GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Data Retention: Corporate Liability and the Complexity of Electronic Records

Alan Lewitton

GSEC Assignment 1.3

Abstract

The complexity of managing an organisation's data has been a recognised issue for some time. Many organisations have a data retention policy however, most have neglected to enforce the policy across all types of records. The dynamics of new technologies, combined with the low cost of electronic storage has brought about a situation where the cost and complexity of enforcing the policy is prohibitive.

The risks associated with data retention and destruction have recently been highlighted in high profile lawsuits. Andersen USA is facing criminal charges for destruction of evidence, while in Australia, British America Tobacco lost a key anti tobacco case because their "destruction of documents" policy effectively denied the plaintiff a fair trial.

Why a Data Retention Policy?

Organisations generate mountains of paperwork and terabytes of electronic data. The sensitivity of this data varies from harmless correspondence to documents that could have a significant impact if obtained by outside parties.

Some of this data has great value to the organisation. It may fulfil a business need, provide an audit trail or prove title to assets. However, a significant portion of this data has no further use.

Storing all this paper and electronic data costs money. Retrieving this data creates a further administrative cost. Therefore, we would save money if we could minimise storage facilities and destroy all records we no longer need.

The challenge is identifying the data that has must be kept from that which is no longer required. There are many factors that influence the value of data, however legal requirements are probably the most important for retention purposes. Legislation dictates the period of time that different types of data must be kept and failure to meet these requirements will expose the organisation to liability. Some organisations may find that there is a fine balance between complying with legal requirements, and retaining data that may prejudice the organisation in legal proceedings. Recent lawsuits have highlighted this dilemma and the consequences of stepping over the line.

Andersen

The collapse of corporate giant Enron raised questions about the conduct of Enron's management and its auditors. Suspecting violations of federal securities

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

law, the Securities and Exchange Commission (SEC) initiated an investigation into Enron in October 2001.

As auditors, Andersen had responsibility for ensuring that Enron's results were fairly stated. On hearing of the imminent SEC investigation, Andersen commenced a process of destroying any "unimportant" documents. [1] Emails circulated the firm, "reminding" audit staff about Andersen's documentation and retention policy. This was inappropriate, as the investigation classified any records relating to Enron as evidence. The firm was served a grand jury indictment for obstruction of justice, referring to "wholesale destruction of documents". [2]

In April 2002 former partner, David Duncan pleaded guilty to obstruction of justice, admitting he tried to thwart an Enron investigation by the SEC. The charge carries up to 10 years in prison and hundreds of thousands of dollars in fines. [3]

At the time of writing, Andersen is still in the process of responding to these charges. However, scores of clients have deserted the firm and the majority of non-US Andersen practices have been sold to other auditing firms. The future of the US firm is uncertain.

Regardless of Andersen's conduct as Enron's auditors, the firm stepped over the line when it destroyed documents that were evidence to a SEC investigation. Any evidence in a criminal or legal proceeding must be produced on instruction. Andersen may have engaged in inappropriate activity as auditors, however the single act that did the most damage to its reputation and integrity was the destruction of evidence.

British America Tobacco (BAT)

In April 2002, Rolah McCabe, a 51 year old Australian woman was awarded AU$700,000 to compensate for her damaged health from smoking. Legal proceedings in this case were cut short when the judge ruled that BAT and its lawyers had destroyed documents "with the deliberate intention of denying a fair trial". [4]

Justice Geoffrey Eames ruled that the company's so-called document retention policy was in fact, a document destruction policy. He emphasised that the process of discovery of documents is "central to the conduct of a fair trial in civil litigation". BAT and its solicitor prevented the process of discovery with the deliberate intention of denying a fair trial to Mrs McCabe.

As a fair trial was not possible, Mrs McCabe did not have to prove the company was negligent. The juror was instructed to decide only on the amount of damages.

Data Retention Requirements

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

These proceedings highlight that an inappropriate data retention policy can expose an organisation to significant liability. To manage this risk, data retention policies should carefully consider legal and regulatory requirements, business requirements, industry standards and process-related future retrieval requirements.

Some examples of legal and regulatory requirements in Australia are listed below (extracted from an OzNetLaw fact sheet on electronic records). [5]

Legislation	Requirement
Proceeds of Crime Act 1987 (Commonwealth)	Financial institutions must retain certain essential financial transaction documents for seven years after a transaction takes place or seven years after the date on which the account is closed.
Financial Transaction Report Act 1988 (Commonwealth)	Financial institutions must report transfers of money greater than AU$10,000, verify the identity of persons opening or becoming signatories to accounts and keep records for seven years after the relevant account is closed.
Income Tax Assessment Act 1936 (Commonwealth)	A person or entity subject to income tax must keep records in a document or electronic form. Records must be kept for five years and be readily accessible and convertible into writing in the English language. Capital Gains tax requires that an entity maintain records to prove when assets were purchased.
Statutory Limitations	Statutory limitation periods outline the time in which an action may be brought against a person or entity. A statutory limitation period is typically six years from the cause of action arising but this may vary in certain cases. The period may only start when the plaintiff becomes aware of suffering some harm, which may be more than six years after a transaction completed. The period may be extended in extenuating circumstances or if the plaintiff is a minor. The Limitations Act in Australia provides that no action is maintainable if it is brought after an expiration period of thirty years. [6]

Statutory limitation requirements are possibly the most difficult to manage. An organisation should consider the nature of its business and the potential liability of its transactions. If transactions stretch over long periods of time, records should be retained until there is some assurance that neither party has come to harm.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

International Record Keeping Standards

ISO 15489-1, *Information and documentation - Records management - Part 1:General* and 15489-2 *Information and documentation - Records management - Part 1:Guidelines* have been published and reproduced in Australia and New Zealand in March 2002.

AS ISO 15489.1 provides guidance on managing records, including responsibilities, policy, procedures, systems and processes. [7] AS ISO 15489.2 is an implementation guide for AS ISO 15489.1. These standards provide a good framework for managing records and should be considered as part of any quality process framework that complies with ISO management systems, ISO 9000 or ISO 14000.

The standards define the regulatory environment to include: [7]

- statute and case law, including regulations governing the sector-specific and general business environment,
- mandatory and voluntary standards of practice,
- voluntary codes of conduct and ethics, and
- community expectations about what is acceptable behaviour.

Preparing the Policy

Each business unit in an organisation should consider requirements specific to the nature of their business. This process may be co-ordinated by a group function, however it is ultimately each business unit that best understands the liability of their business and the types of records that are kept.

The type of records kept should also be considered as this has a significant impact on enforcing the policy. A data retention policy is easier to enforce in a structured, paper based environment. Paper documents are easily identifiable, and enforcement is a matter of appropriate administration procedures. Managing electronic data can be far more complex.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Difference between Paper and Electronic Records

The courts will generally treat electronic records in the same manner as paper records. In fact, electronic records are likely to contain more information than paper records as they also show the date and time of creation, the author and possibly a history of changes. The challenge of electronic records is the volume of records that are kept, the complex nature of the records and the lack of clear ownership, particularly with user managed data.

Electronic storage costs have decreased dramatically and new storage devices are constantly added to expand capacity. It may actually cost more to undertake the process of identifying data for removal than keeping all data. However, the hidden cost of keeping all data should be considered as this exposes the organisation to unnecessary legal liability.

Electronic data can be held within application systems, databases, spreadsheets, documents, emails or many other formats. Data can be stored on an office PC, network server, home PC, personal digital assistants (PDAs) or on backup tapes. There is often no central control over electronic data and the data retention policy must be implemented by its weakest link, the end user.

Studies indicate that a significant portion of electronic data is inactive or duplicate. In an article in Records Management Quarterly, David Stephens quoted that more than 50% of electronic data on a typical network has not been accessed in several months and only 20% of network storage is active data. [8] A separate but similar study noted that 85% of documents filed are never retrieved, while 50% or more are duplicates. [9]

Ownership of Electronic Data

The data retention policy can only be enforced if a manageable structure is imposed on electronic data. Data within specific application systems or databases is generally easier to manage, as the purpose of the record is known and the retention requirements are better understood.

Identifying the retention periods for other electronic data is more difficult. Files stored on PC hard drives or shared network drives typically relate to end user computing and are difficult to manage. The data retention policy can only be enforced if a well defined structure is imposed on these files and end users take responsibility for retention requirements. Training and awareness is possibly the greatest tool in enforcing the policy.

In a 2001 survey, CNI noted that although 49% of organisations have a data retention policy, 41% of users ignore this policy, 36% of users are neutral to the policy and only 23% of users adhere to the policy. [10]

Removing Electronic Data

Deleting an electronic file may not actually remove all traces of the record. Firstly, there may be other versions of the file elsewhere, particularly on backup

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

tapes. Secondly, even after deletion, there may be hidden traces of the file on disk. Deleting a file generally removes the pointer or reference to the file, but the actual data is not removed. To effectively delete a file, the physical space on the disk must be overwritten.

This issue is made worse by sophisticated tools that may recover overwritten data, particularly if a single character has been used to overwrite the data (eg. zero). This is possible because the magnetic memory of disk retains a 'shadow' of deleted data. The US department of defence has established a national security standard for deleting data (5220.22). [11] This standard specifies that data must be overwritten three times. Firstly with zeros, then with ones and finally with random characters between two and nine. This however, does not apply to top secret information, which requires more stringent destruction procedures.

This process of overwriting data may actually alert investigators that data has been intentionally destroyed. A disk that has been systematically overwritten will have a distinct image and while the data may be gone, inference could be gained from the fact that the disk has been 'wiped'. Forensic analysis has developed into a mainstream industry and can be used to document the history of an electronic record (or absence of a record).

Procedures for removing data should also consider the decommissioning of equipment. Many organisations donate old PCs to charity or schools. If this is the case, the best intentions may actually expose the organisation to risk as data could be recovered by outside parties. Procedures should document the process of removing all sensitive data from decommissioned equipment. Probably the most effective method of removing data is to physically destroy the disk drive or storage device. However, this would defeat the purpose of donating the hardware.

Removing all traces of electronic data can involve considerable effort. Each organisation should assess the risk associated with its data and determine the most appropriate procedure to remove data.

© SANS Institute 2000 - 2002, Author retains full rights.

Retention of Email

Email has compounded the problem of the proliferation of electronic data. Once sent, copies of an email may exist on any number of servers between the host and destination. The message itself may be copied, forwarded or archived by the recipient and sender may also retain copies in an email database, folder or archive. The message and its copies will probably be backed up on tape and kept long after the original was forgotten. Synchronisation between desktops, laptops, home computers and PDAs may further distribute the message.

Email records may also be more harmful to the organisation as people tend to be more conversational in email, disclosing information that they would not include in a paper record. Damaging email records have come back to haunt many executives, most notably Bill Gates in the Microsoft antitrust suit. Commenting on the impact of email evidence in this case, Joan Feldman, President and founder of Computer Forensics in Seattle likened the proliferation of email to the breeding habits of rabbits "Think about their (rabbits) incredible reproductive nature, and think about trying to get them all back. That's the challenge for people trying to get rid of email". [12]

A CNI 2001 survey identified that although a significant portion of business critical information is stored within email systems, 81% of respondents indicated that end users were unable to retrieve backed up or archived email without the assistance of IT. The survey highlighted the complexity of email archiving and that current practices do not address the requirements of email retention. [13]

Proposed solutions for email archiving and retention involve centralised storage and retrieval systems that capture all incoming and outgoing messages. Local message stores only contain current messages and are purged when messages are moved to secondary storage. Under this arrangement, users manage their message stores and centralised storage facilitates a coordinated backup and retrieval process.

The Discovery Process

The cost of discovery is becoming more of a burden, particularly with email. An organisation can be called on to produce all emails sent and received relating to an investigation. This could involve extensive costs, requiring backup restores, searching through emails and preparation of evidence to hand to investigators. Central backup and retrieval processes may reduce costs however, in some cases it may be cheaper to settle a dispute, rather than incur discovery costs.

As previously discussed, destroying records once legal proceedings have begun can lead to serious penalties. In criminal proceedings, charges of destruction of evidence can be raised or in civil proceedings, a jury can be instructed to assume that missing documents existed and are harmful to your case. Removing electronic data must always be performed subject to the guidelines outlined in the data retention policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security Considerations

Security mechanisms used to protect electronic records should also be considered when identifying retention requirements. Procedures used to encrypt or otherwise secure data should be retained, as records will be lost if the 'key' is no longer available. Security protection measures cannot be used as a defence if called on to produce evidence. Your position is the same as if paper records were physically locked in a safe.

Off-site Storage Facilities

Many organisations use off-site storage facilities, primarily for paper records. Arrangements with off-site storage facilities should relate closely to the data retention policy to ensure that the policy is enforceable. Archived records should be clearly marked to indicate destruction periods. The organisation must satisfy itself that the off-site storage facility has effective inventory processes and is regularly complying with any destruction requirements.

Conclusion

Many organisations already have a data retention policy. As with any policy, this should be regularly reviewed to ensure that it is in line with current thinking and that all requirements are addressed. The data retention program as a whole will only be effective if it is enforced across all types of records. If any type of record or technology is excluded from the program, objectives will not be achieved.

Probably the most significant retention issue at this time is enforcing the policy on email. Failure to address this issue has a significant impact, particularly considering the nature of email and its potentially damaging content. However, we can be assured that new technologies will continue to add to the complexity of data retention efforts.

I would like to think that most organisations act as responsible corporate citizens. A data retention program should ensure that the organisation accepts responsibility for its actions, but should limit responsibility to the extent required by the codes imposed by society (in the form of regulations and ethics). An organisation acting responsibly should not need to disregard these codes by destroying records at all costs. These records should prove it acted with honesty and integrity.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

[1] *Lawyer who wrote document memo quizzed.* CNN.com. January 21, 2002 http://www.cnn.com/2002/LAW/01/21/enron.temple.duncan/

[2] *Grand Jury Indictment. United States District Court, Southern District of Texas, USA against Andersen LLP*. Reproduced by FindLaw. http://news.findlaw.com/hdocs/docs/enron/usandersen030702ind.pdf

[3] *Andersen Auditor Cuts Plea Deal*. The Associated Press. April 9, 2002. http://www.cbsnews.com/stories/2002/04/05/national/main505473.shtml

[4] *Lawyers ways, and fairer trials.* Sydney Morning Herald. April 13, 2002. http://www.smh.com.au/articles/2002/04/12/1018333417181.html

[5] *Fact Sheet - OzNetLaw : Keeping Electronic Records.* http://www.oznetlaw.net.au/facts.asp?action=content&categoryid=228

[6] Mark Allen. e-Business, the law and you: a guide for Australian business. Pearson Education Australia, 2002. Page 28.

[7] Standards Australia International Ltd. *AS ISO 15489.1-2002: Records management Part 1: General.* Published March 13, 2002.

[8] David Stephens. *Megatrends in Records Management.* Records Management Quarterly. Reproduced at *Fios, Inc.: Digital Information: Statistics and Relevant Facts*. http://www.fiosinc.com/digital_info_stats.html

[9] Tony McKinley. *Managing All Information Assets.* Document Management. Reproduced at Fios, Inc*.: Digital Information: Statistics and Relevant Facts.* http://www.fiosinc.com/digital_info_stats.html

[10] *Executive Summary of CNI Email Data Management Survey Sponsored by OTG Software*. Reproduced by OTG Software. 2001. http://www.otg.com/media/CNI_summary2001.htm

[11] Department of Defence. *National Industrial Security Program Operating Manual. Chapter 8, Clearing and Sanitization Matrix.* http://www.dss.mil/isec/nispom.htm

[12] Paul Festa and Lisa Bowman. *PC sleuths search for Enron's shredded secrets.* ZDNet News. February 5, 2002. http://news.zdnet.co.uk/story/0,,t269-s2103739,00.html

[13] *Executive Summary of CNI Email Data Management Survey Sponsored by OTG Software*. Reproduced by OTG Software. 2001. http://www.otg.com/media/CNI_summary2001.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event