Global Information Assurance Certification Paper

Data Retention Policies: Smart Business Practice

Katharine Hindes

March 11, 2002

GSEC Practical, Version 1.3

Abstract

Electronic evidence is quickly becoming a central point of focus for discovery in U.S. courts and is creating considerable problems for many corporations. Many corporations are preparing themselves for the possibility of discovery during litigation by developing a data retention policy. A policy that is well thought out and properly executed will enable companies to retrieve and evaluate possible electronic evidence in a more organized and efficient manner, possibly avoiding the loss of hundreds of thousands of dollars in legal discovery fees. To define an effective policy, companies should consult resources from several internal departments to determine what data and media should be covered and how it will be enforced.

Introduction

Most of the media coverage regarding the recent Enron fiasco has focused its attention on the "paper evidence" that was destroyed by shredding machines at Arthur Andersen. But, despite Andersen's alleged efforts to destroy certain documentation, much of that "paper evidence" can be found on personal computers, servers, laptops and backup tapes. Even if employees at Enron and Arthur Andersen allegedly took steps to delete incriminating evidence, federal marshals and computer forensic experts should be able to retrieve documents, emails and other data.

Electronic evidence is quickly becoming a central point of focus for evidence gathering, or discovery in U.S. courts. This trend is creating enormous problems for many corporations, since in most civil cases the defendant must bear the discovery costs. The increased use of personal computers and sophisticated backup systems in recent years have driven up the cost of discovery so much, that some corporations will simply settle out of court rather than pay the high costs. A corporation may also choose to settle to avoid the possibility of other "smoking guns" being found in the discovery process.

Many corporations are preparing themselves for the possibility of discovery during litigation by developing a data retention policy. A data retention policy is a set of documents that identifies different types of data and defines how long the data should be kept, how it should be stored, and how it should be destroyed when it's retention time has expired. A data retention policy that is well thought out and properly executed will enable corporations to retrieve and evaluate possible electronic evidence in a more organized and efficient manner. Furthermore, many corporations recognize that having a data retention policy in place before they are faced with the pressure of litigation is a much better option than formulating one after it's too late.

Hypothetical case and potential outcomes

A woman recently lost her job because her position was eliminated. The woman feels that she was wrongfully terminated because she held several different positions during her

tenure at the company and always received stellar performance reviews. The woman suspects she was let go because she had complained to her manager that several co-workers had offensive images on their computer screens. She also learns that three other people had been terminated during the past year after complaining about the distasteful images on their co-workers' computer screens. The woman hires an attorney, who, after hearing her story, decides to sue the company for wrongful termination and for fostering a hostile work environment. During the process of evidence gathering, the attorney asks the company (defendant) to provide him with the following:

- All email generated during the past year that has any sort of content in which the plaintiff was discussed.
- All email generated during the past 18 months that has any sort of content relating to the three other former employees who had complained about inappropriate images on computer screens.
- All email generated during the past two years regarding acceptable computer use policy.
- All email generated during the past two years that has any content regarding disciplinary action for unacceptable computer use.
- Copies (and all revisions) of Acceptable Computer Use Policy
- Hard copies of plaintiff's performance reviews for the entire duration of plaintiff's employment.

Because the defendant must produce this evidence or face a court order, all servers and backup tapes must be searched for this information.

Most system administrators do not have the time or resources to produce this information efficiently and reliably, so the majority of corporations will need to hire a third party with expertise in electronic records retrieval.

This service does not come cheap. The hard disks of servers, personal computers and laptops must be searched. A server environment must be built so that all backup tapes that the company keeps may be restored. All passwords must be overwritten so that the data may be reviewed and retrieved. If the data is encrypted, it must be decrypted. It is not uncommon for discovery fees to fall in the six-figure range; this means having to pay out hundreds of thousands of dollars before the company even steps in front of a jury.

Outcome A

XYZ Corporation does not have a data retention policy and keeps one month worth of backup tapes.

XYZ Corporation produced hard copies of its computer acceptable use policy and hired a computer forensics expert to retrieve the email it had on its servers and backup tapes. The experts also searched hard drives of the manager of the terminated employees and Human Resources department for any email relating to the terminated employees. They were unable to retrieve email going back the full two years that the plaintiff had requested because they only keep one month's worth of email backups before tapes are overwritten.

The jury found the defendant guilty of wrongful termination and fostering a hostile work environment and awarded the plaintiff $150,000, plus legal fees. Since XYZ was unable to produce all of the requested documentation, and they also did not have a data retention policy in place, the plaintiff's attorney was entitled to a "jury instruction," under the "Spoliation of Evidence" doctrine. This means that the court is stating that in this case, since the email evidence that the plaintiff sought was destroyed either intentionally or negligently by the defendant, the jury was allowed to draw it's own conclusion on whether the destroyed evidence was potentially harmful to the defendant in this case. The jury referred to Telectron, Inc v. Overhead Door Corp., 116 F.R.D. 107, 123 (S.D. Fla. 1987) "The absence of a coherent document retention policy during the pendency of this lawsuit was cited as leading to a possibly damaging document destruction occurring in both routine and non-routine manners."

Outcome B

XYZ Corporation does not have a data retention policy and has two years worth of backup tapes.

XYZ Corp opted to settle out of court for $50,000. Because XYZ had no data retention policy and, at the time of the discovery request, they had 2 years worth of email backups available, the discovery costs to go through 2 years worth of backups would be so high, that they took the advice of their attorney and decided it would be less expensive to settle out of court.

Outcome C

XYZ Corporation has had a data retention policy in place for several years. Email backup tapes are kept on a two-week rotation schedule.

XYZ Corp has had a data retention policy in place for several years that sets reasonable storage limits for all types of documents, including email and is reviewed yearly. The data retention policy states that email backups will be kept for two weeks prior to being overwritten. Emails that are older than ninety days will be automatically purged from the system. Emails deemed as "official business" will be archived and stored for a pre-determined length of time, depending on the content of the email. The contents of personnel files are stored for five years. XYZ was able to produce the documents the plaintiffs requested, except for the email since they only keep backups for two weeks. The court found in favor of XYZ Company because there was no evidence that XYZ

fostered a hostile work environment or wrongfully terminated the plaintiff. Because they had a reasonable data retention policy in place, the court referred to Willard v. Catapillar, Inc., 40 Cal. App. 4th 892, 921, 48 Cal. Rptr. 2d 607, 625 (1995) "Good faith disposal pursuant to a bona fide consistent and reasonable document retention policy could justify a failure to produce documents in discovery." Furthermore, XYZ may be able to recoup their discovery costs and legal fees from the plaintiff.

The above scenarios are fictitious, but they are not exactly out in left field, either. Decisions will vary from courthouse to courthouse and from jury to jury. In just about every situation, a corporation would benefit from having a data retention policy that is properly implemented.

Benefits of a well-written data retention policy

- Reduced litigation expenses – electronic discovery is expensive, and the less useless data to sift through, the better.

- More effective communication with corporate counsel – having document storage information in writing makes it easier to focus on the issue at hand, rather than trying to locate or reproduce lost documents.

- Identification of weaknesses – while creating your policy, you may find system vulnerabilities that need to be addressed.

- Better business practice – A good data retention policy will allow your documents to be organized so that they may be quickly produced if needed. At the same time you are also ridding your organization of any unnecessary documents.

- Reduced risk of theft of proprietary information – having intellectual property stored in a secure place, away from everyday production systems can prevent "unfriendly" access to your corporation's trade secrets.

Creating a data retention policy

Clearly the cost of not having a data retention policy in place is significant, particularly when one considers the cost of creating one. For starters, the company should form a policy committee. The committee should, at the very least, include members from the legal, IT, financial and human resources departments. Other members that could also be included would be from research and development, engineering and anyone who deals with any regulatory agencies your company may be affiliated with.

For the policy to be effective, it must be enforced. It must be determined who is responsible for enforcement. Make sure the IT department is involved in the decisions regarding policy enforcement so that any conflicts with existing systems policies may be addressed and resolved before implementing the data retention policy. While a high level executive may be accountable for enforcing the data retention policy, it is crucial that key

IT personnel be informed of the importance of the policy. Most systems administrators have been trained and conditioned to keep the systems from losing any data in the event of a disaster and may not know the implications of keeping data for too long.

It is also a good idea to know in advance who will be called to testify about the corporation's data retention procedures, and educate that person before litigation occurs.

A list of document types must be formulated, and then the following questions need to be addressed for each document type to determine how long a document should be kept, or even if it is to be kept at all:

- What is the legal reason for keeping this document? Federal, state and local governments, as well as some regulatory agencies require reporting on certain issues, such as health and safety, wages, hazardous materials, and product test data.

- After the document is used for its intended purpose, could it be used for another purpose? Maybe the document could be used to support a tax deduction or a business decision down the road.

- What are the consequences if the document is destroyed? If needed, can the document be reliably reproduced? Can you get the needed information from company files or databases? Does someone else have a copy of the document?

The committee should also determine what media and data should be governed by the policy. Those that should be considered are:

Email - Electronic mail presents its own set of unique problems. It is commonly used as evidence in litigation, and most attorneys believe that email is a gold mine. It is common for email to be used in place of actual telephone or face-to-face conversations. It is often used for non-business communications and email messages seem to have taken the place of office "water cooler conversations." Email communications may also be taken out of context and used the wrong way. Once the "send" button is hit, the sender basically has no control how that email will be disseminated. It could be edited, printed, or forwarded around the globe. Many users horde emails thinking they "might need it later." End users are also mistaken in thinking that when an email is deleted, that it is really gone. The email may just be sitting in the "trash" bin waiting for easy recovery. Even if the contents of the "trash" bin are purged, the email will sit on a hard drive or backup tape until it is overwritten. For professionals skilled in electronic recovery, producing deleted emails is not too difficult a task.

There are varying opinions on how long different types of documents should be retained, but when it comes to email, most experts agree there is no good reason to save email. Many companies purge all mail on servers that has reached a certain age, usually sixty to ninety days old. Something else to consider would be to designate email as either "official" or "non-official." All mail deemed as "official" should be considered an

official business record and meet certain criteria. "Official" email will have a longer retention period than "non-official" email and will be archived separately from "non-official" mail. Email backups are used primarily for recovery after a system crash, therefore only the most current backup tapes are needed. It is recommended the email backup tapes be kept on a two-week rotation; this schedule can be altered to fit your company needs and comfort level.

The importance of end user education cannot be stressed enough, specifically: defining email etiquette. No data retention policy will save you if unprofessional and offensive email communication is rampant throughout your organization. Make your users aware that anything written in email is generally not private. Remind them that their emails may be forwarded or printed without their knowledge. Let users know that the written word can be taken the wrong way and that some things are better discussed face-to-face. Stress that email is to be used for professional, business communication. A good rule of thumb is that "If you or your company would be embarrassed to see what you wrote on the Internet somewhere, then don't say it in email."

One last thing to consider when developing an email retention policy is email communication with corporate counsel. Attorney-client privilege may be compromised if any email communication with corporate counsel is forwarded to another party because the recipient wasn't aware that this was privileged information . Corporate counsel should clearly state on any email communications "CONFIDENTIAL ATTORNEY-CLIENT PRIVILEGED COMMUNICATION."

Corporate counsel should also notify recipients that these communications are "NOT TO BE FORWARDED WITHOUT PERMISSION OF COUNSEL."

General Correspondence -Letters, memos and other general correspondence have a way of cluttering file servers. Knowing what to keep and what to get rid of will help to reduce some of the mess. Letters and memos which require no acknowledgment and form letters that require no follow-up should be destroyed fairly quickly. Letters requesting a specific action should be destroyed after the requested action is completed. Some companies will keep a letter relating to establishing credit for five years, while another company may keep the same letter for one year. The bottom line is - different types of letters will be retained for varying periods depending on company requirements.

Voice Mail/Voice Messaging- Like email; the general consensus is that there is no benefit to saving voice mail backup tapes longer than a week or so. Voice mail backups are used primarily in the event of a system failure, therefore only the most current information is needed.

Web Pages -Depending on the purpose and content of your corporation's web page, it is generally recommended that each major revision be saved in case there is some sort of dispute regarding its content in the future. The retention period will vary from company to company.

Accounting and Financial Records -Generally, the retention period for general ledgers, bank statements, checking account records, checking account statements and cancelled checks should be kept for twenty years offsite. Projections, forecasts and planning reports should be kept for ten years. All balance sheets and other financial statements should be kept permanently.

Tax Related Items -The company should keep sufficient records to compute its earnings and profits permanently. Therefore, tax statements, depreciation schedules, tax returns, state income and property records should be retained permanently. Sales and use tax records, unemployment tax records and excise tax records should be retained until the statute of limitations has expired. Statute of limitations will vary from state to state.

Sales Records -Sales records should be retained for the length of the sale plus the limitations period in all states the company does business in, unless the records can be reproduced in some other way. The limitation period will vary from state to state. A copy of each version of sales circulars, literature and other materials should also be saved, along with the dates that each version was used in case there is a dispute in the future. Sales materials that resulted in a sale may be used as evidence of promises made during the sale. Market research and projections reports may be kept for historical comparison. Save these types of documents for as long as the company would like to track sales history.

Quality Control and Inspection records -It is important to keep inspection records because these documents may help support the company's position in litigation. If the company is affiliated with a regulatory agency, these documents may be required in an audit or for reporting purposes. Documents such as material substitution records, inspection and test records, equipment calibration records and supplier quality data should be kept for fifteen years. At the very least, these documents should be retained in compliance with any regulatory agency requirements.

Personnel Records/Employment Manuals -Most employee records should be kept for the duration of the employee's tenure with the company, plus the limitations period. You will need to check your own state's laws for the statute of limitations in your state. There are some documents that may be retained for a shorter period of time. Employment applications for non-employees may be kept for three months to one year; general attendance records, timesheets or timecards should be retained for approximately three years. Affirmative action programs should be kept for one or two years after they have been superceded. Job descriptions should only be kept for two years, depending how often they are revised. Some documents need to be retained for a longer period of time. Safety and injury frequency reports should be kept for ten years. Individual employment contracts, employee insurance records and fidelity bonds should be kept for ten years after termination. Employee's personnel records, including application forms, individual attendance records, performance evaluations, termination papers, exit interview records, withholding information and garnishments should be retained for six years after termination. A copy of each revision of employment and training manuals

should be retained with the dates that version was in use. In the event of litigation, the timing or reason for the change may be important.

Safety Documents -The company must keep all documents regarding employee injuries and safety to demonstrate compliance with regulations and standards that are constantly changing. The following documents should be for thirty years after termination: occupational injury records, OSHA annual summary forms, employee exposure and medical records, and asbestos records. Material safety data sheets should be kept until revised, and previous versions should be kept with the date they were used.

Environmental Records -Environmental records are usually retained in compliance with state and federal laws. Some of the documents to be considered are hazardous waste manifests, treatment, storage and disposal facility inspection records and monitoring reports. Again, retention of this type of documentation is usually government regulated, so these will vary from state to state.

Records relating to inventions/intelligence - It is important to retain documents relating to trade secrets as long as possible since trademarks, patents, and copyrights can be challenged at any time. It is recommended that original patents, trademarks, royalty records, copyright permissions and registrations, confidentiality and non-disclosure agreements, trade secret documents and documentation related to security measures taken to protect trade secrets are retained permanently. Because information relating to intelligence is usually extremely confidential, it is important that this type of documentation is stored in a secure location.

The above list of documents is by no means a complete listing of all possible records that should be included in a data retention policy, as many other areas must be considered. Other areas may include contracts, customer credit information, property records, office supplies, service and manufacturing records. Each company is different and will have different types of documents and different levels of retention needs. The laws vary from state to state and it is crucial that corporate counsel, or a third party who is familiar with these laws be involved when creating the company's data retention policy.

Conclusion

In order for the policy to be successful, it must have the backing of senior level staff. All employees must be educated in the importance of the policy and how it pertains to them. The policy should be reviewed and if needed, revised annually.

If the company is involved in litigation or suspects it will be in the near future, certain areas of the policy will need to be revised, and records critical to the case should not be destroyed under any circumstances. Employees should be instructed not to destroy critical data that is pertinent to the case. All data related to the litigation should be kept until the case has been resolved and all appeals have been exhausted.

Implementing a data retention policy is a good idea and smart business practice. It takes a lot of time, thought and hard work from people in all areas of the corporation. Actually taking the time to think about what to save and what to delete according to policy requires even more diligence throughout all levels of the organization, but it can be done, and the rewards are often worth the trouble.

Last but not least, as important as data retention polices are, they are not a substitute for ethical business practices. The corporation must operate at the highest ethical standard possible. A data retention policy is not an alternative to educating the company's employees about professional communications. A data retention policy is only a set of documents that contains a consistent, methodical approach to the retention and destruction of electronic documents, and by having one; the corporation will fare well in the eyes of most courts.

References

1. Festa, Paul and Lisa M. Bowman "Can PC Sleuths Undo Enron Shredding?" *ZDNet News,* Feb 4, 2002. URL: http://zdnet.com.com/2100-11-829071.html (Feb 13, 2002)

2. Surmacz, Jon. "Five Thoughts About…Record Keeping at Enron." *Darwin Magazine.* Jan 30, 2002. URL: http://www.darwinmag.com/read/thoughts/column.html?ArticleID=243 (Feb 13, 2002)

3. DiSabatino, Jennifer. "Enron Bankruptcy Case Highlights E-Mail's Lasting Trail." *Computerworld*. Jan 21, 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO67583,00.html (Feb 13, 2002)

4. Springsteel, Ian. "Are You Sure You Want to Save That?." *CIO Magazine*. Sept 15, 2001. URL: http://www.cio.com/archive/091501/save.html (Feb 14, 2002)

5. Rosenberg, Geanne. "Electronic Discovery Proves Effective Legal Weapon." *The New York Times*. Mar 31, 1997. URL: http://telecom.canisius.edu/cf/electronic_discovery.htm (Feb 9, 2002)

6. Llewellyn, Virginia. "Document Retention and Destruction Policies for Digital Data What You Don't Know Can Hurt You." *Applied Discovery White Papers*. URL: http://www.applieddiscovery.com/lawlibrary/whitePapers_DocumentRetention.stm (Feb 18, 2002)

7. Gall, Barbara Weil. "Document Retention Policies: Legal Reasons to Keep E-mail, Web Pages and Other Records." URL: http://www.gigalaw.com/articles/gall-2000-09-p1.html (Feb 9, 2002)

8. Ballon, Ian C. "How Companies Can Reduce the Costs Associated With Electronic Discovery." *Glasser Legal Works*. 1999. URL: http://smallbiz.biz.findlaw.com/library/lg_internet/articles/glass000014.html (Feb 9, 2002)

9. Unknown. "Data Retention Policies." *Electronic Evidence Recovery, Inc*. 2000. URL: http://www.cyberdetective.com/dataret.htm (Feb 9, 2002)

10. Flynn, Nancy. *"The ePolicy Handbook: Designing and Implementing Effective E-mail, Internet, and Software Polices."* New York: AMA Publications, 2000.

Last Updated: July 28th, 2017

Upcoming Training

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
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS