THE LAWYER
BRIEFING
CYBER SECURITY

INFORMATION GOVERNANCE

A 'just in case' habit?

Organisations need to put a clear strategy in place for the management and disposal of sensitive information

Are you keeping information just in case?

If we said that a third of households keep grocery bills from the last three years, you wouldn't believe it and you'd be right. However, when we go into the workplace our mentality in relation to keeping information goes into hyperdrive. Recent research by PwC shows that over a third of organisations retain information 'just in case'.

The value of big data: quality or quantity?

Traditional ways of managing information are laborious and time consuming for many organisations with little tangible benefit. This approach usually brings about 5 per cent of their unstructured data under some form of control. Some companies avoid the issue altogether, continuing to invest in extension to their IT storage costs and infrastructure.

There is no denying that big-data analytics can unlock great insight from an organisation's information resources, however what constitutes a resource worth mining? To be worth exploiting, it should be of sufficient quality and have its own intrinsic value. That value relates to the usefulness of the information from the time it is authored until its destruction or archiving. The archive of old was never a resting place for the unloved. Organisations that have useful archives fine tune their selection criteria to determine future utility and value. While they don't always get it right (no one has a crystal ball), selection is an important concept in the big-data world.

As information ages, its utility and its value fluctuate. Governing information relies on not just the regulations that control how long to keep it for but how to influence its usefulness and its short-, medium- and long-term value to the business.

Understanding what you have, why it's important and how it is used, provides insight into the 'shelf life' of the information you retain. This allows you to target information investment. It would be sensible, for example, to retain and protect your information 'crown jewels' in a more robust way than draft emails or duplicate internal communications.

Risks of retaining too much information

How does keeping too much information cause a problem?

An average of 20 per cent of time is wasted in many businesses finding out-of-date or inaccurate information. The risks associated with this affect customer retention, loss of productivity and inevitably compliance failings.

The frequency of disputes and investigation means that costly information discovery exercises are no longer the preserve of the unlucky few. The proportionality of cost for a discovery exercise relies heavily on being able to reduce the volume of relevant or potentially relevant information that is captured, processed and reviewed.

More sinister threats that organisations face, such as cyber attack, data loss or breach and insider leak are becoming more sophisticated, frequent and costly. Information hoarding and poor information governance increase the risk and likelihood of incidents occurring.

Gavin Siggers, PwC information governance lead, says: "Knowing your data and adopting a value-based approach provides insight into what needs to be protected, what can legitimately be done with it and how inherent risks can be mitigated."

How does governing information help?

The disposal processes that are applied to your information over time are not as straightforward as deletion. Rules on keeping information vary from country to country. Even when you have deleted a piece of information, how confident are you that the data and all of the versions of it have actually gone?

As part of an information governance programme, defensible disposition allows an organisation to confidently migrate, destroy or exploit its data by understanding and re-evaluating what happens to the data across business processes at various points in what is often referred to as the information lifecycle. This helps mitigate information risks of destroying data when it should still exist or inappropriately archiving, re-using or re-purposing sensitive or personal data sets.

What does the future hold?

If you have to respond to a discovery request, there are significant cost implications. The RAND review identified that 70 per cent of the costs of a given e-discovery case are taken up in the review process.

Taking proactive steps to regain control of your information by embarking on an information governance programme should form a part of your discovery-readiness strategy.

Being able to defend how you manage and dispose of information over time relies on understanding the data, its value and usefulness. That knowledge will help you put a clear strategy in place for managing and removing information.

Umang Paw, PwC partner, and head of e-discovery and e-investigations, says: "Being 'discovery ready' relies on being in control of your information as much as having the right processes and technology in place. Information governance must play a vital part in the discovery armoury of any organisation."

By Gavin Siggers (top), PwC information governance; and Umang Paw, PwC partner and head of e-discovery and e-investigations
Follow at: @UmangPaw

pwc

PwC LLP
1 Embankment Place
London
WC2N 6RH
Tel: +44 (0) 20 7583 5000
Fax: +44 (0) 20 7212 4652
Web: www.pwc.co.uk/fts