Coping when everything is digital?

Digital Documents and Issues in Document Retention

White Paper

Julian Gillespie, Patrick Fair,
Adrian Lawrence, David Vaile

BAKER & McKENZIE CYBERSPACE LAW AND POLICY CENTRE

acla
AUSTRALIAN CORPORATE LAWYERS ASSOCIATION
- *the* professional association for in-house lawyers

Baker & McKenzie
Cyberspace Law & Policy Centre

Baker & McKenzie

EMC²
where information lives

ORACLE®

iSKCOVERY
information management solutions

Coping when everything is digital?

Digital Documents and Issues in Document Retention

White Paper

Julian Gillespie, Patrick Fair,
Adrian Lawrence, David Vaile

acla
Australian Corporate Lawyers Association
- the professional association for in-house lawyers

Baker & McKenzie
Cyberspace Law & Policy Centre

Baker & McKenzie

EMC²
where information lives

ORACLE

DISKCOVERY
Information management solutions

National Library of Australia Cataloguing-in-Publication data

Bibliography.
ISBN 0 646 43894 8.

1. Business records - Law and legislation - Australia.
2. Electronic records - Law and legislation - Australia.
I. Gillespie, Julian. II. Baker & McKenzie Cyberspace Law and Policy Centre.

346.940664

Authors:

- Julian Gillespie is a barrister and solicitor whose practice areas include corporate governance.
- Patrick Fair is a partner at Baker & McKenzie Sydney office, former President of NSW Law Society and chair of the Internet Industries Association.
- Adrian Lawrence is a senior associate at Baker & McKenzie Sydney office and author of the looseleaf service *The Law of Ecommerce*.
- David Vaile is Executive Director of the Baker & McKenzie Cyberspace Law and Policy Centre at the UNSW Faculty of Law, Sydney.

Acknowledgments:
Note that responsibility for the content of this paper is solely that of the authors, and not those named below. Thanks to the following for generous contributions towards the creation of this document:

- Diskcovery http://www.diskcovery.com.au
- EMC http://www.emc.com
- Oracle http://www.oracle.com
- Australian Corporate Lawyers Association http://www.acla.org.au

Research by:

- Galexia Consulting http://www.galexia.com.au

Other support by:

- Interns Peter Garay, Diede van Lamoen, Steven Fung, Ada Ko, and Stuart Loh

Designed by UNSW Publishing and Printing Services Ref: 32399
Printed by: Agency Press Pty Ltd

Contents

Contents in detail


DOCUM
PAPERLESS OFFICE
ON
DA

Will you cope when everything is digital?

Recent legal and business developments mean renewed attention is being directed into corporate computer systems in Australia, the US and around the world. Questions such as the following are becoming common:

- How can digital documents be used, and when can they be destroyed?
- What happens if you ignore them after they are no longer 'useful'?
- Will you be able to rely on them when you need them?
- In a court case, could you prove they mean what they say?

Do you have a policy?

Many organisations do not have an adequate policy. Their existing document management policy may not cover digital documents, nor recognise challenges thrown up by a chaotic hybrid document environment. Does your company have:

- Staff sure of which documents to keep for legal reasons, and which to delete?
- A clear policy for digital document retention and destruction?
- Specialists tasked to implement and maintain such policies and protocols?
- Hardware that enables access to archives created with obsolete devices?
- Awareness not only of core servers, desktops and laptops, but also peripheral 'personal digital assistants' (PDAs), smart phones and home computers?
- A litigation plan to provide 'discovery' over all your digital documents?

Are digital document polices too hard?

Some suspect that digital document issues can affect their organisation's performance and reputation, but are tempted to use the 'Too Hard' basket. This is not a survival strategy. With a guide like this and some advice, anyone can follow a structured approach providing business benefits as well as protection from hazards.

Complex legal, technical and business issues raised by digital documents can also be an excuse for passing the buck between IT, legal and corporate departments. It is critical that you know who is talking to whom, and that everyone knows where the buck stops.

Our audience

This paper looks at issues affecting digital documents, and suggests how to create protocols for managing the risks and potential rewards of handling these assets safely.

Is it for legal departments, finance, records managers, IT, corporate executives, someone else; or all of these audiences? Probably 'all of them.' Anyone participating in corporate governance or operations where understanding digital document risks is involved should find this paper of value.

Although there are limits on how far we explore technical issues, in some places we offer legal or technical detail that will not interest everyone. Don't let this put you off. You should be able to get the gist and move on.

The focus is primarily on the Australian jurisdiction, but the principles in standards, case law and legislation are increasingly being reflected in different jurisdictions around the world. Companies operating in Australia may also be subject to similar obligations in other countries.

Accordingly, we offer international equivalents in certain sections or footnotes, though these are by necessity illustrative, rather than exhaustive. (Some of our legislation reference conventions are modified to assist the international reader.) You can also consult the References section at the end for a consolidated list of these comparative references.

1 Digital Document Retention & Destruction

1.1 Introduction

Recent legal and business developments, and the replacement of paper by digital documents as the main information format for modern business, mean that a spotlight is shining into the dark recesses of the corporate computer cupboard. Seemingly innocuous questions are emerging with ever more serious implications:

- What documents should be created electronically?
- How can digital documents be used and stored?
- When and for what reasons can digital documents (or the hard copy originals they are based on) be destroyed?
- Will you be able to rely on them when you need them?
- Can you prove they mean what they say if they have to be produced in a court case?
- What risks do you face if you don't take enough care of what happens to them after they seem to be no longer useful?

Are digital document polices just too hard?

Some governance-level managers and directors have an inkling that how they deal with digital documents can have a big impact on their organisation's performance and their professional reputation, but they may be tempted to pass it off to the 'Too Hard' basket, or hope that someone else is taking care of it.

This is often no longer a survival strategy. The risks can now be too great. With the help of a guide like this supplemented by expert advice on specific issues as necessary, virtually anyone can address most of the core issues in a structured approach that provides substantial business benefits as well as protection from the more obvious hazards.

Do you have a policy?

Many organisations don't have an adequate policy or a practical system for dealing with the questions raised by retention and destruction of digital documents. Their existing document management policy may not cover the technical realities of digital versions of documents, or it may not recognise the challenges thrown up by the hybrid document environment (part paper, part electronic, part chaos).

A negative answer to any of the following questions may mean that your company (or client) is not sufficiently managing its digital documents.

Does your company have:

- A clearly articulated policy for digital document retention and destruction?
- Employees who know which documents they should keep for legal reasons, and which they can safely delete from day to day?
- Specialist individuals specifically tasked with the responsibility of implementing and maintaining protocols for digital document retention and destruction?
- An internal committee that reviewed your policy within the last 12 months?
- An internal committee that tested your protocols within the last 12 months?
- New hardware that enables access to earlier archives created with obsolete hardware?
- A policy for digital document retention that operates to include not only the core of office servers, desktops and laptops, but also peripherals like PDAs, Blackberries, and home computers of staff and key consultants?
- Its policy and protocols periodically assessed by objective third parties for review and validation?
- A plan in place in the event that litigation is commenced, where your company can expect to be required to provide discovery over some or all of your digital documents?

Who talks to whom – where does the buck stop?

The complex legal, technical and business issues converging on digital documents can easily be used as an excuse for passing the buck (for instance between IT, legal and corporate departments). These complexities mean it is critical you know who is talking to whom about it, and that everyone knows where the buck stops.

1.2 Why a digital document retention, destruction and production policy is important

Most documents are now digital — 70% are never printed

More than 90% of all documents produced in many organisations today originate as digital objects[1], and around 70% of these are never printed. Moreover, paper documents are increasingly scanned and retained only in digital format. Paper-only document policies are now clearly inadequate.[2]

Corporations will now often hold archives, back-ups, and day-to-day working files in the realms of the 'terabyte' (the equivalent of several hundred million pages of information). Once served with a request for discovery of digital documents in litigation, the task of cataloguing, screening and providing e-documents to an opponent can be daunting and expensive, and even more so if there has been little or no prior preparation.

---

[1] Peter Lyman and Hal Varian, *How Much Information* (School of Information Management and Systems, UC Berkeley: 2003) <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/> accessed 11 August 2004.

[2] Sue Bushell, 'When documents rise from the grave' (2003) *CIO*, 8 August 2003 <http://www.cio.com.au/index.php/id;1439680944;fp;4;fpid;56491> accessed 23 August 2004.

High profile court cases raise the bar

British American Tobacco (BAT) v. McCabe: Even when a company has an established document retention policy in place to facilitate provision of e-documents in the event of discovery orders, this may not guarantee that the company's policy will be spared exhausting judicial scrutiny, as the Victorian Supreme Court case of *McCabe v British American Tobacco Services Limited (BAT)*[3] showed.

The initial trial judge concluded that with the assistance of its lawyers, BAT had undertaken a concerted programme of document destruction to eliminate material that could prove harmful to BAT in future litigation. The judge found that 30,000 documents were destroyed, including information on what had been destroyed, in circumstances where, though no actual litigation was on foot at the time it was destroying documents, BAT nonetheless 'anticipated' the likelihood of future claims being brought against it.

Many of the critical documents were digital images of hard copy originals, not the paper originals themselves, which had generally been destroyed after being scanned.

The result, according the trial court: Ms McCabe was denied thousands of documents and thus, in effect, the right to a fair trial. This conclusion led the court to strike out BAT's defence entirely, effectively handing her victory without even having to prove she smoked BAT cigarettes!

This remarkable result was reversed on appeal, but both trial judge and Court of Appeal had no hesitation using US case law on how a party maintains and ultimately destroys its documents. Given the spread of global corporations, Australian courts increasingly look to US case law to settle international problems of document retention.

US regulators also expressed significant interest in the original principle in the Victorian Supreme Court, even after it had been overturned on appeal.

In separate proceedings BAT's legal advisor, Nicholas Cannar, lost his appeal in May 2004 against the US Department of Justice using the NSW Supreme Court to take evidence from him in relation to the 'document management policies' for litigation in the US.

US Department of Justice and Big Tobacco: In September of 1999 the US Dept of Justice initiated proceedings against all cigarette manufacturers and their offshore parent companies. Through allegations of fraud, conspiracy, racketeering and misrepresentation, the US government is seeking damages to cover its annual bill of $20 billion for health care costs associated with smoking related illnesses.[4]

---

[3] [2002] VSC 73 (22 March 2002) <http://www.austlii.edu.au/cgibin/disp.pl/au/cases/vic/VSC/2002/73.html> accessed 23 August 2004.

[4] *United States of America v Philip Morris Inc* (First amended complaint) <http://www.usdoj.gov/civil/cases/tobacco2/DOJ%20Web%20-%20Amended%20Complaint.pdf> accessed 23 August 2004.

American law entitles a party to discover and call for evidence held by a company's subsidiaries or parent company that may be located overseas. The same is generally true in Australia. After the US Dept of Justice read the first instance decision in McCabe, that is exactly what they did. The US Department of Justice sent Letters of Request[5] *in accordance with the Hague Convention on Taking Evidence*[6] to the Supreme Court of NSW and to the Queen's Bench Division in England.

In both instances NSW and England have agreed to summon former BAT internal and external lawyers to give evidence on the document destruction policies of BAT (for both hard copy and digital formats) to be used in US Dept of Justice proceedings.

Overseas Courts are Now Joining Forces: Once companies may have thought that they could use their subsidiaries and overseas related entities to deal with sensitive documents, believing that to do so outside the jurisdiction of the home country would provide sufficient protection from home country prosecution. Given the ease with which NSW[7] and England have sought to assist the United States understand the activities of global 'Big Tobacco' organisations, it can be safely suggested that the 'good old days' of jurisdiction shifting of documents are drawing to a close.

Andersen/Enron: Although based on different facts to those in *McCabe*, in another illustrative US case American accounting firm Arthur Andersen was fined US$500,000 and placed on five years probation for having destroyed files of its client, Enron, in circumstances where Andersen knew that civil and criminal investigations were imminent. As is well known, the court's sanctions were a significant factor in the eventual destruction of the global Andersen empire.

Increased scrutiny and professional liability

On appeal[8] in *McCabe*, two critically important issues arose – intention and anticipation.

First, other than for legitimate reasons, no company's retention policy can be seen to possess a positive intention to destroy materials for the purpose of preventing their disclosure at future or imminent litigation.

Secondly, where a company is not actually on notice of impeding litigation (such as a threatening letter) but litigation could be 'anticipated' by a company, it remains undecided whether a company can or should continue normal wholesale document destruction, particularly if the type of documents destroyed could be later shown to have been relevant to a later case. (This point has not been conclusively determined.)

---

[5] Letter of Request from US Department of Justice to the Supreme Court of NSW, 3 October 2002 <http://www.usdoj.gov/civil/cases/tobacco2/Nicholas%20Cannar%20letter.pdf> accessed 23 August 2004.

[6] *Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, 847 UNTS 231, entered into force 7 October 1972 with 46 signatories <http://hcch.e-vision.nl/index_en.php?act=conventions.text&cid=82>, accessed 28 August 2004.

[7] Supreme Court of NSW decisions on Letter of Request (Bell J) <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/supreme%5fct/2003/802.html?query=%22letter+of+request%22> accessed 23 August 2004; <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/supreme%5fct/2003/1267.html?query=%22letter+of+request%22> accessed 23 August 2004.

[8] [2002] VSCA 197 (6 December 2002) <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/vic/VSCA/2002/197.html> accessed 23 August 2004.

Clearly this second issue bears upon considerations relevant for determining the first, namely, the intentions behind the policy – an unfavourable determination on both counts will be likely to lead to charges of either perverting the course of justice or contempt of court.

Should a company risk such an outcome then not only is the future of the company at grave risk, but also the personal reputations of those directors or executives who drive the company. Judicial findings of contempt, or perverting the course of justice, carry with them the likelihood of further criminal sanctions against culprits, involving fines, suspensions by regulators such as ASIC, and, increasingly, a real possibly of imprisonment.

Strategic importance to the organization: methodical solutions needed

The judicial gaze has begun to focus upon the entire stores of information held by companies, and how companies deal with those stores. Other cases, like HIH in Australia and Worldcom and Enron in the US, continue the judicial charge towards full accountability for corporations' dealing with their documents.

Corporations that do not have in place strategic, comprehensive and reasonable document retention policies, methodically and consistently adhered to in implementation, choose to chance a fate immeasurable in its potentially destructive outcomes, if the ire of judicial condemnation falls upon them.

1.3 What do generic document control policies cover?

Clearly, document control policies already exist in the non-digital world, and typically cover issues such as those below, which remain relevant for digital documents:

- **Retention:** keeping the records in one form or another.
- **Destruction:** destroying the originals and copies, in some cases with detailed logs of the name and content of destroyed documents.
- **Coverage:** not every scrap of paper warrants formal treatment.
- **Purpose:** the reason or purpose for decisions to retain or destroy.
- **Process:** the means and media for putting retention or destruction decisions into effect, with associated protocols and worksheets.
- **Timing:** the various periods a document or file must be held for.
- **Responsibilities and plans:** clear documentation indicating who is responsible and procedures and routines to be followed.

1.4 What are 'digital' documents?

The modern corporation generates a plethora of digital documents. For example:

- Imaged versions of original paper documents
- Files (including word processing, spreadsheets, presentations)
- Email (including email messages, instant messages, logs and data stores)
- Databases (including records, indices, logs and files)

- Logs (including accesses to a network, application or Web server)
- Transaction records (including, in particular, financial records)
- Web pages (whether static or dynamically constituted)
- And others too numerous to mention!

1.5 Digital or non-digital?

Digital documents, as opposed to traditional hard copy ones, are distinguished by attributes such as:

- **Ease of copying, searching, retention and destruction**
  There are different physical limits to the cost or convenience of the primary record creation tasks compared to those for hard copy documents, so some things become feasible that were not previously so.
- **Sheer volume**
  The absolute number of digital documents can be very high, leading to demands for production as a litigation tactic.
- **Significance of file formats, media, and data types**
  As technology evolves, the file formats and underlying media on which documents are written also change, leading to problems with obsolete formats and recovery of old files when the drives or file formats are no longer supported.
- **Potential for a chaotic, un-managed mix of formats**
  There are a number of different mixes of document types that create the risk of confusion and *ad hoc* approaches: paper and digital, formal and informal, structured and unstructured. While most of us may have a few of the above combinations under reasonable control, the very diversity and complexity of document collections means that there are often pockets of chaos that are perhaps easier to ignore. For instance, if you have a paper file on a matter or project, are all emails and casual instant messages related to it printed and added to the paper file? If not, how are they linked? Do you also print all relevant contact records from your database?

1.6 Destruction

Various technical, operational and legal issues arise from attempting to destroy digital documents, including whether:

- traces are left on the disk,
- reasons for destruction are recorded, and
- other questions described later in this document are invoked.

Digital document management strategies

Throughout this paper, we will be discussing issues that arise from the technologies, models, risks and benefits associated with digital document management strategies and the policies that implement them

2 Types of Digital Document

Different digital document formats show specific technical and processing attributes, so it's not surprising that they raise a range of different legal and policy issues regarding retention and destruction.

This section outlines some of those technical features, and their practical implications.

2.1 Email

Many organisations are only now grappling with the implications of ubiquitous email, which was not a significant concern a decade ago. It has often been treated informally, but it is increasingly central to communications between businesses, government officials and individuals, and needs to be considered in some detail.

Email consists of both individual email messages traversing networks, and aggregated data stores at the mail server.

Q: What's in an email message?

Email messages are sent individually in a package that includes the text content of the message, formatting information, some visible header information (like Subject and Date) and a series of usually invisible header data. These are passed through various internal and Internet mail server systems until they reach their destination, gathering routing and other transaction data as they pass each stop on their way.

Q: Are they stored anywhere in one big file?

Some email server systems, such as Microsoft Exchange Server, effectively accumulate all the messages into one large database file for processing and storage, with each message becoming a series of records and relationships in that file. Typically, these files, and the messages within them, are difficult or impossible to read except using the host software. Details of the transactions through which the message passes are often closely associated with the message itself. This information can be of great value for forensic purposes.

There can also be locally stored personal versions of an individual's email data file, either as the main operational source file, or as an extract or archive of all or part of it. For example, see 'Recipient copies' below for a discussion of .PST files.

In other cases each message and each attachment exists as a separate file, so a search of the mail server storage disk (or in some cases a local disk) would reveal a multitude of separate files, each of which may be separately readable. There will also be a number of other files containing transaction details, some of which may be appended to the meta data in the message.

Email headers and 'meta data'

Q: What is 'meta data,' and where is it held?

Hidden behind the scenes, each email message (and many other kinds of document) contains or is associated with a set of 'headers' and 'meta data' which describe its path, origin and destination and other characteristics, including the timing of critical events. They are normally hidden but can be revealed.

Q: Why is meta data important?

This meta data contains a wealth of forensic information, which can be critical in tracing the email message's path through various networks and the Internet and establishing its authenticity.

It also gives critical information on timing (which may however be subject to errors in the clocks of the host systems.) Here is a sample:

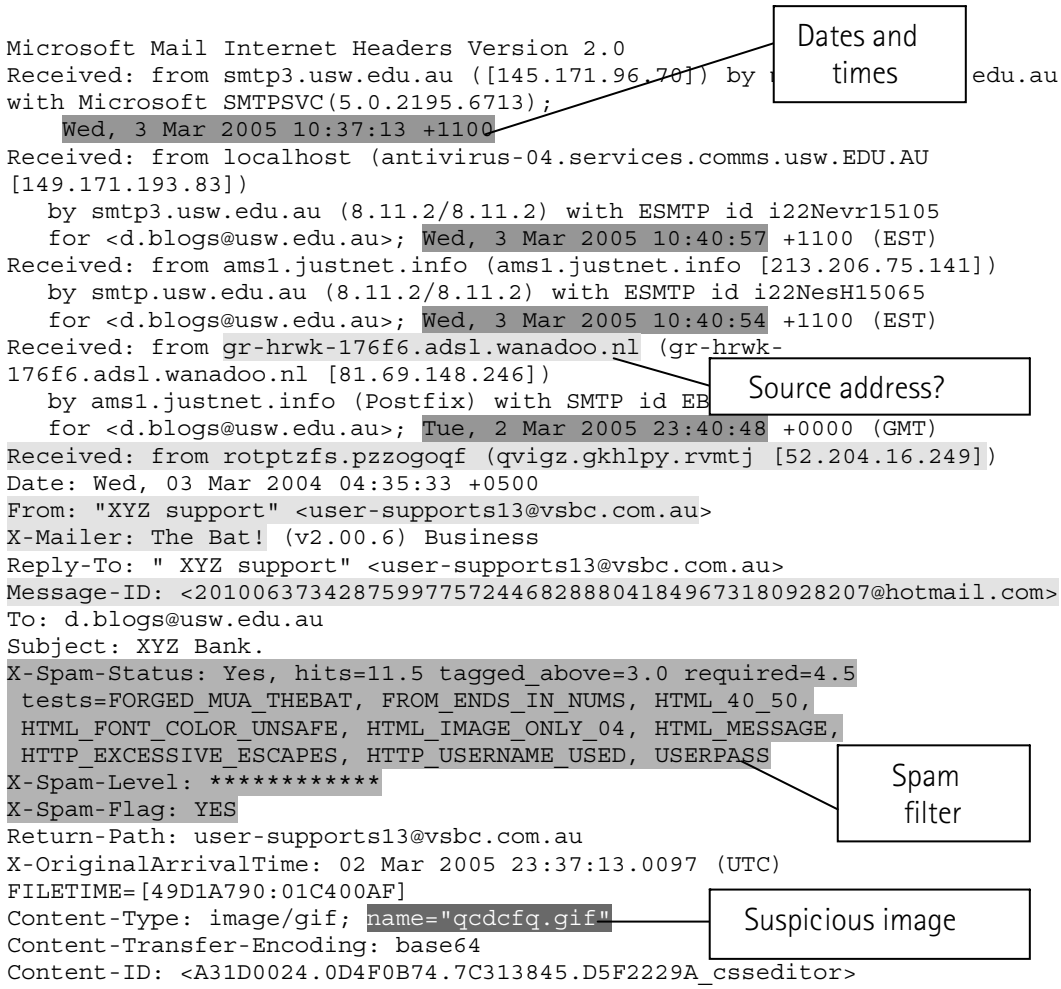
```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp3.usw.edu.au ([142.171.96.70])
by mail.law.usw.edu.au with Microsoft
SMTPSVC(5.0.2199.6713);
3 Mar 2005 12:40:06 +1100
Received: from localhost (antivirus-04.services.comm
s.usw.EDU.AU [149.171.193.83])
 by smtp3.usw.edu.au (8.11.2/8.11.2) with ESMTP id
i231hpr00700
 for <d.xxx@usw.edu.au>; 3 Mar 2005 12:43:51 +1100
(EST)
Received: from smtp1.central.local (host13.apansys.c
ust.telecomplete.net [214.160.122.78])
 by smtp.usw.edu.au (8.11.2/8.11.2) with ESMTP id
i231hmH00620
 for <d.xxx@usw.edu.au>; 3 Mar 2005 12:43:49 +1100
(EST)
From: <orderstat@apansys.com>
To: <d.xxx@usw.edu.au>
Subject: apansys Order Confirmation (4312-48BE-52FD)
Date: 3 Mar 2005 01:43:35 -0000
Message-ID: <SMTP1MLdP4GLqfjE7BR00012557@smtp1.centr
al.local>
Return-Path: orderstat@apansys.com
X-OriginalArrivalTime: 03 Mar 2005 01:40:06.0863
(UTC) FILETIME=[74ED0DF0:01C400C0]
```

Q: What does suspicious email meta data look like?

Here is meta data from a malicious spam email message seeking the user's banking details, supposedly from XYZ Australia. It is discussed here as an example of the sort of features which you could look at for forensic purposes.

Note the precise timing information, the suspicious appearance of domain names in the internet addresses for countries like Holland (.nl), and of free email services like Hotmail; and the use of a picture of text (.gif) not actual text. It has been through a spam filter; note the comments added by this system.

Email Header with Clues




```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp3.usw.edu.au ([145.171.96.70]) by t                edu.au
with Microsoft SMTPSVC(5.0.2195.6713);
     Wed, 3 Mar 2005 10:37:13 +1100
Received: from localhost (antivirus-04.services.comms.usw.EDU.AU
[149.171.193.83])
   by smtp3.usw.edu.au (8.11.2/8.11.2) with ESMTP id i22Nevr15105
   for <d.blogs@usw.edu.au>; Wed, 3 Mar 2005 10:40:57 +1100 (EST)
Received: from ams1.justnet.info (ams1.justnet.info [213.206.75.141])
   by smtp.usw.edu.au (8.11.2/8.11.2) with ESMTP id i22NesH15065
   for <d.blogs@usw.edu.au>; Wed, 3 Mar 2005 10:40:54 +1100 (EST)
Received: from gr-hrwk-176f6.adsl.wanadoo.nl (gr-hrwk-
176f6.adsl.wanadoo.nl [81.69.148.246])
   by ams1.justnet.info (Postfix) with SMTP id EB
   for <d.blogs@usw.edu.au>; Tue, 2 Mar 2005 23:40:48 +0000 (GMT)
Received: from rotptzfs.pzzogoqf (qvigz.gkhlpy.rvmtj [52.204.16.249])
Date: Wed, 03 Mar 2004 04:35:33 +0500
From: "XYZ support" <user-supports13@vsbc.com.au>
X-Mailer: The Bat! (v2.00.6) Business
Reply-To: " XYZ support" <user-supports13@vsbc.com.au>
Message-ID: <20100637342875997757244682888041849673180928207@hotmail.com>
To: d.blogs@usw.edu.au
Subject: XYZ Bank.
X-Spam-Status: Yes, hits=11.5 tagged_above=3.0 required=4.5
 tests=FORGED_MUA_THEBAT, FROM_ENDS_IN_NUMS, HTML_40_50,
 HTML_FONT_COLOR_UNSAFE, HTML_IMAGE_ONLY_04, HTML_MESSAGE,
 HTTP_EXCESSIVE_ESCAPES, HTTP_USERNAME_USED, USERPASS
X-Spam-Level: ************
X-Spam-Flag: YES
Return-Path: user-supports13@vsbc.com.au
X-OriginalArrivalTime: 02 Mar 2005 23:37:13.0097 (UTC)
FILETIME=[49D1A790:01C400AF]
Content-Type: image/gif; name="qcdcfq.gif"
Content-Transfer-Encoding: base64
Content-ID: <A31D0024.0D4F0B74.7C313845.D5F2229A_csseditor>
```

Archives

Many email systems generate archives, where a large number of the oldest messages held on the operating mail server are copied to a permanent archive medium then deleted from the server.

Recipient copies, and local data stores

Managing personal storage of emails is one of the biggest headaches for many IT managers – once on a hard drive, messages can be backed up to DVD, the hard drives can be pulled out, anything can happen. How can a company track this?

The person or persons who receive an email will have a copy within the mail system created automatically in the process of opening it. They may also manually make copies of single messages on their disk drive or network, on floppy disks or other removable media, or by forwarding the whole message on to other email addresses.

Some of the biggest areas of exposure can be aggregate files, which contain not just one email but potentially all of those to and from a particular person. ".PST" is a Microsoft Exchange term for a local storage profile that is set up and managed by individuals on their own local hard drives. There are analogous concepts with other common systems such as Lotus Notes Mail. These need particular attention.

Disclaimers

Many organisations now attach standard automatic disclaimers and warnings to outgoing email messages, often indicating they are intended only for the named recipient, prohibiting re-use and requesting notification in the event of misdelivery.

The effect of these disclaimers is untested in the Australian context.

2.2 Imaged versions of paper documents

It is increasingly common for organisations to scan hard copy paper documents to create digital images of those documents, with descriptive meta data stored along side the images to assist in efficient management and later retrieval.

In some cases these images act as mere 'backups' to the paper originals, but more often the originals are destroyed after scanning, leaving the digital documents as the only copy. The decision to systematically retain or destroy hard copy after scanning is one that needs considerable care, for practical reasons as well as those outlined in this paper.

This process also directs attention to the adequacy of the technical and procedural environment in which the conversion happens, and the capacity of the digital system to provide reliable and ongoing access to the images when required.

An imaged document can be as relevant as the hard copy version. The value of the document image as evidence, compared with the paper originals, is a central concern that we deal with in Chapter 5 below.

2.3 Backups, archives and extracts

You can end up with 'copies' of data from primary digital documents in several different ways. It is important to be aware of the differences between the various models, and some of the issues that arise.

Backups

Backups are made automatically to guard against the failure of a disk or system. They are typically a periodic snapshot of the complete set of live data files at a particular moment.

Users may be unaware what items are backed up and what are not. There may be no effective policy to settle this issue in a way that supports an organisation's interests, legal obligations or its users' expectations, and no procedure to verify that it has been followed, or to inform users about what backup practices are actually in place.

In addition, backup systems are typically not designed to enable searching for individual messages or documents, instead being intended only for retrieval of large slabs or the whole of a disk file system in a disaster. In some circumstances, legal discovery (see below) may require the creation of separate search facilities to find relevant information in the backed up corpus of documents.

Q: Are backups forever?

The storage media to which documents are transferred (tapes, removable or fixed disks etc.) are typically re-used frequently, so that you will often only find copies going back the last several backup periods (hours, days or weeks), with the older media being wiped and re-used. Some operators do keep selective archive copies of backup media.

A key question to ask is, does purging from the server mean it is purged from the back-up system?

There are risks for excessive retention in breach of a policy: material that may be adverse evidence is unnecessarily retained, and may have to be searched. In *Murphy Oil v. Fluor Daniel*, the company had 20 million pages of e-mail and attachments to search through because they failed to follow their own backup policy. The cost was nearly $10 million over six months. "Fluor's e-mail retention policy provided that backup tapes were recycled after 45 days. If Fluor had followed this policy, the e-mail issue would be moot. Fluor does not explain why, but it maintained its backup tapes for the entire 14-month period."[1]

[1] *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 (E.D.La. Feb. 19, 2002).

Archives

Archive copies are a creation of a whole or partial duplicate of the contents of a digital document system in perpetuity, either purely as a historical record or as a means of enabling old records to be deleted from the main current storage system.

Q: Are archives forever?

Archives may not be complete, but they are typically likely to be physically available over the long term (months and years). However, on older systems the technology may change so that it is hard to find a device that will read old files, file formats or media.

The question is, will a file format be readable 'forever' if it keeps being superseded every few years? This falls into the category of risk management of the capacity to preserve and read digital documents. There is increasing attention to best practice and standards for permanence of e-records.[2]

Some suppliers are addressing this with archive formats created for such a purpose. For instance there is a PDF-A variant of the PDF format. Others suggest use of a human-readable structured open format such as XML.

Extracts

It is possible to make an extract of most digital document systems at any time and for various purposes. The content and availability of these extracts will vary greatly.

2.4 Office productivity software files

A major category of digital documents is files created by office software, such as word processing documents, spreadsheets, presentations and images.

Authentication

It can be a forensic challenge to establish the provenance and authenticity of a given digital file of this type.

Hard disk traces

There are often traces of old, deleted files left on a hard disk. When you ask most standard installations of disk operating systems (such as Microsoft Windows , Apple Mac OS or GNU/Linux) to delete a file, they will merely omit the reference to the file in the disk's directory, rather than actually scrubbing the data from each block of the disk where it is stored.

---

[2] Arp C and J Dickman, 'Information Preservation: Changing Roles', *The Information Management Journal*, Nov–Dec 2002, Vol. 36, No. 6, PDF by subscription: <http://www.arma.org/bookstore/productdetail.cfm?ProductID=1268>.

(While one could use a variety of tools and options to remove the actual data, these are often not implemented routinely even if installed, and may indeed cause an unacceptable performance slowdown if they are implemented.)

Garbage in the file

Some software (such as versions of Microsoft Word) also leaves traces of other data on the same or other disks inside the electronic file. Sensitive information can inadvertently be transmitted with an innocuous file. While not normally seen on screen or printed, in some circumstances this information can be revealed.

(Certain computer viruses can also extract parts of documents and distribute them randomly in other files, but this is outside the scope of our discussion here.)

Versions

Documents go through different versions, a number of which may have later significance. Depending on the technical and procedural decisions your organisation makes, there may be no information on these prior versions, some fragmentary information, or a full 'roll back' archive which enables recreation of an arbitrary version on any date, with logged meta data. (See also section 8.1)

Meta data

Another hidden set of information is meta data. Microsoft Office tools have a "Properties..." pull-down menu item that displays these meta data.

2.5 Databases

Databases are structured files associated with sophisticated programming functionality. Databases are the heart of many modern digital tools, from email servers to document management, from online banking transactions to staff record systems.

Data stores

Data stores are the virtual containers and actual files on computer disks, which hold the information in individual records in a database. They can also contain other associated indexing, linking, transaction control and related functional and historical details. These are usually invisible to the ordinary user, but they may potentially be available on closer inspection.

Data stores can be as simple as a list in a single spreadsheet file or as complex as online relational systems with different components hosted in different countries, with fragments of virtual files spread over different hard disks and other media.

In some cases what a computer user sees may look like a single record, but the complete data displayed may not ever exist in any one place as an actual record in the data store, only as a transient representation on screen (and perhaps in print), or a series of editing and change-tracking entries.

Reports

Reports are formatted extracts from the data within a database showing certain fields from certain records. Depending on the design, you may be able to go back and re-create a particular report with particular data at any time, or a report may be transitory indications of current status which will be irretrievable when the status changes.

Report creation can be quite an arcane science, and substantial skill or documentation can be required in order for them to be reliably recreated at some future date (if it is possible at all).

Exports and archives

Certain records and fields can be extracted from a database, in what could be either an 'export' (if done in essentially plain text files) or an 'archive' (usually if saved in some complex binary file format). Sometimes these are created on an *ad hoc* basis, but often they are part of routine data management procedures.

Conversion

Databases and records can sometimes be converted from one format to another. It becomes important to be able to determine if they are essentially identical or not after the conversion process.

2.6 Document management systems, logs, and transaction records

Modern digital document systems generate a large amount of data in operation, often as logs or transaction data. Various questions are raised about the value and accessibility of these working files:

- Are they reliable?
- What information do they hold, in what format?
- What do they show us when analyzed?

(See also section 8.1 for more on this topic.)

2.7 Networks and the virtual storage place

Digital resources are frequently held on network storage devices (i.e., a hard disk on a distant server) instead of, or as well as, on local devices like personal computers, laptops or, increasingly, on handheld PDAs or smart phones. The user may not be aware where the data he or she is using actually resides; the system administrator may not be aware where extracts or copies have been distributed.

Grid systems - Where is it stored, if anywhere?

Increasingly it becomes less certain where actual files are held, as RAID (Redundant Array of Inexpensive Disks) systems may distribute fragments or copies in several drives, and

newer grid computing systems may distribute them over components of a network (or even around the world).

Business-critical content can exist throughout the enterprise (in repositories, on the Web, on email databases or PSTs) in multiple languages, making all the issues of discovery and production even more challenging.

2.8 Web pages

Web pages can be simple and static, or complex and dynamically assembled. One could envisage a continuum, from simplest to most complex:

- Static (all text rendered by a Web browser reading the page is coded literally and unchangingly on the source Web document code often in separate files)
- Dynamic (what the user sees is a combination of static text from templates and elements that are assembled 'on the fly' from various sources, including databases and other programming systems)
- Host database (all aspects of the apparent document read by the user are created on the fly from a database containing all elements and functionality)
- International components (material assembled to show a page dynamically comes from several database servers in different countries)

It is clear from this that it may not be a simple task to establish exactly what was shown on a web page viewed through a browser at a given point in time, other than from a 'screen shot,' an image of a specific user's screen taken at that moment. In other cases, the web content is more stable and predictable.


file not found
TROJAN HORSE
VIRU
recovery
data lo

3 Overview of Obligations

This chapter provides an overview of the sorts of obligations to retain, produce or destroy digital documents that arise in typical situations. The next chapter gives more detail on specific examples.

This paper uses developments in Australian law as a starting point for examining these obligations, but the issues raised often have more general application. We also make reference to parallel or relevant US and European law. Similar challenges are emerging in these jurisdictions and in others around the world. While of course there remain substantial differences on particular principles, there is also increased international cooperation between regulators and courts, and bilateral and multilateral moves to harmonise at least some of the relevant laws, practices and standards.

3.1 Legal obligations: statutory, case law and code compliance

There are a number of reasons you may *wish* to retain documents in certain digital or non-digital formats:

- the documents may remain active within the organisation – that is, they may be needed for the day-to-day running of the business
- the documents may form an important part of a business's corporate memory, such as documents which have value as precedents or otherwise add to a corporation's knowledge base
- the documents may otherwise retain ongoing reference value within the organisation, for example employee files held by the human resources department
- the business may anticipate it will use the document in relation to a dispute (whether offensively or defensively)

A well-crafted digital document retention policy must include a method of identifying and tracking such documents, and setting out practical criteria for their creation or conversion, and subsequent retention or destruction.

However, such a policy will also need to analyse the second major reason for the retention of digital documents – where you are *required by law* to retain the documents. Such requirements will tend to fall into one of the following categories:

1. where a statute either:
   - specifically requires the retention of the document, or
   - operates in such a way that the document should be retained in order to prove compliance

2. where there are retention obligations related to compliance with industry codes or to satisfy industry regulators
3. where the retention of the document is required because there is a reasonable anticipation of litigation to which the document in question is likely to be relevant

This section provides an overview of such legal and compliance obligations.

3.2 Evidentiary issues and litigation

3.2.1 Circumstances where you must retain or can destroy

Certain statutes will require that particular types of documents be retained for a certain period following their creation. This may include, for example:

- obligations under the *Corporations Act* to retain financial records; and
- obligations under income and other tax legislation to retain supporting documentation; and
- certain professional obligations, such as lawyers' requirements under the *Legal Profession Act*.[1]

In addition to such statutory obligations, however, the common law may impose obligations on you to retain records, which are or may become relevant to litigation. Although the precise basis for this requirement remains somewhat obscure[2]:

- it is clear that once litigation is commenced, there is an obligation on the participants to retain all records relevant to the litigation; and
- prior to the actual commencement of litigation, it appears that a court will balance the knowledge of the corporation as to the likelihood of the litigation, and the reasonableness of the corporation's conduct in the face of such knowledge. A corporation, which anticipates litigation, is likely to have an obligation to retain all records potentially relevant to that litigation even before it has notice of the commencement of proceedings.

Further, certain industry codes of conduct to which your company is a party may require retention of particular records.

3.2.2 Responding to requests

Requests for information stored in retained documents may come from a variety of sources, such as:

---

[1] *Legal Profession Act* 1987 (NSW), <http://www.austlii.edu.au/au/legis/nsw/consol_act/lpa1987179/>

- requests relating to proposed or existing litigation, which could be:
  - **direct**, such as discovery obligations where you are a party to litigation; or
  - **indirect**, such as subpoenas or preliminary discovery obligations, where you may hold information relevant to proceedings to which you are not a party;

- requests from law enforcement agencies, for example to an ISP for subscriber details under the *Telecommunications Act* or to a bank for details of transactions under the *Financial Transaction Reports Act*.[3]

The precise detail of such obligations will vary, but, as a general principle, the scope of your obligations to provide information will be limited to information within your power or control.

3.3 Tactical requests

Finally, in this context, it is worth noting the increasing use of requests for information as a tactical "weapon" in commercial litigation.

A corporation, which does not have an adequate document retention policy, is clearly vulnerable to large-scale requests for records relevant to the proceedings which, whilst legitimate, impose a huge strain on corporate resources and add to the already stressful nature of the litigation.

In such circumstances, a corporation without an adequate document retention policy may be compromised in its ability to defend a claim properly, due to the excessive resources expended in responding to the request for information — it may simply choose to settle the litigation, notwithstanding good ultimate prospects for success in the case.

[2] See the discussion at paragraphs 1.2 and 4.1.

[3] See also US equivalents of the *Telecommunications Act* such as the *Cyber Security Enhancement Act*, section 225 of the *Homeland Security Act* of 2002 <http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm>.

4 Specific Types of Obligations

This chapter goes into some detail on obligations to retain, produce or destroy digital documents arising from a range of factors.

4.1 Obligations related to litigation

Is litigation contemplated?

Commercial cases comprise the bulk of all litigation before the courts. Every corporation should expect litigation in some form at some time. Once this is accepted, then the question really becomes, 'as a corporation, have we contemplated the realities of litigation, and the demands they would place on the corporation and its digital document assets?'

What level of foreknowledge is required?

Once a corporation gets into gear for addressing the real demands that litigation can place on it, then a key consideration that arises in the context of electronic document retention is the degree of knowledge of actual or impending litigation the firm has to have before it must alter its practices of electronic document retention and destruction.

Clearly, once legal proceedings have been instituted a corporation is obliged to preserve all potentially relevant documents in its possession. But what happens prior to proceedings?

As the case of *McCabe*[1] highlighted, it remains unclear under what circumstances a corporation can periodically destroy potentially relevant documents if it simply 'anticipates' litigation in the future, but is not yet actually involved in or on notice of any impending litigation.

Recently, the District Court in Queensland convicted a citizen for attempting to pervert the course of justice where that person had shredded papers knowing that they 'might' be required in judicial proceedings. (*R v Ensby*[2])

Until this conviction, Queensland, like every other Australian state, had maintained that there must be legal proceedings under way at the time records are destroyed before such a charge could be laid against an offender, be they an individual or corporation.

---

[1] See Section 1.2 above.

[2] Unreported, Queensland District Court, 2004, per Samios J; indictment 21/08/03, trial concluded 11/03/04.

In light of this judicial shift, it can no longer be safely stated that the decision in *McCabe does not* set a new standard of 'anticipation' in Australia, particularly when the Court of Appeal in *McCabe* went on to state:

> ... we consider that this court should state plainly that where one party alleges against the other the destruction of documents *before the commencement* of the proceeding to the prejudice of the party complaining, the criterion for the court's intervention ... is whether that conduct of the other party amounted to an attempt to pervert the course of justice or, if open, contempt of court occurring before the litigation was on foot.

In these circumstances, the issue of foreknowledge must be approached with the greatest caution. A corporation can choose to rely upon the pre-existing threshold of 'legal proceedings under way,' but as the Queensland case and above statement indicate, the judiciary appears ready to raise the standard to 'anticipation.'

Steps for dealing with foreknowledge

Chapters 6 and 7 provide considerations and examples of the type of digital document regime that a corporation should consider adopting. Once policy creation starts, tailoring is required to address the specific regulatory environment in which the corporation works. During this process a key *continuing question* always is, ' where can we reasonably expect litigation to arise?' As discrete areas of potential litigation are continually identified, destruction protocols must be adjusted for the longer retention of all related digital records.

Critically, corporations must ensure that they comprehensively document the end-to-end process of adopting a digital document retention policy, its continued assessment, adjustment, and the reasons why particular protocols have been adopted, right down to clear and reasonable descriptions of the types of files that are to be deleted.

In this way, when the first hint of potential litigation comes to the knowledge of a corporation, and is recorded as part of the general administration of the policy, then such a complete record showing reasonable response measures should assist to avoid the potential for damning allegations of purposeful destruction later.

4.2 Corporate governance obligations – directors and executives

Who is responsible for digital documents?

The responsibility for creating and implementing a digital document control policy rests with a corporation's board of directors.

Courts have only shown a willingness to question directors on this subject, therefore it must be assumed that the buck starts - and stops - at the board level. Specific definitive statements to this end are rare in national legislation. For instance, no specific provisions address digital document control policies within the *Corporations Act 2001 (Australia)*.

Establishment of a policy should really be viewed as a corollary of the specific legal requirements to retain records concerning the financial and other affairs of a corporation.

How should a board address digital documents?

Corporations must first locate, identify, network and synchronize servers, PCs, laptops, home office hardware, PDAs and foreign offices, before the task of electronic data management can properly begin. Paper's weight and space has been replaced by the complexities of computing.

Cases such as *McCabe* and the Enron matter inform us that boards need to be aware that all recoverable electronic data, from complex meta forms to simple spreadsheets, is discoverable at law. All data is therefore valuable, and if unreasonably destroyed or missing, then potentially lethal at law.

Due to the complexity of information technology and the fact it requires specialised learning to understand and manipulate, when creating and implementing a digital document control policy, directors and company officers should take advantage of provisions, which entitle them to rely upon, delegate and use advice from specialist employees or external IT advisors. For instance, see ss. 179 – 190 of the *Corporations Act 2001 (Australia)*.

How should a board begin to delegate responsibility?

At a minimum, board governance duties will be satisfied on this issue by the creation of a committee specifically tasked with the formulation and implementation of a digital document control policy containing underlying retention and destruction protocols.

A board must then ensure that it becomes reasonably informed about the details of the policy that is created, should satisfy itself about recommended protocols, and thereafter should continually and reasonably review the depth, breadth and strict implementation of the policy on a regular basis.

Necessarily such a committee will require the continued involvement of both corporate in house counsel and the chief technology officer, or their equivalents, and they should regularly update the board with the committee's progresses.

The general form of mandate by which a committee should begin to operate is further addressed in Chapters 6 and 7.

4.3 Obligations concerning taxation and money laundering

There is extensive legislation setting out a wealth of obligations in relation to records for taxation and the tracking of cash transactions and money laundering. The details of these are outside the scope of this paper. Specific advice on the details of these obligations on your particular circumstances should be obtained from a lawyer or accountant.

The digital aspect will be introduced not only by the internal storage and processing tools used to record financial transactions (accounting, billing and payment systems), but also when external banking, business and consumer transactions are put online, with a consequent increase in the importance of ensuring the availability of digital equivalents to traditional transaction records.

4.4 Human resources, employment, administration, accounting

There are a wide range of obligations on organisations in relation to human resources and employment, administration, and accounting systems. The details of these are outside the scope of this paper. Again, advice on the detail of these obligations on your particular circumstances should be obtained from a lawyer or accountant.

It will be important to update internal policies to take account of new technical developments, such as employee self service Web sites, outsourced administrative data processing, and the introduction of new accounting and auditing standards.

4.5 Legal professional practice and 'privilege'

What is 'legal professional privilege'?

Legal professional privilege is a special status that attaches to communications and materials generated between a lawyer and client in anticipation of or in preparation for legal proceedings. Communications and materials that are privileged in this way cannot be accessed by the opposing party in litigation, so they do not form part of the materials that may be required for disclosure when discovery takes place.

Can you claim privilege over digital documents?

Absolutely. For instance, it has become common practice for lawyers and clients to communicate via the Internet, where documents relevant to pending litigation are commonly attached to emails. Such attachments, if created in anticipation of litigation, would normally be privileged.

Can you lose privilege over digital documents?

Once again, yes. The confidentiality that privilege affords can be deemed lost by a Court if a communication is disclosed or somehow revealed to a third party, or to the opposing party through inadvertence. If privilege is lost, then the other side can seek to use your confidential communications to their own ends.

Generally speaking, if a privileged email is sent to the wrong recipient, even though inadvertently, this could ground an argument that the party waived privilege over the email, thereby making that email discoverable by the opposing party.

Similarly, if a digital document is sent to a lawyer and also to an expert assisting with the litigation, and if that expert produces a report for use in the litigation which also mentions details of the transmitted document, then again privilege could be lost over all of the contents of that document.

On another front, when a company's electronic files are subject to pre-trial orders for discovery, if these files are not properly reviewed by lawyers assisting in the matter, then files over which privilege could be claimed could again inadvertently be copied and sent to the opposing side.

Alternatively, the files created and retained by a lawyer in preparation for litigation could also be improperly accessed and released into the public domain. Regardless whether the release is through negligence or by the commission of a criminal act, once the privileged document makes it into the public domain, a client could expect all privilege to be lost.

How can you protect privilege over digital documents?

Lawyers are obliged to ensure the reasonable protection of their client's confidences. As such, a lawyer's choice of communication medium must provide a reasonable expectation that such protection will be afforded to any communication. Lawyers and their clients should examine their choice of communication medium as soon as litigation is anticipated.

Besides the traditional use of telephones and fax machines, lawyers and clients who propose communicating via email should assess the methodology they propose to use.

Email communications can be, either separately or in combination:

- by normal open email channels,
- via direct link (secured) extranet,
- authenticated by digital signatures, and/or
- highly secured, by encryption.

The level of security to be used should be in response to the content of the communication, where lawyers should instruct their client as to how to assess the importance of each communication. Given the increasing availability of encryption software today, then the option of providing the full range of potential security measures should not be ignored.

When discovery is taking place, all digital documents must be properly reviewed by lawyers assisting, so to ensure that no privileged documents go where they should not. This process should involve the use of meta data software search tools to help ensure that all duplicates of privileged documents are located in archives, individual computers or servers, backup tapes, PDAs and the like.

Being generally prepared is always the best course for possible litigation. The company that already has a digital document litigation protocol in place will avoid paying premium costs to quickly implement software and experts for the entire process, let alone the task of separating out privileged documents from archives and other storage mediums.

The security of privileged digital documents held within a law firm is usually given the utmost attention. However, given the increasing prevalence of computer hacking today, firms should be seen to operate at least in conformity with minimum standards set down

by such groups as:

- The International Organisation for Standardization (ISO)
- Standards Australia or equivalent
- State and Federal Law Societies and Bar Associations
- State and Federal record keeping agencies

4.6 Obligations related to Insurance

Officers and directors insurance and general company insurance terms and conditions vary with each policy written. Inadequate digital document retention policies could, in some circumstances, lead to a loss of coverage, depending on the significance of digital records for the organisation's business and the particular claim in issue.

Most policies will deny coverage wherever it can be shown that the company or one of its officers acted without good faith, or acted with an intention to cause harm, or wherever a judicial determination of contempt and/or attempting to pervert the cause of justice is proven.

The legal devices by which insurance companies seek to deny coverage are by no means limited, and could be expected to grow once courts and legislatures better clarify offences concerning corporate record keeping, particularly in relation to records that *may* relate to future litigation.

For those companies that choose to properly invest in the creation of a digital document retention and destruction policy suited to their risk profile and business, there is an argument that once routinely implemented, an insurer should be willing to consider providing a discount on your usual premiums for the added security that the policies provide.[3] (There may be some practical limitations, like the ability of an insurer to audit the target company, but the existence of and use of a clear policy would be the first step towards satisfying such an insurer.)

4.7 Obligations related to the public

The *Privacy Act 1988 (Australia)* and the *Corporations Act 2001 (Australia)* place clear obligations on companies to deal with personal information and business records in a prescribed manner, or so as to comply with broad principles such as Australia's *National Privacy Principles* (NPPs), which were based originally on OECD guidelines.

These NPPs set out the legal basis for record-keeping practices dealing with 'personal information' (information which can be linked to an individual) in areas such as security, accuracy, access, right to correction, restrictions on non-consensual use, or disclosure except for legally authorized purposes, and so on.[4]

---

[3] See for example Kalinich K and M Greisiger, 'Network Risk Insurance: A Layman's Overview,' Aon and NetDiligence, July 2004, <http://www.arma.org/pdf/articles/NetworkRiskOverview.pdf>.

[4] By comparison, in USA see *Privacy Act of 1974*, and in Europe the *EU Directive 95/46/EC*.

Companies operating in the finance sector also have the additional burden of the *Financial Services Reform Act 2001 (Australia)*.

Failure to observe the provisions of these Acts can and does result in financial and other penalties to corporations, adverse findings by regulators such as the Office of the Federal Privacy Commissioner (such as those in the recent complaints about the TICA tenancy databases[5]), and at times the loss of operating rights.

The *Financial Services Reform Act* places a particularly high level of recording and reporting standard upon companies. Due to the large number of intermediaries and individuals involved with the provision of financial products, it is now of the utmost importance to be able to prove the form and content of every step in the various processes used for the supply of these products. This becomes particularly significant in non-traditional work settings such as call centres, which may operate with a high proportion of digital rather than hard copy documentation.[6]

However, the *Privacy Act* does not so clearly prescribe periods for which organisations should retain certain personal information before it can be destroyed. In the absence of industry codes of practice or other guidelines which operate in some sectors, in many instances it becomes a judgment call for the individual company concerned, based on the circumstances of its business and the records it keeps in relation to identifiable individuals, one that can not be taken lightly due to the penalty provisions involved.

4.8 Obligations related to intellectual property

Copyright

Proving copyright in material often involves showing that you or your organisation was the 'first in time' to produce certain content. Having implemented a secure and reliable digital document retention policy helps overcome the evidentiary hurdles when faced with litigation for proving who in fact possesses the rights, whether it be for printed material or software. Such a system would of course record all the attributes of copyright files, to enable comparison with alleged infringing copies.

Digital Rights Management Systems (DRMS) are increasingly being used to document, assert and enforce claims of copyright over digital artefacts. A detailed treatment is beyond the scope of this paper.

Even without a full-blown DRMS, any creation of material for further external use based on existing content should entail a logging production system for recording the ownership of such content and the steps taken to 'clear' it for use with such owners.

---

[5] *Tenants' Union of Qld Inc v TICA Default Tenancy Control Pty Ltd.* Determinations on four representative complaints about accuracy, cost of access for correction, security, relevance, completeness etc. are described at <http://www.privacy.gov.au/news/media/04_07.html>, and found in [2004] PrivCmrA 1 through 4, at <http://privacy.gov.au/act/casenotes/comdeter0401.html> through <../comdeter0404.html>.

[6] See also US equivalents such as the *Financial Modernization Act* of 1999 (also known as the *Gramm-Leach-Bliley Act*).

Patent

Patents on the other hand are typically the province of national governments through registration bodies such as patent offices, like IP Australia. However an accurate document retention policy could prove decisive when seeking to resist claims of "prior art" that could lessen or obliterate expected rights to a new invention. Conversely, an accurate document policy could greatly assist with attacking another organisation's claims to hold patent rights.

Given that a great many of the disputes in this area occur across national borders, it may become important to have in place a document retention policy that meets national and international standards – particularly when there are differing evidentiary requirements and standards of proof in foreign jurisdictions where a company may be forced to comply.

5 Evidence

There are detailed rules on what may be introduced into a court case as evidence; whether these enable a certain document to be admitted or not may be crucial to the outcome of a case.

5.1 Factors affecting validity and admissibility

In general, digital documents will only be considered to valid and admissible as evidence in litigation if they can be authenticated. In assessing the authenticity and integrity of such documents, a number of factors are often considered, including:

- Are electronic signatures used to identify the originator of the digital record?
- Are formalized business processes and procedures in place to verify the production of digital records in the course of business?
- Are formalized business processes and procedures in place to verify the secure storage of digital records?
- Can audit trails easily be produced to trace the movement of the digital record in the organisation?
- In the case of electronic communications, is there an adequate system design to identify the destination, time of sending and time of receipt of the electronic communication?

5.2 Conversion from paper to digital form

The two key issues that arise when considering whether to convert paper records into digital form are:

- Will the digital documents be admissible as evidence? (i.e. are the digital versions still reliable?)
- Will the digital documents be given the same evidentiary weight as an original document in paper form? (i.e. how reliable are the digital versions?)

Many jurisdictions, during the last decade, have introduced specific modifications to their evidence legislation to account for digital documents. The definition of "a document" is generally broad enough to encompass digital records easily. Therefore, in most jurisdictions if a computer is used in the course of business to produce documents with certain characteristics then documents produced by that device are presumed to have those characteristics.

For example, a document produced by a computer is presumed to be an authentic copy of an electronic record in the absence of evidence suggesting the computer was not working properly at the time of producing the document.

5.3 Business records

What are "business records"?

A “business record” is generally taken to be any book of account or other document prepared or used in the ordinary course of a corporation’s business for recording any matter relating to the business.

Business records are, in many jurisdictions, an exception to the hearsay rule of evidence and are admissible as evidence.

When it comes to keeping business records, it is therefore important to ensure that there are procedures in place to substantiate the fact that a particular record is regularly used in the ordinary course of business and are reliable enough to be considered a business record for evidentiary purposes.

Equivalence after format conversion

Business records may include digital images of hard copy documents. A specific issue arises when there is any process, which may effectively convert a file or message etc. into another format: has anything significant changed in the translation, or is the information content essentially the same in both formats?

5.4 Digital copies and verification

What is a copy? Is it equivalent to the original after copying or conversion?

The best evidence rule is a common law rule, which requires litigants to present the “best evidence” to the court, rather than some secondary record or copy. Specifically, it required the production of the original of any document by the tendering party to prove its contents, unless the absence of the original can be explained.

Even without amendment to the best evidence rule, if an original document had been destroyed as part of a digital recording process, the destruction would be explicable and the digital record would have become the “best evidence” required for production to the court. The rule would not have required the original documents to be saved in case of litigation.

Does it matter if you do not copy everything?

Although it is good practice to do so, in most jurisdictions there is generally no requirement to copy everything in a particular document (such as all the annexures and appendixes), especially if the parts not copied are not relevant as evidence in proving a particular fact

Where parts of document are not copied, it is good practice to record the nature of the information that was not copied and the reason it was not copied.

When is it acceptable to destroy the original if you have a copy?

If you have a copy of the original, for evidentiary purposes, there is generally no requirement that you must keep the original. The best evidence rule applies, meaning that if the original is destroyed, then the copies will be used as the next best form of evidence. This generally applies to digital images of hard copy.

There may however be some exceptions where a country's legislation requires that originals be presented as proof for specific documents, such as certificates of title or notary public seals. It is important that you are aware exactly what documents are required to be presented in their original form, and ensure that these originals are not destroyed.

5.5 Steps to assess a record for archiving and/or destruction

The decision-making process for determining if a record should be archived or destroyed involves going through the below step-by-step process in order to satisfy yourself that retention is *not* required.

Step	Response	Action
1. Is retention required for current use?	❑ Yes	Archive
	❑ No	Go to 2.
2. Is retention required by contract?	❑ Yes	Archive
	❑ No	Go to 3.
3. Is retention required by law or regulation?	❑ Yes	Go to 4.
	❑ No	Go to 5.
4. Is the limitation period for retention still applicable?	❑ Yes	Archive
	❑ No	Go to 5.
5. Is retention required for business reasons?	❑ Yes	Archive
	❑ No	Go to 6.
6. Is retention required for litigation or other special circumstance?	❑ Yes	Archive
	❑ No	Destroy


SECURE
DATA

6 Governance

6.1 Developing internal digital document control policies

A digital document control policy should seek to completely and faithfully automate the entire life cycle of all documents within a company, from their creation to destruction.

Once an organisation establishes a committee for the creation of a digital document control policy, that committee must begin by addressing key issues that form the substantive basis of the policy.

What is the company's regulatory environment?

The committee must identify the regulatory environment that the organization operates in, for instance:

- What statutes and case law directly affect the company?
- What codes, standards and/or rules of professional practice are the company obliged to follow?
- What codes, standards and/or rules of practices could the company choose to further comply with?

Key factors affecting your Digital Document Control Policy

The committee must simultaneously develop a firm-wide digital document policy that will orchestrate how all the regulatory factors are to be dealt with. Key considerations to be kept in mind are:

- Are sufficient records being created, received and used to meet all *compliance* and *regulatory* issues?
- Are records being stored on appropriate *media*? (this covers not only digital media, but also the hard copy or digital option for paper originals)
- Is the data within all records in functional *formats*?
- Is all data and meta data *accessible* now, and will it always be in the future, despite foreseeable and unforeseeable changes in IT?
- Is all data and meta data *secure* now, and will it be in the future, despite foreseeable and unforeseeable changes in IT?
- Can the company *provide evidence* for the *authenticity* and *integrity* of each record that is created, received and used within the company?
- Is the implementation and continued operation of the policy and its underlying protocols being itself *adequately documented*?
- Where protocols eventually call for the deletion or destruction of documents, are full and adequate *descriptions* of those documents being *retained*?

What are the benefits of a digital document control policy?

After implementation of the policy several benefits should be seen to flow to the company. For instance:

- Improvements in decision making processes
- Reduced paper costs
- Reduced reliance on paper storage requirements and associated costs
- Reduced costs for couriers, postage and fax communications
- A better balancing of workloads between departments and satellite offices
- A streamlining of the compliance process with statutes, rules and standards
- An ability to guarantee the accuracy, authenticity and integrity of documents
- The ability to track and record the entire life cycle of all documents required for legal purposes.

6.2 Who else should be responsible for the digital document control policy?

Once all aspects of the regulatory environment have been itemised and readied for specific attention in accordance with the control policy, the next task is the committee's assigning of responsibility for protocols and various regulatory items. Regulatory items affecting the company must be apportioned appropriately between executives, record management professionals, system administrators and other staff.

Records managers: Internal records managers should be tasked to design, develop and implement the digital records system and required protocols, in co-ordination with system administrators. It is advisable to pilot, test and refine such systems and protocols with actual users and support staff prior to enterprise-scale rollout.

Supporting infrastructure: In turn, systems administrators must be tasked to have in place hardware and processes that insure all digital documents remain accurate and accessible at any given time, including after inevitable changes to IT. IT managers should be made aware of the various evidentiary and long-term production requirements, and asked to explicitly address technical obsolescence of media formats, and meta data features, which offer proof of certain essential attributes of digital documents as evidence (see above).

Training: All employees must undergo training to inform them about the digital records system and processes, the regulatory environment that requires a policy, the responsibilities they must adopt to assist directly with observance of the policy, and particularly how each employee's specific duties affect the proper observance of the policy, right down to discrete items such as memos and emails. (This may also be a good time to make sure there is a sensible and widely understood policy about email and web usage.)

Compliance and enforcement: Lastly, senior executives must insure the continued firm-wide adherence with and implementation of the policy, and they must utilise an appropriate reporting system for efficiently communicating with the committee all

issues as they arise regarding ongoing adherence and implementation of the policy. Where anomalies or practical difficulties do arise, these should be addressed explicitly (perhaps by variation of the digital document policy) rather than being seen merely as a compliance problem.

6.3 Other matters

Due diligence: Bear in mind that external and internal due diligence investigations may take into account the state of an organisation's document management systems and information assets, and whether the stated policies and actual practices give confidence that appropriate records would be available to meet a variety of foreseeable risks. One feature of this inquiry may be the degree to which the unique challenges of digital documents have been addressed.

Standards: Local and international formal standards can establish the foundations for what constitutes standard practice, and should be explicitly taken into account when developing a digital document retention policy. See the next chapter for more details.

Customised: Your specific circumstances should affect the strategic approach and the procedural details of a digital document retention policy, as simply adopting a generic policy may not be appropriate for your risk profile, technical infrastructure or operational realities, or specific enough to give necessary guidance to users.

7 Creating a Policy

So what do you look at for taking concrete steps to deal with the problems revealed above? This chapter provides the authoritative sources to start the process properly in the absence of external professional assistance.

7.1 How do you develop a policy to deal with all these issues?

Section 4.2 and Chapter 6 broadly described the main considerations and issues that a corporation must investigate when formulating a digital document policy.

A helpful flow chart for the entire process can be found in the Australian Standards 'Guidelines' for AS ISO 15489 at 3.2.1

This chapter highlights specific Standards that have been developed and adopted around the world and within Australia. The Standards described below are used by the home government departments in the countries of their creation (and by degrees their private industries and business communities), therefore each of the Standards has been tried and tested before being incorporated into governmental practice.

A written and effectively distributed internal policy document encompassing both digital and paper records can provide strong evidence that a company has legitimately destroyed documents by following reasonable and objective standards. Bolstering such a conclusion would be clear evidence of a firm having reasonably incorporated variously stated domestic and international Standards.

However, the creation of a firm-specific digital document policy is no easy feat. The authors suggest that firms consider consulting with digital document management professionals, particularly in view of the ease with which essential issues could be overlooked, and for the other reason that what may appear to be too difficult for a firm to implement itself from first principles may nevertheless be readily and affordably solvable by those with extensive practical experience in the field.

7.2 Classification of documents

A fundamental issue for the policy is to assist the classification of documents into categories that have consequences for decisions on use, retention or destruction.

Criteria These classification criteria will need to be tailored for both operational business needs, and the specific retention or destruction obligations revealed by a detailed analysis of the legal and other constraints on your various activities and digital assets. The classification criteria and policies will need to be checked by a variety of stakeholders and advisers, and refined by trials in practice.

Simplicity The criteria and classification procedures will become embedded into the core processes of the organisation, so they should be as simple and clear as possible while still permitting the various requirements to be met.

Who decides? Substantial effort may be required to establish efficient procedures for the involvement of various people in the classification process. Depending on the nature of the criteria, certain classification decisions may need to be made by more senior staff or even legally qualified advisers, while the bulk of such decisions should be made routinely, either by automated methods or simple choices at the time of creation.

Review Classification does not necessarily occur just once. A routine process of reviewing document classification, or at least the triggers for such a review, should be described.

This is so that if circumstances change (such as through the onset of a litigation risk, or a fundamental change in a technical process supporting certain types of digital document) certain groups of documents can be reviewed for reclassification – otherwise they may be inadvertently retained or destroyed inappropriately to new circumstances.

7.3 Document and media formats

A *Digital Document Retention and Destruction* policy needs to explicitly address the issues surrounding document and media formats, including:

- standard file and media formats
- backup and archive formats
- expected format conversions for archiving or exporting
- long term compatibility issues
- processes for different physical and electronic media
- the approach to determining and changing decisions on these issues.

7.4 Guidelines: what should be included?

With the global standardization of IT software and systems, together with what appears to be a judicial determination to standardize a common cross-border jurisprudence towards IT evidentiary issues, it is no longer surprising to find that IT standards in many countries are beginning to reflect one another.

With the above in mind, the reach of a firm's business beyond its national borders should, we believe, require that a firm at least examine and consider the adoption (partially or otherwise), of standards found outside its home country.

At the very least, a digital document policy should seek to strongly reflect those standards already created within a firm's home country.

Sedona Principles

These principles were created by a group of leading US litigators in response to evidentiary and record keeping responsibilities arising out of Enron, Arthur Anderson and the *Sarbanes-Oxley Act of 2002.*[1]

Most of the 14 principles concern issues endemic to pre-trial discovery, which are instructive for any lawyer. However, attention is directed here to the first principle, which states:

> "Electronic data and documents are potentially discoverable under FED.R.Civ.P. 34 or its state law equivalents. Organisations must properly preserve electronic data and documents *that can reasonably be anticipated to be relevant to litigation."*[2]

This principle is emphasized purely to show the detail to which a digital document policy should run. Failure to create a truly global policy that readily provides for response actions when notice of litigation is received could see all prior efforts with creating and adhering to an effective policy made irrelevant once a firm walks into a courtroom, if its policy failed to address what to do when litigation is on foot.

Australian standards

Australia's current Australian Standard is AS ISO 15489 entitled 'Records Management,' published on 13 March 2002.

The Standard comprises two parts, 'General' and 'Guidelines,' and was prepared for both paper and electronic documents. The Standard is available via Australian Standards' subscription service for a small fee.[3]

This Standard was created by a working group consisting of Federal and State government agencies, Australian universities, together with representatives from private document management companies. The Standard is exhaustive in detailing the many issues and considerations that a company should examine when formulating a policy, and as such is an excellent tool for any firm needing to create a digital documents policy.

Of particular note is the fact that the International Organisation for Standardisation (ISO) (see below) chose Australia's former AS 4390 Standard in this area as the model for international standardization. As such, Australian Standards have only improved upon an already internationally recognized benchmark with the production of AS ISO 15489.

---

[1] Other relevant US legislation includes *Health Insurance Portability and Accountability Act* (HIPAA), *California Security Breach Information Act* and the *Support Anti-Terrorism by Fostering Effective Technologies Act* of 2002.

[2] Sedona Conference, *The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production* (2004) <http://www.thesedonaconference.org/miscFiles/SedonaPrinciples200401> accessed at 23 August 2004.

[3] *Standards Australia* (2004) <http://www.standards.org.au> accessed at 23 August 2004.

However first instance resort to a digital document management company could save a firm both time and money when first confronting this complex terrain, particularly where document management consultants are already specialists in the field of business of the company needing a policy.

US standards

DoD In the US an influential standard of compliance came out of the Department of Defense on June 19, 2002, known as the 'Design Criteria Standard For Electronic Records Management Software Applications' (5015.2-STD).[4]

Though the level of detail is at times extreme due to its use throughout the US military, (and due to the number of personnel and the computing power it has at its disposal), it has nonetheless been adopted and largely implemented (when suitably tailored), by many US agencies and businesses. It is a very instructive model for IT management processes for data. Note also that in 2003 NARA endorsed this DoD standard.[5]

Use of this standard (or aspects of it) by any corporation is a question of what a corporation really needs. Should security over sensitive data be a prime issue for a firm, then the DoD's approach has a lot to offer, particularly since so much security software produced since 2002 complies with this standard.

NARA Otherwise, for a less extreme standard used by many other US government agencies, see the National Archives and Records Administration's (NARA) 'Electronic Records Management.'[6]

NARA's policies and the Australian Standards' complement each other well.

International standards

As mentioned above, the International Organisation for Standardisation (ISO) used Australia's former digital document Standard (AS 4390) for production of the ISO's most recent Standard in this area – the 2001 document *Information and Documentation – Records Management* (ISO 15489).[7]

Though there is much to be said for following instead the current Australian Standard mentioned above, consideration should be given to the fact that the ISO Standard had first to be adopted by no less than 75% of the 148 member countries, who worked in partnership with international organizations, industry, business and consumer representatives.

---

[4] United States Department of Defense, *Design Criteria Standard for Electronic Records Management Software Applications* (2002) <http://jitc.fhu.disa.mil/recmgt/p50152s2.pdf> accessed 23 August 2004.

[5] <http://www.archives.gov/records_management/policy_and_guidance/bulletin_2003_03.html>.

[6] NARA, 'Part 1234 – Electronic Records Management' in *NARA Code of Federal Regulations* (2001) *<http://www.archives.gov/about_us/regulations/part_1234.html>* accessed 23 August 2004.

[7] ISO, *ISO 15489-1* (2001) <http://www.inform-consult.com/download/ISO_15489-1.pdf> accessed 23 August 2004.

As such, any firm at least complying with the current ISO Standard would, in a judicial respect both here and overseas, be likely to be seen to have implemented a legitimate digital document policy.

EU standards

The current EU policy is contained in the March 2001 document, 'Model Requirements for the Management of Electronic Documents.' Also known as the MoReq Specification, it primarily focuses upon electronic data, and was placed forward to be used by EU governmental members and agencies, as well as for use by European industry and business.[8]

The Specification is specifically for the management of records by an Electronic Records Management System (ERMS).

This Specification is another worthy and comprehensive resource, and its production relied upon ISO Standard 15489 and the US DoD's Design Criteria. However it may be counter-productive for a corporation to expend its time and money considering every aspect of this lengthy document (particularly one designed for the EU), especially since Australia's own Standards are held in such high regard internationally.

In the result, companies that create and implement digital document policies incorporating all the essential considerations mentioned in the above standards will not only have ensured that their enterprise works better, but will have consciously safeguarded the enterprise from the many pitfalls and costs associated with litigation, should it arise. This may help underpin its real commercial and net value.

(Although primarily aimed at the public sector, which is outside the scope of this paper, useful guidelines from the UK Public Records Office, now known as 'The National Archives,' could also be considered here,[9] as could VERS.[10])

[8] IDA, *Model Requirements for the Management of Electronic Records* (2001) <http://europa.eu.int/ISPO/ida/export/files/en/635.pdf> accessed 23 August 2004.

[9] <http://www.nationalarchives.gov.uk/electronicrecords/>

[10] <http://vers.imagineering.com.au/regulatory_environment/uk.htm>

8 Pulling it All Together

Once the digital document types are identified and analysed, the obligations for each type are understood, the classification criteria developed, and procedures trialled, these components can be drawn together and integrated into normal operations.

8.1 Interaction with document management systems

The smooth operation of a *Digital Document Retention, Destruction and Production* policy will depend on how well it interacts with and is supported by tools such as Document Management Systems (DMS). A critical issue is the interface with hard copy documents.

You need to inspect the range of functional options presented by your DMS, as actually installed, configured and used in practice (or as you intend to implement it in future), to assess the degree to which it is viable to take advantage of the opportunities it offers.

Records management applications can be deployed in organizations with or without document management systems in place. Records management provides a strong complement to *document* management by asserting full control over records to ensure compliance with current regulations and best practices. The leading records management solutions are often integrated with document management solutions, and are built specifically to address the retention, disposition, and authentication goals that are unique to information compliance. Records management modules have been designed to address regulations that specify not only which documents to protect but how to protect them.

Document Management Systems store a variety of content types in a special repository, supplemented by tools to improve information handling and automate business processes. Among the core services typically provided by a DMS are:

- Version control: Enables tracking of document versions to ensure team members work from the most recent draft.
- Library services: Provides check in/check out capabilities to eliminate simultaneous edits and duplicate work.
- Workflow: Streamlines business processes by automatically routing documents, internally among co-workers and externally among partners or suppliers.
- Lifecycle management: Manages movement of content through stages such as reviewed, approved, published, archived, and retired.
- Security: Controls access and editing rights through user-based and role-based privileges, often with LDAP, SSL, and digital certificate support.

- Audit trails: Tracks changes, downloads, delivery, printing, and other events to ensure government and industry compliance.
- Full-text searching: Enables navigation of large sets of information without knowing how it is organized or stored.

8.2 Implement and integrate

The components of the policy need to be integrated into a master document.

Draft materials for various groups of users may be derived or extracted from this master document, then checked and tested in practical trials. All the various work groups affected by with the policy should be involved in these trials, and the assessment of changes likely to be required in their areas.

Once you are satisfied that the revised core policies and the associated materials for various user situations have been proven in practice, it is time for rollout and implementation.

This should include a substantial training component at all levels of the organisation, and extra assistance tailoring the policy to specific critical areas.

8.3 Audit and evaluation

It is important to design a development, audit and evaluation process to assess and help refine the operation of each part of the policy in each area of work and with each document type.

This audit and evaluation is worth doing both during the initial implementation stage to fine tune the policy and criteria before they are fully established, and also later in a routine maintenance mode, to demonstrate things like:

- The policy is well known, understood and implemented in practice, with a training element and appropriately helpful documentation.
- All digital documents are classified according to the policy, and as far as possible, that classification is associated directly with the document to enable automated processing of rules.
- Backups can actually enable restoration of intended files.
- Archives exist and are in a format that will remain accessible for a long time, and have been constructed according to the policy, and the classifications in it.
- Litigation risks have been identified and reviewed, and their relevance to specific document types and classifications has been taken into account in automated and manual processes.
- Staff are aware of the nature of risks concerning email, and take these into account in its use and management.
- Retention and destruction of digital documents of all types and in all areas of operation occurs subject to the policy and the controls it stipulates.
- Staff are aware of the hazards of a mix of digital and hard copy documents in a variety of systems, and have rules of thumb for managing these hazards.

In many cases, the audit process may merely confirm that you have got it roughly right, but it is important to carry out such an exercise at various times to ensure that the system you set up is viable and operational in all major respects. As discussed above, it may be too late or too expensive to fix it if failure is revealed only at the onset of an external crisis or litigation.

The audit should be integrated with the audit processes for other aspects of the organisation's activities, but produce a specific report addressing the adequacy and operation of your Digital Document Retention, Destruction and Production policy.

9 It's not too hard!

We started by noting the discomfort that consideration of the complexities of digital document management can sometimes cause, and the tempting call of the 'too hard' basket.

We have shown how you can analyse the various technical, legal and business issues in turn, and then develop a range of actions that can both reduce the risk of a digital document disaster, and at the same time increase the value of your information assets.

We hope that by now you will have concluded that it is not all too hard.

You need only go into a little more detail than we have covered here to ensure that the specific circumstances of your situation are properly taken into account along with the general principles we describe. We have mentioned a few of the types of expert assistance that may be of value in such an exercise. Eventually the outcomes of such a review will just be integrated with other IT and operational issues to help refine your standard operating procedure.

The benefits of dealing with these matters properly and in advance outweigh the risks, and in time, we expect that this will become just another policy for the modern corporation to use to encourage compliance with best practice and good governance.

Think how glad you will be when you can find all your documents – even if the one you are looking for has been deleted, you will know where it went and why. We hope that this will bring relief from that nagging concern that there may be a nasty surprise awaiting somewhere in your organisation's tangle of data, documents and records.

10 References

Standards, laws, cases and articles referred to in the text and footnotes.

10.1 Standards

IDA, *Model Requirements for the Management of Electronic Records* (2001), <http://europa.eu.int/ISPO/ida/export/files/en/635.pdf>, accessed 23 August 2004.

ISO, *ISO 15489-1* (2001), <http://www.inform-consult.com/download/ISO_15489-1.pdf>, accessed 23 August 2004.

NARA, 'Part 1234 – Electronic Records Management' in *NARA Code of Federal Regulations* (2001) <http://www.archives.gov/about_us/regulations/part_1234.html>, accessed 23 August 2004.

Sedona Conference, *The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production* (2004) <http://www.thesedonaconference.org/miscFiles/ SedonaPrinciples200401>, accessed at 23 August 2004.

Standards Australia, AS ISO 15489 *Records Management*, 13 March 2002, <http://www.standards.org.au>, accessed at 23 August 2004.

United States Department of Defense, *Design Criteria Standard for Electronic Records Management Software Applications* (2002), <http://jitc.fhu.disa.mil/recmgt/p50152s2.pdf>, accessed 23 August 2004.

10.2 Laws

Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, 847 UNTS 231 ('Hague Convention on Taking Evidence', convention No. 20), <http://hcch.e-vision.nl/index_en.php?act=conventions.text&cid=82>, accessed 23 August 2004.

Corporations Act 2001 (Australia), ss. 179 – 190, <http://www.austlii.edu.au/au/legis/cth/ consol_act/ca2001172/>, accessed 28 August 2004.

Directive 95/46/EC EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf>, accessed 23 August 2004.

Financial Modernization Act of 1999 (USA), also known as the *Gramm-Leach-Bliley Act,* <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws &docid=f:publ102.106>, accessed 28 August 2004.

Financial Services Reform Act 2001 (Australia), <http://www.austlii.edu.au/au/legis/cth/consol_act/ fsra2001242/>.

Financial Transaction Reports Act 1988 (Australia), <http://www.austlii.edu.au/au/legis/cth/ consol_act/ftra1988308/>.

Homeland Security Act 2002 s.225 (USA), also known as the *Cyber Security Enhancement Act* , <http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm>, accessed 23 August 2004.

Legal Profession Act 1987 (NSW), <http://www.austlii.edu.au/au/legis/nsw/consol_act/ lpa1987179/>

Privacy Act of 1974 (USA), <http://nces.ed.gov/statprog/rudman/c.asp>.

Privacy Act 1988 (Australia), <http://www.austlii.edu.au/au/legis/cth/consol_act/ pa1988108/>.

Sarbanes-Oxley Act of 2002 (USA), <http://www.aicpa.org/info/sarbanes_oxley_ summary.htm>.

Telecommunications Act 1997 (Australia), <http://www.austlii.edu.au/au/legis/cth/consol_act/ ta1997214/>, accessed 28 August 2004.

10.3 Cases and litigation

British American Tobacco Services Limited v McCabe [2002] VSCA 197 (6 December 2002) <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/vic/VSCA/2002/197.html>, accessed 23 August 2004.

Letter of Request from US Department of Justice to the Supreme Court of NSW, 3 October 2002 <http://www.usdoj.gov/civil/cases/tobacco2/Nicholas%20Cannar%20letter.pdf>, accessed 23 August 2004.

McCabe v British American Tobacco Services Limited [2002] VSC 73 (22 March 2002) <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/vic/VSC/2002/73.html>, accessed 23 August 2004.

R v Ensby (Unreported, Queensland District Court, per Samios J, concluded 11 March 2004).

The Application of Nicholas Basil Cannar; re Sharon Y Eubanks, being the person nominated by the United States District Court for the District of Columbia in proceedings United States of America v Phillip Morris Incorporated et al Civil Action No.99-CV-2496 (GK), for the purposes of applying for orders under section 33 of the Evidence on Commission Act 1995 [2003] NSWSC 802 (8 October 2003), Supreme Court of NSW (Bell J) <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/supreme%5fct/2003/ 802.html?query=%22letter+of+request%22>, accessed 23 August 2004.

Sharon Y Eubanks for the United States of America v. Nicholas Basil Cannar and British American Tobacco (Investments) Limited [2003] NSWSC 1267 (19 December 2003), <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/supreme%5fct/2003/1267.html?query=%22letter+of+request%22>.

Tenants' Union of Qld Inc v TICA Default Tenancy Control Pty Ltd. Four determinations [2004] PrivCmrA 1 through 4, <http://privacy.gov.au/act/casenotes/comdeter0401.html> through comdeter0404.html, described in <http://www.privacy.gov.au/news/media/04_07.html>, accessed 23 August 2004.

United States of America v Philip Morris Inc (First amended complaint) <http://www.usdoj.gov/civil/ cases/tobacco2/DOJ%20Web%20-%20Amended%20Complaint.pdf>, accessed 23 August 2004.

10.4 Commentary

Bushell S, 'When documents rise from the grave' (2003) *CIO*, 8 August 2003 <http://www.cio.com.au/index.php/id;1439680944;fp;4;fpid;56491>, accessed 23 August 2004.

Lyman P and Varian H, *How Much Information* (School of Information Management and Systems, UC Berkeley: 2003) <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/>, accessed 11 August 2004.


DOCUMENTS
ESS OFFICE?

Notes