruptions to business activities;
- (g) To prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control

The objectives of this section are:

- (a) To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy

The objectives of this section are:

- (a) To provide management direction and support for information security.

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