The Law Society Gazette

Are your IT departments the weakest link?

By Mike Brown, Ramin Tabatabai

As the risks of getting it wrong multiply, information governance is no longer just a technical issue, write Mike Brown and Ramin Tabatabai.

Knowledge may be power, but it can also be a serious liability if it is not managed proactively. Doing so, however, is becoming more and more complex as data volumes grow and the legislative regime around data management becomes increasingly stringent. Where data management was once left to the IT department, it is now an issue that needs to be taken seriously by senior management and their legal advisers for a possible crisis to be averted.

Some of the risks created by the growth of data, such as cybercrime and data theft have been well publicised. Others are less obvious, but no less important and carry significant financial and reputational risks. For example, the growth of anti-bribery laws, competition law and large-scale litigation all pose significant threats to a company's wellbeing. The key to preventing problems in these areas is to stay in control of the company's data.

This is the only way to ensure that incidents can be either prevented in the first place, quickly identified if they occur or, that the company has the information and the audit trail to defend itself against potentially damaging prosecutions and financial and reputational risks.

The status quo is, however, that many companies do not have the policies and frameworks in pace to effectively mitigate these risks. In a corporate survey* that Control Risks carried out in conjunction with the Economist Intelligence Unit, 33% of the respondents at leading companies said that their data management policies left them ill-prepared to deal with problems in these areas.

Firm foundations

So what does a good information policy look like? To a large degree, information governance strategy is as much about common sense as it is about technological solutions. This should include policies on email, internet and social media usage policy and the management of employee-owned devices on company networks. The use of cloud networks also needs to be monitored carefully to ensure that customer data does enter jurisdictions that contravene customers' home data protection or privacy rules. Whistleblowing and reporting mechanisms should also be put into place to ensure that senior management are made aware of issues as they develop.

Data retention and destruction policies need to be carefully planned to ensure that companies comply with the law in all of the jurisdictions in which they operate – so that they are fully prepared in the event of an investigation or legal dispute.

Trigger happy

When designing an information governance policy, it is essential to ensure that the company is prepared to respond quickly and comprehensively in the event of a regulatory inquiry or investigation or other potential litigation.

A 'litigation hold' strategy should also be in place to ensure that data is not destroyed, damaged or lost after the company is notified of an investigation or the commencement of litigation. There should also be a clear map of where and how a company's data is stored and who is holding it. This may seem obvious, but is important for a number of reasons that can seriously impede a company's crisis response if not planned for prior to a triggering event.

The longer it takes to access and assemble data, the greater the chance that it will be lost or destroyed whether deliberately or inadvertently thus affecting

the defensibility of the e-discovery process. Any delay in retrieving relevant information may impact a company's ability to demonstrate their cooperation to a regulator or to seek leniency in the early stages of an investigation.

For larger businesses, the biggest challenge is likely to be navigating through and adhering to the data protection laws of the countries in which they operate or their data is held. These vary significantly between jurisdictions and can have serious effects on the ability of an organisation to access its own data and assemble it in response to an event.

In some jurisdictions, most notably Germany and Switzerland, consent from individual employees might have to be required before data can be collected from their devices and this needs to be considered in advance. Also tight legal frameworks of those jurisdictions have to be considered regarding the usage and disclosure of personal data of employees in question.

Other jurisdictions, meanwhile, have severe penalties for the removal of data beyond their borders which can include heavy fines and imprisonment for company executives. In this context, it is always important to get local legal and expert advice if problems are not to ensue.

Practical steps include identifying who the key people will be in the event that a triggering event occurs, what arrangements cloud or other third-party providers have in place to provide access to data and who the consultants, e-discovery professionals and legal advisers will be. It also important to bear in mind that an information governance strategy is a living document that needs to be reviewed and updated regularly as technology, data protection legislation and the nature of the business and its employees change.

Taking a lead

As already noted, responsibility for the implementation of information governance policy is often left to the IT department, but as the issues become more complex, and the risks grow for the company's business and its reputation, this practice is increasingly inappropriate. IT departments cannot be expected to have a grasp of the multiplicity of legal, organisational and practical issues that influence the effective of information governance strategies and in the survey referenced above, only one in five respondents were confident that their IT departments were well-informed on data protection matters.

It remains essential that IT is kept in the loop as part of the process, but information governance is now a central strategic issue for companies and needs the ongoing attention of senior management, the compliance team and - above all - a company's legal advisers, whether in-house or external. Lawyers should be front and centre in both putting these information governance strategies in place and advising on the response in the event that a problem arises.

*Survey: Control Risks, in conjunction with the Economist Intelligence Unit, conducted an international survey of 316 companies, across seven regions (Western Europe, Middle East, South Africa, Latin America, North America, CIS, and Asia-Pacific).

Mike Brown is the director of legal technologies, EMEA and Ramin Tabatabai is a senior consultant for legal technologies at Control Risks. Ramin is also a dual-qualified lawyer admitted to the Bar of Cologne, Germany and roll of solicitors of England and Wales