www.pwc.co.uk

Defensible disposition

Are you still keeping your information 'just in case'?

March 2016

pwc

Are you still keeping your information 'just in case'?

The value of big data: Quality or quantity?

Proliferation of data is a global phenomenon, now and for the foreseeable future. Traditional approaches to managing information are laborious and time consuming for many organisations with little tangible benefit, usually bringing about 5% of their unstructured data under some form of control. Often this has resulted in companies avoiding the issue altogether preferring instead to invest in the continual extension of their IT storage costs and infrastructure.

The development of big data analysis has been accompanied by the suggestion that not only is it okay to keep all information, it advantageous to do so. This view is bolstered by the failure in traditional approaches to information management failing to adapt to the dramatic increase in digital information we create. New ways of exploiting vast swathes of data continue to develop; does this mean that keeping everything for ever may lead to a data gold mine in the future?

There is no denying that sophisticated data analytics can unlock great value from an organisation's information resources but what constitutes a resource worth mining needs to be of sufficient quality to begin with. To be worth exploiting it should 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 invest in and constantly tune their selection criteria to determine future utility and value. Whilst they don't always get it right (no one has a crystal ball), selection is an important concept that has merit in the big data world.

Know your data

As the age of information increases, its utility and its value fluctuate. Governing information from the outset provides insight into not just the laws that control how long to keep it for but how to influence its usefulness and its short, medium and long term value.

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

How does keeping too much information cause a problem?

Increasing volumes of information retained by organisations have exposed them to ever increasing risks and costs.

An average of 20% 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. These costs and risks increase with greater regulation, whilst compliance failings lead to reputational loss.

The prevalence of disputes and investigation means that costly information discovery exercises are no longer the preserve of the unlucky few; this cost is so worrying that it has drawn the attention of the judiciary with, for example, the Jackson reforms in the UK calling for proportionality. 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.

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

By failing to consider a defensible disposition regime, organisations place themselves in a position where their information risks increase. The consequences of this can be significant if information has been destroyed when it should still exist or exists when it could have been destroyed. Similarly, archiving, re-using or re-purposing data sets that contain sensitive or personal information can incur significant penalties or present risks to individuals.

Defensibility in how an organisation manages and disposes of its information over time relies on understanding the data, its value and usefulness. This provides insight into what needs to be protected, what can legitimately be done with it and how inherent risks can be mitigated.

When does information utility change?

Not all information carries equal value.

Drafts
For some businesses drafts are as valuable as the final record but for the majority of business processes they are soon out of date and redundant.

Duplicates
Proliferation of duplicative information across a business is inefficient and expensive. Destroying records without destroying the duplicates is a stress point in any defensible disposal programme.

Transactional records
Valuable information is retained based on business, legal and regulatory requirements. Adequately managing those records allows value to be realised and utility to be optimised.

Short term value with lengthy retention requirements?

Extracting added value
Prolonging information utility relies on availability of the data and understanding how information flows between business processes.

Reducing retention cost
Defensible policies that keep retention periods down and a storage strategy that reflects information value can significantly drive down costs.

Added value and long term utility relies on knowing the data and having defensible processes in place.

Long term value
Exploiting information for historical or business purposes requires close attention to the sensitivity of the data.

Evidential value
Producing evidential records requires sound processes to keep costs and response time down.

Six key elements to defensible disposition

Sound policy and process, coupled with effective communication and systems, enable defensibility and compliance to be embedded throughout the information lifecycle. The earlier the end of life is considered, the more resilient and defensible the disposition process becomes.

1 Policy

Adequate retention policies rely on knowing your data, processes and jurisdictional obligations.

2 Processing

Use of information determines its value. Changing that use has implications for retention and may breach privacy laws.

3 Protection

How you store and secure information throughout its lifecycle is determined by its value and utility.

4 Redundancy

Removing out of policy, obsolete, duplicate or low value data legitimately can provide cost savings and improve efficiency.

5 De-sensitising

Exploiting information value over the long term may require additional levels of scrutiny to remove sensitive terms from your data set.

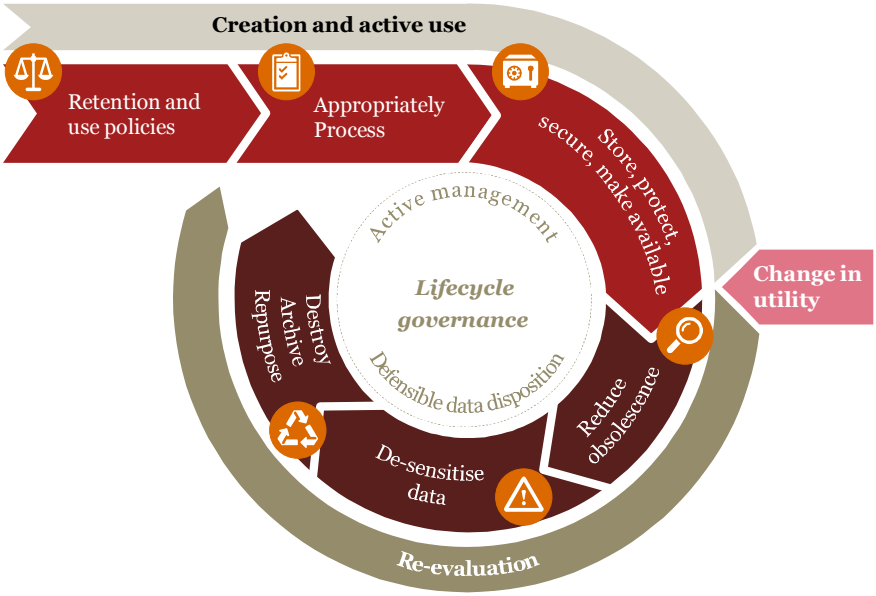
6 Disposition

Re-purposing, data divestiture and long term archiving potentially unlock value. Destroying data requires appropriate processes to be defensible.

How does governing information help?

The disposal processes that happen to your information over time are not as straight forward as deletion. Disposition of data is made more complex with proliferation of data volume and interactions between systems; information is subject to statutory and regulatory retention demands that vary from country to country. Once a deletion is actioned how can you be confident 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 at various points in what is often referred to as the information lifecycle. In other words, governing the lifecycle by understanding and re-evaluating what happens to the data across business processes. As information utility changes, the organisation and its systems should be able to respond appropriately.



Applying defensible disposition throughout the information lifecycle

Understanding the data within the organisation, the business processes that created it and the legal and regulatory obligations that apply to it allows the organisation to define policies that control acceptable use and required retention regardless of jurisdiction.

Contacts

Umang Paw

Partner

T: +44 (0) 20 7804 4347

E: umang.paw@uk.pwc.com

Matt Joel

Director

T:+44 (0) 20 7804 7117

E: matt.joel@uk.pwc.com

Tim Callister

Senior Associate

T: +44 (0)20 7804 0027

E: tim.callister@uk.pwc.com

"Poor information practices expose the enterprise to a variety of risks potentially leading to significant financial penalties and reputational loss.

Understanding what information you need to keep and how you can improve the way it is managed reduces these risks and prepares you for scrutiny."

160229-143441-AP-OS