Crisis management for law firms dealing with data leaks

18/04/2016

Practice Management analysis: Following the recent spate of high profile data leaks, Tony Williams, principal of Jomati Consultants, examines the legal obligations placed on law firms which have been implicated in a crisis and offers advice on what steps they can take to address issues which might arise.

What are the key types of crises that can affect law firms?

The crises that can hit firms can be of an internal or external nature. Internal crises can include a major defection of partners or a practice group, a major claim by a client, a partner being arrested or something of that type or a major breach of security from someone from within or outside. Most of these are reputational issues.

Then there are external crises like a major problem in the country in which a firm operates—like a coup, a terrorist attack which would cause them to lose everything or to massively disrupt their business or a natural disaster of some kind. All of these events may be relatively rare but nonetheless the likelihood of any one of them occurring has to be addressed.

What are the first steps firms should take if they are implicated in a crisis, data leak or scandal, if they have engaged in conduct that was illegal or could be seen as ethically questionable?

This relates to the first group to which I referred. In these cases the classic scout motto—be prepared—applies. Firms must ask themselves what their responses would be and what procedures should they have in place to address these events. While you can't be totally prepared for every eventuality, you can still have a good crisis plan in place. This would address matters such as:

- Who would be in the crisis team?
- Who its leader would be?
- Who would be the spokesperson for the firm?
- What external support would be needed?

Firms that think all these things through before a crisis arises are in a stronger position when it occurs.

If the crisis relates to an individual or say a partner, you would also need to consider what your response would be. Would you suspend the partner? Under the terms of the partnership agreement or employment agreement, would you have the right to do so?

As to the loss or leaking of data—firms may want to think about how much data should be readily available within the firm and on what devices. Firms could also ask whether say, material that is more than two years old should be archived. They may need to grade data so that only certain kinds of data are available to certain higher ranking individuals. It may be that certain data should only be available to people when they have gone through certain security clearances. If people are leaving the firm, their downloads may have to be monitored. Preplanning is necessary.

Some firms test their crisis management plans and sometimes with external consultants. Certain scenarios can be tested to determine how well they are prepared to manage and mitigate certain risks. These include getting out information on any crisis that is occurring. Often saying 'no comment' isn't on. Firms have to decide what to tell staff, clients and regulators as well as the general public. You must be able to respond quickly and your messages must be consistent.

What if they are the source of the documents? How should possible hacks/employees who may have stolen documents and breached confidentiality be addressed?

This is more challenging. Firms must recognise that hackers are now more sophisticated. Employment contracts should have strict provisions on matters like confidentiality. Access to data and client information should be regulated. As mentioned above, the management of data and its storage and security is vital. Many firms now may need more rigor in

the management of their systems and must test them. Until now, the hacking of professional firms has often related to price-sensitive information that can be traded so it often hasn't become publicly available. But leaks to the public can be more malicious. Every firm will have to think about this scenario now.

What legal obligations are firms under once the leak has come to their attention?

These may vary from country to country. Firms obviously have obligations of confidentiality to clients. Clients would expect that they would be informed of any crisis that had an effect on them and would expect their firm to do everything to address and mitigate any risk or damage to them. This may include, for example, pursuing injunctions or any other legal remedy available. Firms may also have a duty of disclosure and a duty to act imposed on them by regulators.

What are your best practice tips?

Firms must now review their crisis plans and ensure that they are using the latest tools—like any software available—to prevent and deal with crises when they arise. They must follow any best practice on the storage and access to data and ensure that their employment contracts are up-to-date. All the pieces have to fit together. I suspect that clients increasingly will be asking about the security systems of their advisors now so firms must be doubly prepared.

Interviewed by Diana Bentley.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor