Data security breach: Part 2 — How to respond in a crisis and reduce risk

In the second of a two-part series of articles on data security breaches, Ashley Hurst, Partner, and Louise Lambert, Senior Associate, at Olswang LLP consider how best to respond in an information security crisis to reduce the risks involved

Against a backdrop of increased cyber attacks, increased fines and the proposed changes to the EU data protection regime, there has never been a better time to take stock and ensure that you are best prepared to respond to any data security breach, be it as a result of a hack, process failure or employee error.

In the last issue of *Compliance & Risk*, we looked at the legal landscape that applies to data security and some of the challenges that may arise in a data security crisis.

In this second part of our two part article, we address the practical consequences of a data security breach, including how to respond in the immediate aftermath.

We also consider the steps that businesses can take now to reduce their risk.

Staying calm in a crisis

In the age of electronic media, the potential to lose a vast amount of information quickly and for that information to be disseminated at great speed is enormous, so acting swiftly to work out what has gone wrong and contain the breach will be of the essence.

Well-informed, tactical decision making will be required at the outset to limit reputational damage and the risk of regulatory action or criminal investigation.

Strategic thinking will also help limit disruption to business and potential claims by third parties, as well as the disclosure of commercially sensitive material to competitors.

A team approach to the problem

Effective management of a data security crisis will typically involve a large cast of people, but requires a coordinated approach.

IT security experts will be working to establish and contain the breach, possibly with legal assistance to track down the perpetrator using technical information and court orders.

Public relations and communications advisers will be engaged to handle the perception of the breach externally, including through social media channels.

If the incident is serious, there may be an investigation by internal audit. And the involvement of the legal function will be important not just to advise on legal risk and regulatory requirements, but also to retain confidentiality and legal privilege where possible.

Authority to act

The above-mentioned are just some of the potential players involved and, as the cast list grows, so does the need for communication protocols and effective lines of reporting. In times of crisis, some people run for the hills (perhaps in fear for their jobs) and others step forward and see their chance to assert authority and make a play for promotion. Those at the forefront of decision-making must be able to handle all of these personality-based and political factors, as well as obtaining a mandate to make decisions.

For example, who has the final say on whether to notify the data protection regulator of a data breach? Who decides what to tell customers and the press? Who decides whether to terminate a supplier relationship or the employment of an incompetent member of staff?

Often, making no decision at all can be worse than making a bad decision, and where speed is of the essence, as is usually the case with a major data breach, it will be vital to take decisions (preferably the right ones) and to communicate them internally and, where necessary, externally.

This cannot happen if the necessary authority to act has not been obtained. Sometimes, the authority to act may be obvious, such as when the Chief Executive is centrally involved. But often dealing with data security breaches is delegated to senior

(Continued on page 10)

(Continued from page 9)

officers of the company and what the General Counsel thinks may differ from what the COO or Director of IT think. Such conflict can cause delay unless it is clear who has the final say.

There may not always be time to convene a board meeting, so it must be clear who is in charge and what the scope of that authority is. If necessary, this should be recorded in board minutes and revisited as the crisis develops.

Data crisis checklist

Whilst it may be easy in calm conditions to list what needs to be done in a crisis, plotting a clear plan of action once disaster has struck may prove more challenging.

Businesses should therefore ensure that they have proper procedures in place, and tested, so that they can react appropriately and speedily in the event that the worst does happen.

A company's data security crisis checklist should include the following:

- Appointing a senior team to handle the crisis, possibly including experienced external counsel.
- Establishing chains of communication between the in-house team and external counsel to maximise the chance of communications and documents being protected by legal professional privilege. This applies during and after the immediate crisis.
- Getting the facts straight to establish what information has been compromised and how it happened.
- Containing the vulnerability that caused the incident.
- Formulating external messaging, including via social media as appropriate.
- Containing the spread of information in the media, particularly online. A twin track approach by public relations advisers and media lawyers might be helpful to limit potentially damaging publications.
- Notifying the regulators as required by law or as appropriate, though companies should beware of over-notification. Depending on the information concerned and the seriousness of the breach, notification may not in fact be necessary, and would simply draw unwanted attention to the problem.
- Notifying affected individuals as required by law or as appropriate. Where notification is given, this should include relevant guidance for reducing the individuals' own risk, for example ensuring that passwords for accessing 'at risk' data are reset. Again, companies should be careful not to over-notify and cause unnecessary panic either within the organisation or externally.
- Preparing for complaints and claims by third parties.
- Considering action against third parties responsible for the incident. If the perpetrators of the breach are anonymous, it may still be possible to trace them using technical information and court orders against third party intermediaries.
- If the breach is extremely serious and there is a threat to life, notifying the police. Where such a threat does not exist, companies should be aware that reporting the breach to the police may take the matter out of their hands, including in relation to how the breach is communicated externally.

"Analyse the vulnerable areas in the business, based on a fully informed risk assessment of the data handling processes and policies across the organisation. The assessment should include the risks of using third party providers and the risks inherent in the company's supply chain"

Proactive risk reduction

Of course, it would be preferable if the data security breach could be avoided in the first place. Proactive risk reduction may help to guard a business against cyber attacks and other data security breaches.

As with other business critical risks, prevention is better and very considerably cheaper than cure. We recommend that in order to reduce the risk of future breach, companies should take the following steps now:

- Analyse the vulnerable areas in the business, based on a fully informed risk assessment of the data handling processes and policies across the organisation. The assessment should include the risks of using third party providers and the risks inherent in the company's supply chain. A business is only as secure as its weakest link in the chain.
- Consider how company resources should be deployed to target the most critical areas in the most effective way.
- Create or update the company's records management and retention policies to ensure that data which it is not legally required to maintain, or has no legitimate business reason to maintain, are promptly and securely wiped.
- Create and ensure compliance with data access protocols and limit staff access as appropriate.

- Make sure that information security arrangements are properly checked for all transactions within the organisation and that appropriate provisions protecting information channels are included in the transaction documents.

- Ensure that the organisation's data security policies cover home and mobile working and comply with best practice, such as the UK Information Commissioner's guidance on 'Bring Your Own Device' concerning employees using their personal computing devices in the workplace.

- Put in place a data security incident plan with an identified crisis team (including legal and public relations personnel) with clear reporting lines and the possibility of escalation of serious issues to board level where necessary.

- Keep a record of the company's obligations to notify regulators, customers and employees, and identify a notification subject matter expert.

- Create standard questionnaires and risk assessment reports to be completed following a breach, with clear escalation paths.

- Ensure that appropriate backup policies are in place.

- Implement a comprehensive training programme on data security for all staff.

- Review insurance cover for cyber breach and data loss risks.

Risk assessment

A compliant organisation is not always a secure one. Given the large volume of law and regulation and the complexity of global IT systems in an increasingly extended supply chain, there is often a temptation to "tick the boxes" and adopt standard policies and approaches. This can include certifying to general information security standards across the board and relying on contractual terms, without necessarily "looking under the bonnet", resulting in a poor focus, unnecessary cost, and failure to achieve the objective of making the organisation more secure.

Organisations need to address two discrete areas of risk, both of which can lead to significant reputational damage:

- operational risk arising from information security breaches (including theft of intellectual property and confidential information); and

- the risk of legal claims and regulatory fines for non-compliance.

Risk assessment tools are now available which address both of these areas of risk and are designed to:

- put organisations in control of the information gathering process in order to keep costs down;

- provide a fully auditable log of entries;

- identify conflicting and inaccurate information by providing a single collection point for all data, therefore reducing risk and delay.

In any cyber risk assessment, companies need to identify, evaluate and prioritise the risks that are specific to their organisation rather than simply using an off-the-shelf service and testing provision.

The cyber risk assessors therefore need to obtain an understanding of the business in question, conduct a direct technical analysis of its key systems and provide on-going monitoring of today's cyber threat environment.

This enables companies to make active business decisions on how much risk they want to accept and how best to deploy their resources.

The purpose of the risk assessment process is to identify flaws and gaps in security and legal compliance with a view to agreeing how to refocus resources and improve security and compliance.

To encourage candour throughout the process, it is important that lawyers work to maximise the chances of legal privilege protecting the inputs and outputs of the risk assessment process. In most cases, where a document, such as a risk assessment report, has legal privilege, it will not be disclosable to litigants or regulators.

Conclusion

There is a great deal being said on this subject at the moment and there is a growing market of lawyers, accountants, management consultants, cyber-specialists and others offering services to combat the constantly evolving issue of information security.

As well as there being a genuine and increasing need for these services, there is also no 'one size fits all' approach and each organisation needs to assess its own needs based on its attitude to risk and budgetary constraints.

But one thing common to every organisation that holds confidential information and/or personal data is that having state of the art cyber-security measures is insufficient to guard against risk if members of staff leave their laptops and memory sticks in the cloakrooms of bars on Friday nights. Even the most secure organisations have weak links.

Ashley Hurst and
Louise Lambert
Olswang LLP
ashley.hurst@olswang.com
louise.lambert@olswang.com