Global Information Assurance Certification Paper

Electronic Data Retention Policy
Brian Wrozek
August 15, 2001
SANS GIAC - GSEC Security Essentials (version 1.2e)

Could this happen to you?

Imagine this scenario. During a routine staff meeting, a coworker from the legal department alerts your team to the fact that a sexual harassment case has recently been filed against an employee. Since both the plaintiff and the defendant use electronic systems that you administer, your assistance is required. Therefore, they need all the electronic documents owned or edited by the employees regardless of where that data may be stored. They need everything from the previous twelve months. This includes all forms of electronic information including email messages sent and received. Backup tapes must be checked as well. Since this is an active case, you can no longer delete any electronic information that could potentially be relevant to this case since it may be requested for evidence as well. Consequently, you may no longer be able to recycle backup tapes or clean up disk space until the case is over. Failure to preserve potential evidence could result in sanctions.

Does this sound impossible in your environment? Even an honest effort could take days, possibly weeks, wreaking havoc on your daily routine and workload.

Why you need an electronic data retention policy

Data retention policies are useful documents that deal with the issue of maintaining information in your possession for a pre-determined length of time. Different types of data require different lengths of retention. In addition to describing how long various types of information must be maintained in your possession, retention policies usually describe the procedures for archiving the information, guidelines for destroying the information when the time limit has been exceeded and special mechanisms for handling the information when under litigation.

The fundamental reasons and overall purpose of having a data retention policy have not changed over the years but the electronic age has brought new twists to this old problem. Computer systems and applications have added increased complexity to the issue. Most notably, electronic email messaging has had a large impact on those who develop and enforce data retention procedures. Electronic data, just like hard copy data from years past, still needs to be retained for certain time periods based on one of three following criteria:

1) Legal requirements
2) Business requirements
3) Personal requirements

Likewise, all information pertinent to a lawsuit must be retrieved and turned over to the authorities during litigation cases regardless of the medium such as paper, hard disk or tape. In fact, it will be shown that litigation and criminal investigations are critical forces that shape any data retention policy.

Challenges of electronic information

Computer systems can store tremendous amounts of data. Storage media continues to decrease in cost while increasing in density. Users no longer have to deal with the mounds of hard copies or overflowing file cabinets. In many cases, the data is stored on huge, remote file servers so the local hard drive size is not a limiting factor.

It is all too easy to instinctively click "save" to store electronic documents. The diversity of applications in use promotes the storing of the same information in different formats in multiple locations. The same Word document stored in a user's home directory on their laptop could be found in a folder as a message attachment on a mail server. It could be posted on a group web server in html format and replicated on a mirrored partition in the data center. Another may have it in hard copy format to present at a meeting. Finally, it is likely to be saved on a nightly backup tape, which could be stored at an offsite facility. Do not forget about the hidden or often overlooked data. Users may not even be aware of some of the data stored on their computers such as cookies or cached data.

There are hundreds of different applications to support a wide selection of electronic hardware. It is not sufficient to simply retain just the data itself. As new software revisions are released and hardware upgrades performed, care must be taken to ensure the new solutions can still read legacy data. If not, data may need to be converted to new formats adding to the overall retention expense.

If that is not enough, even more issues arise if any of this information happens to be encrypted. Key management must be addressed so the data can be decrypted before turning it over to the authorities. Retaining data that can no longer be decrypted is useless.

Additional challenges posed by electronic email messages

The informal nature of email communication poses additional challenges for electronic data retention. Many people write email messages as if they are speaking directly to an individual. Email messages are rarely proofread or edited for content. The electronic thread of email messages and their "off the cuff" content can be a source of damaging evidence. Here is concrete, written proof instead of “hear-say” evidence. A large part of the popularity of email messages is how quickly the information is delivered to the target. Once sent, the composer has no control over the subsequent use the email message. Likewise, the composer cannot prevent further dissemination of the message once it has been sent. Email can be stored on remote servers or forwarded to any number of people. Therefore, deleting an email message from your system does not ensure that all traces of that message have been erased.

Since email use is so pervasive in our daily routines, the application is often used as a mechanism for storing and organizing information adding to the challenge. Email messages containing budget analysis or contractual forms as attachments are saved alongside messages containing inappropriate jokes and questions about where to go to lunch the next day. Most users do not have the time or desire to sort through thousands of email messages to save only those most

critical to the business or required by law. Consequently, everything gets saved indefinitely by adhering to a "just in case it is needed later" mentality.

Legal requirements

The United States government has a number of requirements for retaining various types of records. In the state of Texas for example, disability and sick benefit records must be retained for 6 years and claims of employee inventions must be retained for 25 years. Depending on the nature of your business, there may be other agencies that have their own special requirements. For instance, OSHA requires that certain industrial hygiene records and medical records be retained for 30 years. Information pertaining to the Department of Defense has additional rules that must be strictly followed. Remember that you must examine requirements at the local, state, federal and possibly the international level. The Internet knows no boundaries. Therefore, attention must be paid to regulations outside the resident state and country.

Law enforcement is driving legislation to establish and in some cases increase the data retention responsibility of system administrators, network operators and service providers. Their intention is to preserve and protect data that could potentially be used as evidence to prove innocence or guilt. Another reason is to allow the gathering of intelligence information to track terrorists and organized crime. In one instance, a proposal to the European Commission wanted to require Internet traffic, mainly email messages and usage logs, to be retained and made available for seven years.

Electronic evidence changes the nature of police work. Physical evidence and eyewitness accounts may not be possible when investigating Internet crime. The only evidence available in some cases is the electronic data stored in log files. Log files can help build the date and time sequence of events. Communication data can be useful in establishing the location of suspects. Keep in mind that evidence can also be used to establish a person's innocence. Data retention can be key to ensuring a fair trail for those investigations that span long time periods. Without the ability to retrieve information, the prosecution or defense may not be able to cross-examine facts or corroborate statements. To the government, it is a matter of national security and ensuring a fair trail.

When involved in litigation, the law requires all data pertinent to the case or anything likely to lead to the discovery of admissible evidence to be retained and provided to the lawyers upon request in a timely manner. Otherwise, potential evidence could be destroyed either intentionally or accidentally.

If the litigation is a civil case, a company could be accused of spoliation if potential evidence has been destroyed either intentionally or through negligence. The dictionary definition of spoliation can be misleading in this sense of the word. The Texas Supreme Court, for example, has not officially defined the term but it generally refers to spoliation as the "intentional, reckless, or negligent destruction, loss, material alteration or obstruction of evidence that is relevant to litigation". (Commer) Be aware that different jurisdictions can apply their own working definition to the term, spoliation.

A judge can allow the jury to draw an adverse inference when it has been determined that spoliation of evidence has occurred. This means that the jury can infer whatever they like from the situation. This gives the lawyer the opportunity to present a case where the data was deleted intentionally to cover up the evidence that could have proved the client's guilt or innocence. The data may have been deleted for legitimate business reasons but it is up to the jury to draw their own conclusions. Usually, penalties are assessed only if it is determined that the parties did not act in good faith to preserve or retrieve the information, however, what constitutes good faith is open to debate. Likewise, judgments and penalties differ from jurisdiction to jurisdiction.

If the litigation is a criminal trial then a company could be accused of obstruction of justice, which carries severe penalties.

Litigation requests come in a variety of forms depending on the jurisdiction where the lawsuit is pending. Likewise, discovery requests vary from jurisdiction to jurisdiction. It doesn't help that the law is years behind technology so the rules are still being established.

Business requirements

In addition to legal requirements, businesses may have their own data retention requirements that can range from contractual obligations with customers or suppliers to administrative or operational information such as policies and procedures that define daily functions. Each business must set their own data retention requirements to sufficiently maintain their business operations.

Given the complexity of all the legal requirements regarding data retention, should administrators simply keep everything forever and play it safe? The obvious problems with this philosophy are the expense of storing all data indefinitely and the potential difficulty in retrieving it when necessary.

Lawyers can employ a technique commonly known as burying the opposition in paperwork during the discovery order phase. This ploy is much easier when years of electronic data are available. Companies could literally spend hundreds of thousands of dollars retrieving all the electronic data related to a case. Add the cost of reviewing that information to ensure only the relevant information is made available to the opposition further increases the costs. In these situations, it could be cheaper to simply settle the case out of court.

Retaining too much information can often lead to the "smoking gun" piece of evidence. By now, everyone is familiar with the trouble Bill Gates encountered when old email messages surfaced during the Microsoft trial. Nobody is advocating the destruction of potential evidence, but why risk old, information being used out of context when it would have been easier to delete it in the first place avoiding any future complications? One could draw the conclusion that the individual thought that the information was important enough to keep so it must be relevant and crucial.

Does this mean administrators should simply delete everything as quickly as possible? If only it

were that simple. Day to day business activities often dictate the length of time information needs to remain accessible. Plus, there are many laws governing how long certain information must be retained as we have already discussed. A host of information ranging from financial records to employee health records has set time limits for retention that must be followed. Keep in mind that retained data can also be used establish proof of innocence and validate claims of intellectual property in the event of a patent dispute for example.

The Massachusetts Superior Court memorandum "1999 WL 462015" illustrates what can happen during responses to discovery requests. The defendant in this case was required to produce any email message sent or received by fifteen named individuals during an agreed upon time interval that contained references to a specific list of keywords related to the case. This included not only electronic email messages but also any documents in hard copy format as well as any that could be retrieved from backup tapes. Upon examination, over 500 backup tapes spanning two different software solutions had to be reviewed. Cost estimates for this discovery activity ranged from $500,000 to $1,000,000 that the defendant ultimately had to bear. The judge ruled that the costs associated with the restoring and producing the information was one of the risks companies take when choosing technological solutions.

Another aspect of this case shows the danger of not following the rules. The defendant in this case routinely recycled backup tapes but they failed to halt this practice during a subset of the litigation period. The plaintiff requested a fine upwards of one million dollars because those backup tapes could have contained information relevant to the case and the defendants were under court order to retain potential evidence. The judge, however, ruled that the imposition of sanctions was not an appropriate response to the violation of the discovery order. The court did rule that the jury could draw an adverse inference because the defendant destroyed documents. As a result, the jury could infer that the defendant destroyed potentially relevant evidence since it would have been damaging to their case. The outcome of this decision could have been quite different in another jurisdiction.

The above example shows how data retention issues can impact the bottom line of your business. For most companies, it is a matter of business value or to put more simply, money. Absent legal requirements, companies will not retain data unless they can realize a measurable return on that investment or a substantial reduction is risk. Companies have their own motivations and corporate cultures when it comes to balancing data retention concerns with business initiatives.

One final thought on data retention from the business viewpoint. Don't forget to recognize and save data that could serve as a historical archive of the company.

Personal requirements

Finally, personal data covers all the other information that does not have business specific retention periods nor retention periods dictated by law. Again, the goal is to keep the "good" information and delete the "unnecessary" information. Under no circumstances should information be deleted just because you think it might hurt the company if discovered at a later date. Stick to the policy. A balance must be struck between reasonable expectations of privacy

and the need to protect companies and individuals from unlawful acts such as fraud and threats to their personal well being. To the individual citizen, it is a matter of personal privacy.

International companies also need to understand that some countries are very reluctant to institute any data retention requirements over concerns of misuse by a government with a history of tracking and persecuting individual liberty.

Data retention policy template

First and foremost, your company should have a written policy devoted to data retention. If your company already has a data retention policy, then a review is in order to ensure it measures up to the new challenges posed by use of computers and electronic mail systems. If your company does not have a written policy, here are some guidelines to help with getting started.

Recommended sections of the data retention policy should include:
A) Purpose of the policy
B) Who is effected by this policy
C) What type of data and electronic systems are covered by this policy
D) Define key terms especially legal and technical terminology
E) Describe the requirements in detail from the legal, business and personal perspective
F) Outline the procedures for ensuring data is properly retained
G) Outline the procedures for ensuring data is properly destroyed
H) Clearly document the litigation exception process and how to respond to discovery requests
I) List the responsibilities of those involved in data retention activities
J) Build a table showing the information type and it corresponding retention period
K) Document the specific duties of a central/corporate data retention team if one exists
L) Appendix for additional reference information

Since the information that must be retained typically involves data of a sensitive or proprietary nature, caution must be exercised in securing that data at all times.

Conclusion

While all this may seem daunting and practically impossible to implement, it can be done. It takes the cooperation of many departments: Legal, Human Resources, IT, and Management to name a few. It is also the responsibility of all employees to do their best at complying with the data retention policy. The important thing is understanding what absolutely must be saved and then making a good faith effort to follow your defined process to the best of your ability. Don't forget to exercise caution during litigation and try to plan ahead for how you would respond to discovery requests.

Data retention is a complicated balancing act. On one extreme is the philosophy that promotes aggressive destruction of electronic data after a short time period. On the other extreme is the philosophy that promotes the saving of everything indefinitely. There is no absolute right or wrong answer when establishing a data retention policy. On one hand you need to save

information required by law and vital to your business. On the other hand, you should delete irrelevant, outdated and nonproductive data as quickly as possible. Finally, you need to plan ahead for potential discovery requests in connection with litigation cases. Again, let the content of the document be the driving factor for defining the retention period not the actual format and be prepared to modify the electronic environment and daily procedures to make the overall process more effective.

References

1) Commer, Jason S. "Spoliation of Evidence: A Survey of Texas Law." Texas Trial Lawyers Association 9th Medical Malpractice Conference. Sep 17-18, 1998. URL: http://www.texaslawyers.com/coomer/Paperspo.htm (Aug 10, 2001).

2) McAuliffe, Wendy. "Europe: Police want to monitor all Net traffic." May 17, 2001 12:29 PM PT. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2761777,00.html (Jul 16, 2001).

3) Raysman, Richard and Brown, Peter. "Developing Corporate Internet, Intranet, and Email Policies." Reprinted from New York Law Journal. Jun 9, 1998. URL: http://www.brownraysman.com/publications/techlaw/cllj0698.htm (Jul 16, 2001).

4) Anthes, Gary H. "Tape it or leave it, IS says long-term storage issues may trip up organizations." Dec 11, 1995. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO11939,00.html (Jul 18, 2001).

5) Thibodeau, Patrick. "European Cyber treaty Raising Concerns. Companies, privacy advocates have questions about agreement's impact." Dec 11, 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55022,00.html (Jul 9, 2001).

6) 1999 WL 462015 (Mass.Super.). Massachusetts Superior Court Memorandum. No. 97-2307 Jun 16, 1999. "Thomas F. Linnen (Plaintiffs) v. A.H. Robins Company, Inc. (Defendants)".

7) Yarbrough, Matthew and Henderson, Stephen. Interviewed on May 21, 2001. Fish and Richardson P.C. 5000 Bank One Center. 1717 Main Street. Dallas, Texas 75201.

EOF

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 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