How good is your disaster recovery plan?

Peter Scott

Is it a mystery to all or the lynch pin of your firm's strategy? Read our guide to avoid being caught out

I pose the question in the title to this article because I believe, from what I see in the legal profession, there is a need, especially for smaller law firms, to focus a great deal more on applying *effective* risk management strategies to all aspects of their operations and, in particular, to those risks to their operations that potentially can destroy or severely debilitate a law firm, with consequences for their clients, their people and their owners. Such plans should be real plans and should be communicated to and understood by everyone in a firm, rather than just being theoretical tick-box exercises to achieve compliance that are then put away in a cupboard and forgotten about, which I fear some are.

Law firms need to build into their operational procedures and infrastructure the ability to identify, and to assess the impact of, all the risks to which a firm may be exposed. In large law firms this has meant the appointment of risk managers and other inhouse specialists who are responsible for managing risk and, because they are able to use their extensive internal resources, large firms are likely to already have in place well thought-through and sophisticated disaster recovery plans. I have therefore focused this article more towards smaller firms, which in terms of law firm numbers make up the bulk of the legal profession but which often lack sufficient internal resources to put in place effective disaster recovery plans.

Disaster recovery planning is a very large topic and so in this short article I have deliberately not set out to do more than to challenge firms as to their disaster recovery planning and to suggest some possible methodologies that smaller firms may wish to use to compare with their existing approach to managing such risks.

When discussing this topic it is important to understand the different terminology that is often quite loosely used. Sometimes the term 'disaster recovery plan' is used in the context of only focusing on planning for how to respond to and recover from a disaster that has occurred. The term is also used when discussing the process whereby a business needs first to identify risks that may cause disasters and to take steps to prevent or otherwise minimise those risks, although this process is also often described (perhaps more accurately) as 'business continuity management'. For the purposes of this article, I will refer to both aspects as 'disaster recovery planning'.

The prime objectives of a disaster recovery plan should be:

- to identify and assess risks to the continuity of a firm's operations;
- to put in place control responses to those risks with a view to their avoidance, mitigation or transfer (e.g. insurance arrangements); and
- to develop, test and document an easily understood plan that will help a firm recover as quickly as possible from a disaster that interrupts its operations.

SRA regulatory requirements?

What are law firms required to do to comply with Solicitors Regulation Authority (SRA) regulation regarding disaster recovery planning?

Law firms regulated by the SRA must always have regard to that 'catch all' requirement in principle 8 from the SRA Handbook, which states that:

'You must run your business or carry out your role in the business effectively and in accordance with proper governance and sound financial and risk management principles.'

In addition, if a law firm is unable to operate even for a short time because of a disaster occurring, then it is unlikely that it would be able to achieve many of the outcomes in the SRA Code of Conduct. For example, the outcomes in chapter 7 (management of your business) need to be noted carefully in the context of risk management, including:

- outcome 7.2: '**you have effective systems and controls** in place to achieve and comply with all the Principles, rules and outcomes and other requirements of the Handbook, where applicable';
- outcome 7.3: '**you identify, monitor and manage risks** to compliance with all the Principles, rules and outcomes and other requirements of the Handbook, if applicable to you, and take steps to address issues identified'; and
- outcome 7.5: '**you comply with legislation applicable to your business**'.

Beyond those specific SRA regulatory requirements, if a firm is Lexel accredited, it will also be required to adopt a disaster recovery plan to address emergencies that might disrupt its operation.

How adequate is your disaster recovery plan?

What should be considered when assessing whether a firm's disaster recovery plan is adequate for the task?

Of primary importance is the need to ensure at the outset that responsibility has been assigned to a person or persons in a firm for:

- creating and monitoring the disaster recovery plan;
- ensuring that all the firm's people understand how the plan is to be executed and their duties in implementing it;
- continuously keeping the plan up to date to take account of changing circumstances and improving it by periodic testing in a simulated environment;
- detecting and communicating disaster events occurring;
- activating and executing the disaster recovery plan.

For SRA regulatory purposes, the compliance officer for legal practice (COLP) has responsibility 'to take all reasonable steps to ensure compliance with all the requirements of the SRA Handbook', which will include the requirement that the business is run in accordance with sound risk management principles under principle 8, mentioned earlier. Accordingly, all aspects of disaster recovery planning listed above are likely to be within the scope of a COLP's responsibility, whether it is the COLP or someone else who actually executes the work.

A firm should then consider each phase of its disaster recovery planning as follows.

Have disaster risks to a firm's continuing operations been identified and analysed?

The phase of planning to identify risks should be a starting point when looking at the adequacy of a firm's disaster recovery plan. Unless this process has first been carried out, then a plan is unlikely to be fit for purpose in managing risks to a firm's operations. As Donald Rumsfeld famously once said:

'There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.'

This phase of the process will involve identifying risks that can bring about disasters and then carrying out risk analysis of those threats to a firm's business continuation. A firm-wide approach should be adopted and should involve every function, group and office in a firm.

To do this a firm should begin by listing its essential activities, which are those that, if interrupted, would disrupt the firm's operations and cause loss. These activities will need to be *prioritised* based on their importance to the continued operation of the firm. For example, some of the most important essential activities in a law firm will include:

- people being able to work/get to work;
- use of office space;
- use of data systems;
- use of office equipment, such as desktops and work stations;
- use of communications equipment and facilities, such as telephones and networks.

A firm will first need to ask itself some searching questions about its knowledge of every aspect of those activities that it has prioritised before it can begin to identify and then assess the risks that may impact on it. For example:

- What knowledge do we have about each of those activities?
- Where is this knowledge?
- Has it been captured and stored or recorded anywhere or is it just in someone's head?
- If the knowledge is in people's heads, how can we ensure those people remain with us?
- If the knowledge is stored or recorded, is it under our control in files, in documents, in an IT system, and can it be freely accessed by those who need it?
- Do we have systems in place that, on a continuous basis, enable us to monitor that knowledge (and the risks to our firm related to that knowledge) and to review the effectiveness of our risk management procedures to reduce or eliminate those risks?
- What are those systems, who has knowledge of them, how are they operated and who controls and has access to them?
- Do we have gaps in our knowledge and how can we identify them?
- How can we fill in these gaps in our knowledge?

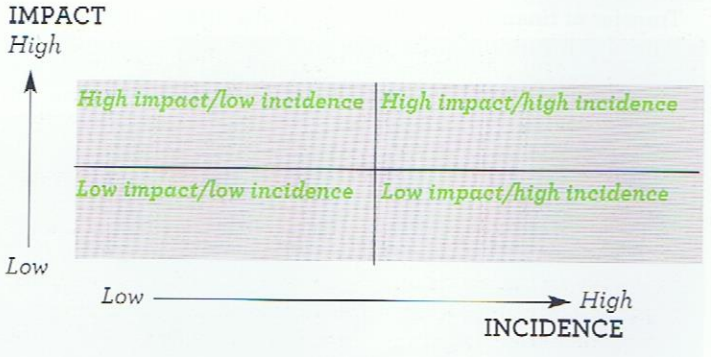
In relation to each prioritised essential activity, all possible risks then need to be identified, and some of the most important are likely to include:

- data systems failure;
- power failure;
- flooding;
- fire;
- loss of a building/loss of access to a building;
- loss of data;
- hacking into data systems;
- public transport failure;
- human risks;
- civil disorder;
- natural disasters;
- suppliers and utilities.

A useful technique to use to identify and then assess such risks is brainstorming, which is a term commonly used today for group sessions to create new ideas. Bringing together relevant groups within a firm to create or gather ideas to brainstorm can be a useful way of identifying risks in respect of any function of a law firm and can be more effective than individuals working alone in generating ideas in relation to identifying and assessing a firm's risks. Questions to be considered might include:

- What processes should we follow to identify the risks to each essential activity in our firm?
- What knowledge do we currently have of the risks to which we may be exposed in each activity?
- Has any risk identification and assessment been carried out in the past?
- Do we have any records of such risk identification and assessment?
- Do we have gaps in our knowledge in respect of the risks to each essential activity?

A firm should then carry out a risk assessment taking into account the likelihood/frequency of the possible risks identified to each essential activity and the impact an occurrence of each risk could have on that activity, the firm, its people and its clients, using a technique such as *risk mapping*, which is a method of analysing probability or incidence versus consequences or impact as illustrated below.



The process of analysing risks in this way against their impact on the ability of a firm to continue its operations will not only enable a firm to understand, assess and categorise its risks, but will then point the firm to the steps it will need to take to eliminate, reduce or transfer those risks.

Has a firm adequately evaluated its responses to risks to its operations?

Once a list of prioritised essential activities has been prepared and the risks to each activity have been identified and assessed, it will then be necessary for a firm to consider in respect of each activity the various responses in order to either:

- mitigate or transfer those risks; or
- in the event that a risk 'crystallises' or occurs, to consider various recovery methods available and to decide the most suitable response.

To do this will involve applying *gap analysis* techniques to risk identification and assessment that will enable a firm to compare **its risk profile**, as shown by the risks to its critical activities it has identified and assessed, against **the objectives** it has identified as being required to be achieved in relation to those critical operations, in order to highlight existing gaps. Gap analysis should force a firm to consider the current risks to its operations and to identify what it will need to do to achieve, through effective management of those risks, the operational objectives it has set.

We now look at each of these in turn.

Mitigation or transfer of risks

A firm will need to put in place plans designed to prevent identified risks to each of its critical activities from occurring. Again, using brainstorming as a technique within a firm can help to identify the measures needed to be taken in relation to each essential activity to prevent disaster occurring. For example, in the case of data systems, such measures will usually involve having critical systems replicated elsewhere and putting them online with the latest backed-up data available.

For each identified risk in relation to each essential activity, a firm will need to consider its most appropriate response to prevent a risk crystallising so as to be able to maintain its activities. Factors to be considered are likely to include, on the one hand, a firm's statutory and regulatory responsibilities (which may clearly define the risk management measures to be taken), while, on the other hand, where it is reasonably and justifiably considered that a view can be taken as to the level of risk management needed, the cost/effectiveness involved of any risk responses.

Transfer of financial risks arising out of a disaster happening will involve insuring against risks occurring and, as part of disaster recovery planning, a firm should carry out a comprehensive review of all its risks relating to the critical activities it has identified, with a view to ensuring that, despite its risk mitigation measures taken, at least financial risks involved are, if possible, insured against. There may, however, be certain residual risks in relation to aspects of a firm's critical operations that cannot cost-effectively be prevented or the financial consequences insured against, in which case a firm will either need to exclude such risks by, for example, discontinuing an activity or considering how it can recover those activities if a risk crystallises.

Recovery methods when a risk has crystallised

It will primarily be the people in the firm who will be required to provide the technical and management skills to ensure a smooth recovery. Accordingly, a recovery plan should ensure that, in the event of a disaster, the people in a firm clearly understand who should be contacted and how notification procedures are be implemented to ensure communication can be established and maintained while recovery responses are put in place. A disaster recovery plan should clearly provide how those responsible will be required to activate the recovery plan and then execute it with a view to restoring the firm's operations as quickly as possible.

The danger is always that a firm will merely document a detailed recovery plan that will exist in theory only and gather dust on a shelf, instead of ensuring in practice that:

- it is an effective recovery plan designed to achieve the realistic objectives a firm has set itself for recovery of its critical activities;
- on a regular basis it is clearly explained to the people in the firm so that everyone understands the plan;
- those responsible for implementing recovery are trained to effectively carry out their roles, including regular refresher training;
- the recovery plan is regularly 'tested' in response to specific risks occurring in a simulated environment and responses reviewed and updated as a result; and
- with a view to complying with SRA principle 8, all the above actions are fully documented so that, if challenged, a firm will be able to *demonstrate* that it has taken steps to ensure it is run in accordance with sound risk management principles.

So, assessed against all the above, how good is your disaster recovery plan?

Peter Scott *runs his own professional consultancy practice, Peter Scott Consulting.*