National Journal of Advanced Research
www.thestudiesjournal.com
ISSN: 2455-216X
Received: 27-11-2025, Accepted: 29-01-2026, Published: 14-02-2026
Volume 12, Issue 1, 2026, Page No. 15-21

Preservation of electronic evidence, computer forensics and its legal admissibility

Dr. S Krishnan[1], Srishti[2]
[1] Associate Professor, Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India
[2] Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

Abstract
Information and communication systems are now breeding grounds for electronic-evidence (e-evidence) in audits, investigations, or litigation. Increasingly organizations are being ordered by law or lawsuit to preserve, retrieve, and hand-over relevant electronic records (e-records) because "the courts are uniformly recognizing the discoverability of electronic communication and documents" [Nimsger and Lange, 2002]. This trend is an outgrowth of aggressive tactics by regulators to ensure corporate accountability and deter fraud.
In cases ranging from Securities and Exchange Commission probes of corporate malfeasance and insider trading to employment lawsuits, e-records are subpoenaed. Investigations conducted by the National Association of Security Dealers, Department of Justice, and Department of Homeland Security routinely require companies, their business partners, or third parties to preserve and disclose e-records, including internal e-mail and instant messages (IM). A high-profile example is the probe into alleged White House leaks of a covert CIA agent's identity in which White House employees received e-mail stating: "You must preserve all materials that might in any way be related to the department's investigation." E-mail, telephone logs, and other electronic documents were mentioned specifically.
Any communication or file storage device is subject to computer forensic searches to identify, examine, and preserve potential e-evidence—the electronic equivalent of a "smoking gun." Preserving e-records and then restoring them so that they can be searched can seriously disrupt IS and over-burden Information Systems staff. What's more, a preservation order might specify not only the type of e-records (data files or email), but also stipulate that processes that over-write data be suspended, or that backup tapes be retained for unspecified duration. These stipulations are very disruptive to IS operations. That disruption depends largely on whether the company had an e-record management (ERM) system to systemically review, retain, and destroy e-records received or created in the course of business.
This article presents an overview of e-evidence and computer forensics and their implications for Information Systems. It aims to encourage research into ERM and fully-indexed, searchable e-mail archives by providing compelling reasons for how these approaches mitigate e-evidence risks and cost. These research issues are important for several reasons. Rarely are IS departments prepared for the challenges that evidentiary rules impose on active and archival data operations. Retaining unessential e-records increases costs and risks. Companies may need to justify their e-record retention and destruction policies as proof of compliance with their accounting, regulatory, or legal obligations. Courts impose severe sanctions on employers who claim they are unable to comply with e-record requests because of Information Systems design flaws or sloppy e-records management if it obstructs an investigation.

Keywords: Electronic evidence, computer forensics, digital discovery, e-record retention and destruction, electronic records management, legal issues

Introduction

Businesses' Electronic Records Create Risk

It is common practice for businesses to retain electronically stored information because it is convenient and cost-effective to store records in electronic format and because regulations require companies to maintain certain business records. Less commonly known is that the numerous e-mail and Instant Messaging (IM) messages sent and received on company e-mail systems may also be considered business records by the courts. Judges and regulators view e-mail and IM messages as business records if communication via e-mail or IM is a standard business practice—or if those messages are created as part of operations [Sleek, 2000] [23]
Clearly, IM for business communications is the trend. IDC estimates that there will be more than 400 million IM accounts by 2004, with nearly half of them connecting businesses with their customers or clients [Smith, 2003] [24].
The legal designation of e-mail and IM as business records is significant. Business records are subject to regulation and to pre-trial discovery, subpoena, or search warrant. Therefore, investigators use e-mail and IM records to create a "chain of evidence" proving illegal activity. With e-mail and IM sources of e-evidence, companies are exposed to risks of liability and litigation because:

1. Casual, private, or seemingly irrelevant e-mail messages or IM may be deemed business records, which even strongly worded disclaimers cannot repudiate.
2. Communications made in confidence are not protected from disclosure if they fit the legal definition of business record.
3. E-mail or IM that did not meet the definition of business record when they were created might nevertheless be required as evidence in court. For example, an administrative e-mail notice of a company softball game could be used as evidence in a workers' compensation claim if an employee is injured during the game [Flynn and Kahn, 2003] [8].

Shoddy e-records management (ERM) exacerbates the risk of civil or criminal liability for improper destruction of e-

records. Penalties for improper e-record destruction can be severe, as evidenced in December 2002 when regulators fined five Wall Street brokerages $8.3 million for failing to preserve e-mail messages [Smith, 2003] [24]. The content and preservation of e-records will be subject to greater litigation and investigations under new legislation, such as the Sarbanes-Oxley Act, to deter corporate corruption and fraud.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) that was signed into law in 2002 [1] represents an aggressive effort by the U.S. Congress to address the data retention and preservation issues arising from the Enron and Arthur Andersen fraud cases. SOX included the creation of the Public Company Accounting Oversight Board to address corporate responsibility issues [Patzakis, 2003] [17]. This law also:

- Mandates the retention of electronic documents.
- Mandates that companies produce their electronic records and other documents when summoned by the new Oversight Board.
- Imposes strict criminal penalties for altering or destroying records, including those kept in electronic form.

Section 802 of SOX imposes fines of up to $25 million and/or 20 years imprisonment against:

> "whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence" any government investigation or official proceeding."

In like manner, the National Association of Securities Dealers (NASD) and several government regulatory agencies issued new regulations and guidelines that expand existing e-record retention requirements. Public companies will need ERM procedures for prompt recovery of e-evidence in the course of the internal audits and investigations that these rules and regulations will inevitably generate.

Federal Rules of Civil Procedure

In 1970, Rule 34 of the Federal Rules of Civil Procedure (Fed. R. Civ. P.) was amended to address changing technology and communication. Amended Rule 34 made electronically stored information subject to "subpoena and discovery" for use in legal proceedings [Rasin and Moan, 2001]. This rule is the one that made e-records and communications breeding grounds for evidence of company activities and conduct. And every computer-based activity—whether it is sending email, invoices, viruses, or hack attacks—leaves an electronic trace.

Federal Rules of Discovery

According to Rule 26 of the Federal Rules of Discovery (Fed. R. D.), each company has the duty to preserve documents that may be relevant in a case [Scheindlin and Rabkin, 2002a] [19]. This duty to preserve is fundamental to, and inseparable from, the duty of disclosure. When involved in a legal action, companies are bound by the duty of disclosure to turn over requested e-records in readable format by a specified date.

Fed. R. D. categorize e-records as:

1. **Computer-stored records:** This category includes active data, replicated data, residual data, backup data, and legacy data.
2. **Computer-generated records:** This category includes cache files, cookies, Web logs, and embedded data or metadata.

The company must be able to produce all e-records that may be relevant in the case as requested in the subpoena, court order, or discovery motion. Furthermore, the Fed. R. D. specifically require that electronic documents be produced, regardless of whether or not paper versions are produced.

Power and Prevalence of E-Evidence

E-evidence

Broadly defined, e-evidence is electronically-stored information on any type of computer device that can be used as evidence in a legal action. Since e-mail can provide especially devastating evidence, the use of e-evidence is increasing. In a survey of 1,100 U.S. companies conducted by the American Management Association and the ePolicy Institute, 14% of respondents said they were ordered by a court or regulator to produce employee e-mail in 2002, which was up from 9% in 2001 [Zaslow, 2003] [30]. Garry Mathiason, whose law firm defends major corporations in employment cases, reported that almost every case his firm handles includes a "smoking e-mail" component [Varchaver, 2003] [28]. In 2000, e-mail was the most common type of e-evidence, and was dubbed "evidence-mail." In legal actions where evidence-mail or other e-evidence is used, it is as powerful as a smoking gun or DNA evidence, and as hard to deny or refute [Varchaver, 2003] [28].

Stricter regulatory compliance, primarily SOX in the financial sector and the Health Insurance Portability and Accountability Act (HIPAA) in health care, is also intensifying the demand for e-evidence. One of the first electronic document destruction cases under the SOX began in February 2002 [4] when Ernst & Young (E&Y) received a subpoena from federal banking regulators. A former E&Y partner, Thomas C. Trauger, had been arrested and charged with fraudulent alteration of audit documents for NextCard Inc. Trauger allegedly altered portions of E&Y's electronic working papers for NextCard's 2000 audit to improve NextCard's financial condition. [United States v. Trauger, 2003] [27].

Computer Forensics And E-Evidence

Computer forensics is the search of computer and communication devices for existing or deleted e-evidence.

> "Computer forensics is a mandatory process whenever the results of a computer investigation may ultimately be presented in a legal or administrative proceeding" Patzakis [2003] [17].

Computer forensics is typically a two-stage process:

1. The discovery, recovery, preservation and control of electronic data or documents.
2. The analysis, verification and presentation of e-evidence in court or investigations.

Federal and state investigations of fraud, negligence, antitrust, discrimination, intellectual property theft, viruses, and sabotage include computer forensic searches. The

outcome of many corporate cases turns on evidence obtained through computer forensics, most prominently Enron, Chase, Imclone, and Microsoft. Computer forensics investigations also revealed deliberate attempts to obstruct justice by destroying evidence, which is a criminal offense.
Computer forensics can be used to detect, trace, or prove a diverse range of crimes or cause of action [Appendix III]:

- fraud, negligence, malpractice
- theft of trade secrets, intellectual property
- violations of non-compete agreements
- safer design of a defective product
- privacy invasion, identity theft
- child pornography, violent crime
- money laundering, terrorist activity
- hacker activity, malware
- workplace harassment, discrimination, defamation

The following cases illustrate the use of computer forensics to find electronic proof of an illegal activity:

- In June 2002, supported by evidence from computer forensics investigations, a jury found Arthur Andersen LLP guilty of "wholesale destruction of documents." It was because of their document destruction— and not fraudulent accounting practices—that Judge Harmon imposed the maximum fine of $500,000 and five years probation on Andersen, which collapsed following its conviction [Eoannou, 2003] [6].
- In the case against American Home Products, manufacturers and distributors of Fen-Phen, internal e-mail was subpoenaed and over 33 million emails were searched. Plaintiffs' computer forensics experts uncovered e-mail stating:

"Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?" [Keena, 2002] [12].

American Home Products was charged with reckless indifference to human life, and settled the case for a record $3.75 billion.

- During the 2003 [28] investigation of SoBig.F, the FBI subpoenaed an Arizona Internet service provider (ISP) to identify the criminal(s) responsible for the e-mail worm that the DHS believed originated from a posting on an Internet site [CNN Money, 2003] [2].
- In September 2003, state and federal prosecutors for the first time searched IM records of licensed brokers and dealers investigating securities fraud [Smith, 2003] [24]. Using evidence from the bank's IM archive, a former Bank of America broker was charged with grand larceny and securities fraud [1].
- In October 2003, prosecutors confronted former Credit Suisse First Boston (CSFB) executive Frank Quattrone, charged with federal obstruction of justice, with copies of his e-mail in which he warned CSFB employees to clean out and destroy files amid investigations of the bank [Neumeister, 2003] [14].

A computer forensics examination may help mitigate permanent data loss and indicate faulty e-record retention practices. Andersen's demise illustrates the importance of conducting a computer forensics investigation to locate and preserve e-evidence, or recover deleted information. In the Andersen case, the firm could neither convince federal officials nor the jury that the destruction of e-records was the unauthorized action of a few rogue employees and managers [Patzakis, 2003] [17]. They also failed to prove that upper management did not tacitly endorsed the destruction.
Without doubt, the discovery of e-evidence assumed enormous importance in litigation. As regulatory agencies intensify investigation of corporate malfeasance and computer crimes, the obligations imposed on companies and their IS staff increases correspondingly. An overview of obligation and rights in legal actions is presented next.

Digital Forensics

Digital forensics is a relatively new science. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology. Whereas computer forensics is defined as "the collection of techniques and tools used to find evidence in a computer" [Caloyannides, Michael A.], digital forensics has been defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [Digital Forensics Research Workshop].
Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer systems. While computer forensics tends to focus on specific methods for extracting evidence from a particular platform, digital forensics must be modeled such that it can encompass all types of digital devices, including future digital technologies. Unfortunately, there does not exist a standard or consistent digital forensic methodology, but rather a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers. Palmer suggests that the evolution of digital forensics has proceeded from ad hoc tools and techniques, rather than from the scientific community, where many of the other traditional forensic sciences have originated [Palmer]. This is problematic because evidence must be obtained using methods that are proven to reliably extract and analyze evidence without bias or modification.
The complete definition of computer forensics is as follows: "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal…." (A Road Map for Digital Forensic Research).
Defining computer forensics requires one more clarification. Many argue about whether computer forensics is a science or art. United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005) ("Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science."). The argument is unnecessary, however. The tools and methods are scientific and are verified scientifically, but their use necessarily involves elements of ability, judgment, and interpretation. Hence, the

word "technique" is often used to sidestep the unproductive science/art dispute.

The key elements of computer forensics are listed below:

- The use of scientific methods
- Collection and preservation
- Validation
- Identification
- Analysis and interpretation
- Documentation and presentation

In order for different law enforcement agencies to effectively work together, they must communicate clearly. The investigative team must keep the entire picture in mind and be explicit when referring to specific sections.

The prosecutor and forensic examiner must decide, and communicate to each other, how much of the process is to be completed at each stage of an investigation or prosecution. The process is potentially iterative, so they also must decide how many times to repeat the process. It is fundamentally important that everyone understand whether a case only needs preparation, extraction, and identification, or whether it also requires analysis.

After examiners obtain forensic data and a request, but before reporting and case-level analysis is undertaken, the examiners try to be explicit about every process that occurs in the methodology. In certain situations, however, examiners may combine steps or condense parts of the process. When examiners speak of lists such as "Relevant Data List," they do not mean to imply that the lists are physical documents. The lists may be written or items committed to memory. Finally, keep in mind that examiners often repeat this entire process, since a finding or conclusion may indicate a new lead to be studied.

Examiners begin by asking whether there is enough information to proceed. They make sure a clear request is in hand and that there is sufficient data to attempt to answer it. If anything is missing, they coordinate with the requester. Otherwise, they continue to set up the process.

The first step in any forensic process is the validation of all hardware and software, to ensure that they work properly. There is still a debate in the forensics community about how frequently the software and equipment should be tested. Most people agree that, at a minimum, organizations should validate every piece of software and hardware after they purchase it and before they use it. They should also retest after any update, patch, or reconfiguration.

When the examiner's forensic platform is ready, he or she duplicates the forensic data provided in the request and verifies its integrity. This process assumes law enforcement has already obtained the data through appropriate legal process and created a forensic image. A forensic image is a bit-for-bit copy of the data that exists on the original media, without any additions or deletions. It also assumes the forensic examiner has received a working copy of the seized data. If examiners get original evidence, they need to make a working copy and guard the original's chain of custody. The examiners make sure the copy in their possession is intact and unaltered. They typically do this by verifying a hash, or digital fingerprint, of the evidence. If there are any problems, the examiners consult with the requester about how to proceed.

After examiners verify the integrity of the data to be analyzed, a plan is developed to extract data. They organize and refine the forensic request into questions they understand and can answer. The forensic tools that enable them to answer these questions are selected. Examiners generally have preliminary ideas of what to look for, based on the request. They add these to a "Search Lead List," which is a running list of requested items. For example, the request might provide the lead "search for child pornography." Examiners list leads explicitly to help focus the examination. As they develop new leads, they add them to the list, and as they exhaust leads, they mark them "processed" or "done."

For each search lead, examiners extract relevant data and mark that search lead as processed. They add anything extracted to a second list called an "Extracted Data List." Examiners pursue all the search leads, adding results to this second list. Then they move to the next phase of the methodology, identification. (Crime Scene Investigation.net)

Examiners repeat the process of identification for each item on the Extracted Data List. First, they determine what type of item it is. If it is not relevant to the forensic request, they simply mark it as processed and move on. Just as in a physical search, if an examiner comes across an item that is incriminating, but outside the scope of the original search warrant, it is recommended that the examiner immediately stop all activity, notify the appropriate individuals, including the requester, and wait for further instructions. For example, law enforcement might seize a computer for evidence of tax fraud, but the examiner may find an image of child pornography. The most prudent approach, after finding evidence outside the scope of a warrant, is to stop the search and seek to expand the warrant's authority or to obtain a second warrant.

If an item is relevant to the forensic request, examiners document it on a third list, the Relevant Data List. This list is a collection of data relevant to answering the original forensic request. For example, in an identity theft case, relevant data might include social security numbers, images of false identification, or e-mails discussing identity theft, among other things. It is also possible for an item to generate yet another search lead. An email may reveal that a target was using another nickname. That would lead to a new keyword search for the new nickname. The examiners would go back and add that lead to the Search Lead List so that they would remember to investigate it completely.

An item can also point to a completely new potential source of data. For example, examiners might find a new e-mail account the target was using. After this discovery, law enforcement may want to subpoena the contents of the new e-mail account. Examiners might also find evidence indicating the target stored files on a removable universal serial bus (USB) drive—one that law enforcement did not find in the original search. Under these circumstances, law enforcement may consider getting a new search warrant to look for the USB drive. A forensic examination can point to many different types of new evidence. Some other examples include firewall logs, building access logs, and building video security footage. Examiners document these on a fourth list, the New Source of Data list.

After processing the Extracted Data list, examiners go back to any new leads developed. For any new data search leads, examiners consider going back to the Extraction step to process them. Similarly, for any new source of data that might lead to new evidence, examiners consider going all the way back to the process of obtaining and imaging that new forensic data.

In the analysis phase, examiners connect all the dots and paint a complete picture for the requester. For every item on the Relevant Data List, examiners answer questions like who, what, when, where, and how. They try to explain which user or application created, edited, received, or sent each item, and how it originally came into existence. Examiners also explain where they found it. Most importantly, they explain why all this information is significant and what it means to the case.

Often examiners can produce the most valuable analysis by looking at when things happened and producing a timeline that tells a coherent story. For each relevant item, examiners try to explain when it was created, accessed, modified, received, sent, viewed, deleted, and launched. They observe and explain a sequence of events and note which events happened at the same time.

Examiners document all their analysis, and other information relevant to the forensic request, and add it all to a fifth and final list, the "Analysis Results List." This is a list of all the meaningful data that answers who, what, when, where, how, and other questions. The information on this list satisfies the forensic request. Even at this late stage of the process, something might generate new data search leads or a source of data leads. If this happens, examiners add them to the appropriate lists and consider going back to examine them fully.

Finally, after examiners cycle through these steps enough times, they can respond to the forensic request. They move to the Forensic Reporting phase. This is the step where examiners document findings so that the requester can understand them and use them in the case. Forensic reporting is outside the scope of this article, but its importance cannot be overemphasized. The final report is the best way for examiners to communicate findings to the requester. Forensic reporting is important because the entire forensic process is only worth as much as the information examiners convey to the requester. After the reporting, the requester does case-level analysis where he or she (possibly with examiners) interprets the findings in the context of the whole case.

E-evidence in Legal Actions

Pre-Trial Discovery

In preparation for trial or other legal action, each party has the right to learn about, or discover, as much as possible about the opponent's case. This pre-trial process is called discovery. A discovery request is an official request for access to any type of information that may be considered evidence [Arent *et al*., 2002] [1]. Information is discoverable (i.e., subject to discovery) if it is relevant to the facts that lead to the lawsuit or litigation, often regardless of whether or not it was personal or private [Gleim, *et al*. 1992] [9].

As discussed in Section I, under discovery rules, litigants can be required to produce e-records by a specific date. Therefore, if an opposing party submits a discovery request for a company's e-mails or other e-records, the company is required by law to retrieve and produce those records in readable format. Generally, courts view the failure to disclose information as an attempt to hide guilt and obstruct justice. For example, a court fined Prudential Insurance Co. $1 million for not turning over electronic data because failure to disclose that data harmed a plaintiff's ability to establish legal claims against the company [Sleek, 2000] [23]. The legal duty to preserve e-evidence is further complicated by the requirement that organizations that might be involved in legal action must take steps to preserve e-evidence even before being ordered to do so.

E-Mail In Discovery

The types of electronic data typically sought in discovery are internally produced e-records and internal and external communications, primarily email. Flynn and Kahn [2003] [8] report that discovery of e-mail occurs in nearly 100% of federal civil and criminal litigation cases and major employment disputes. They identified four reasons why e-mailis targeted, each of which directly relate to the management of IS and end-users.

1. People tend to be candid in e-mail messages, even if they are discussing confidential, incriminating, or criminal matters. E-mail records are notorious as sources of careless remarks that can cause devastating consequences in the courtroom.
2. Most organizations lack e-mail management, which increases the chance that damaging messages lurk somewhere in the e-mail system, servers, laptops, hand-helds, or backup tapes.
3. Producing e-mail, particularly if its unmanaged, can be too costly or inconvenient for a company. Faced with the costs or inability to respond to an e-mail discovery request within allotted time, a company may be forced to agree to huge settlements.
4. Despite the potential to waste millions of dollars or thousands of hours searching archived or deleted e-mail and other e-records, the courts ruled that e-mail searching is not "unduly burdensome."

Many companies are trying to determine how to organize their e-records systems for the eventuality of litigation, given that plaintiffs aggressively pursue them in discovery [Prywes 2002] [18],. Prywes stressed that planning for e-records discovery is especially important for companies that make and sell products used by the public. These companies face almost certain litigation or product liability suits, including class action suits.

Landmark Case About The Discovery Of E-Evidence

In August 2003, U.S. District Judge Shira A. Scheindlin set forth a revised test for determining how electronic discovery costs should be allocated. Her decision in Zubulake v. UBS Warburg, [S.D.N.Y. May 13, 2003] is considered to be a landmark case setting precedent as to which party pays for discovery of e-evidence. When addressing the burden and expense issues associated with electronic discovery, the courts recognize five categories of stored data. These categories are:

1. Active, online data. This data is in an "active" stage in its life and is available for access as it is created and processed. Storage examples include hard drives or active network servers.
2. Near-line data. This data is typically housed on removable media, with multiple read/write devices used to store and retrieve records. Storage examples include optical disks or magnetic tape.
3. Offline storage/archives. This category represents data that is offline on tape or other removable computer storage medium. Offline storage of electronic records is traditionally used for disaster recovery or for records considered "archival" in that their likelihood of retrieval is minimal.

4. Backup tapes. Data stored on backup tapes is not organized for retrieval of individual documents or files, because the organization of the data mirrors the computer's structure, not the human records management structure. Data stored on backup tapes is also typically compressed, allowing storage of greater volumes of data, but also making restoration more time-consuming and expensive.
5. Erased, fragmented, or damaged data. This data was tagged for deletion by a computer user, but may still exist somewhere on the free space of the computer until it is overwritten by new data. Significant efforts are required to access this data.

For data in accessible format, the usual rules of discovery apply, which means that the responding party is required to pay for production. When inaccessible data is at issue (categories 4 and 5), the judge can consider shifting costs to the requesting party.

Impact of Discovery and Orders To Preserve E-Evidence On Information Systems

Disruption of Information Systems

As discussed in Sections I and II, a court or investigator may issue an evidence preservation order for a company's e-records, including active data, data archives, metadata, network logs, cookies, web usage logs, email, and IM. Almost without exception, this order will disrupt Information Systems. To ensure e-evidence preservation, backup or maintenance operations that might alter requested data or e-records must be prevented from doing so.

A company can be charged with an order that is even more disruptive to Information Systems than an order to preserve. A court may specifically order a company to freeze their backup tapes and "to create and retain new backup tapes on an ongoing basis after the litigation is under way" [Shear, 2003 [21]]. This freeze order impairs or complicates IS operations. An order to freeze backup tapes can generate significant costs if backup systems and schedules need to be reconfigured. For legal cases that span several years, the number of backup tapes that need to be managed and the risk of data corruption increase significantly.

Cost And Complexity Of Responding To Discovery

Responding to a discovery request for a corporation's internal e-mail may seem simple and straightforward to the courts or lawyers. However, a company served with a request to produce e-mail messages faces time consuming and expensive processes. The cost and complexity depends on the volume of e-records, how they are organized, and their accessibility. The cost of responding to a discovery request can be in the millions of dollars if several years' worth of archived e-mail and files must be located, restored, sorted through, and cleansed to remove non-relevant confidential material [Sleek, 2000] [23]. Those costs are often in the millions of dollars. At the extreme, Chief of Staff John Podesta estimated the cost of the effort to reconstruct, retrieve and analyze e-mail related to the Monica Lewinsky case to be $11.7 million [Streza, 2003] [25].

Extensive spin-off costs may be associated with discovery. Searching through massive amounts of carelessly stored emails, server logs, or e-records can tie up a company' IS staff for days or weeks. Indiscriminately retaining or destroying information exposes companies to risks that are rarely considered. describes those risks.

The e-mail may pull otherwise unknowledgeable witnesses into the litigation. They may add little, if anything, to the merits of the claims or defenses, yet they are corralled, interrogated and distracted from otherwise productive duties. Instead of uncovering truly relevant facts, producing e-mail prolongs and sidetrack the search for truth, and sometimes may even develop untruth. Some written communications found in e-mail just are not accurate. [Streza 2003] [25].

Research Possiblities

These risks to Information Systems show the importance of research in ERM and compliance monitoring methods to ensure that employees retain necessary e-records. New methods for sorting, categorizing, retaining, and deleting e-mail and other electronic business documents are needed. In addition, while developments in storing and scanning technology increased the ease of storage, the volume and variety of e-records are expanding rapidly. For practical reasons, businesses must develop rules and procedures for deciding what they can discard and what they must retain [Scheindlin and Rabkin, 2002b] [19]. Boeing, the world's largest aircraft manufacturer, illustrated how disruptive a discovery request can be when no ERM or searchable e-mail archive is in place.

Case On Point: Boeing's Discovery Request

In October 1997, Boeing announced a $1.6 billion write-off because of production problems earlier that year. When this news was released to the public, the value of the company's shares dropped so sharply that a class-action lawsuit for securities fraud was filed against Boeing [Melnitzer, 2003] [13].

During the pre-trial investigation, the attorney for the plaintiffs (the party that is suing) learned that Boeing stored 14,000 e-mail backup tapes in a warehouse in Washington, D.C. The attorney filed a discovery request for all Boeing's e-mail related to their production problems. Company officials were required to produce those computer tapes for use as evidence. Boeing faced serious problems because the Information Systems staff could not figure out whose emails were on which tapes without restoring and searching all 14,000 of them.

Tapes are rarely configured so that they can be easily searched. They are the most common backup media, but are designed primarily for disaster recovery where the entire tape is reloaded. Regardless of how difficult or expensive it is to retrieve files from backup tapes, companies must comply with discovery requests and produce the emails or records that are requested [Varchaver, 2003] [28]. Boeing's only choice was to restore all tapes, which took thousands of hours of employee time. In addition to the huge cost of responding to the discovery request, the e-mails that Boeing produced for the plaintiffs' attorney contained so much damaging evidence that the company paid $92.5 million to settle the class-action case.

ERM

ERM (defined earlier as an acronym for Electronic Records Management) is used for "systemic review, retention, and destruction of documents received or created in the course of business" [Scheindlin ad Rabkin, 2002b] [19]. It consists of a broad range of policies, procedures, classification schemes, and retention and destruction schedules for electronic records.

Erm Policy Considerations

E-record retention and destruction policies can reduce costs and disruptions significantly. ERM reduces costs when requested information can be found promptly, preserved, and protected against accidental deletion. Disruptions are avoided because normal backup and overwriting procedures can continue to go on without bringing company information systems to a halt. Scheindlin and Rabkin [2002b] [19] recommend using separate servers for business documents to expedite the identification of privileged material in case of a discovery request. A study of record retention at DuPont validates this recommendation. The DuPont study revealed that more than 50% of documents the company collected for discovery requests between 1992 and 1994 should never have been retained [Melnitzer, 2003] [13]. Because of poor ERM, DuPont estimated that it cost the company between $10 million and $12 million over those three years in unnecessary retention and production costs.

An ERM policy should incorporate several general considerations.

- The policy should address each type of data and where it is stored.
- A policy should also provide for emergency recovery of inadvertently destroyed data.
- User training, compliance, and enforcement must be considered.

The impacts of the failure to manage e-mail as part of an ERM program are shown in numerous litigation cases.

Concluding Remarks

Since the 1990s, in the amount of electronic material that is discoverable for use as e-evidence increased significantly. The number of cases that involve the discovery of electronic material also increased. By 2000 [23], it was standard practice for lawyers who were engaged in discovery to request electronic information that was created, stored, transmitted, discarded, or deleted.

E-evidence, its preservation, and retrieval are issues that urgently need to be researched by those in Information Systems. IS researches may have avoided these challenging issues because they require legal knowledge. Regardless of reason, these research challenges cannot be ignored given that e-mail and other e-records are the primary source of evidence in many controversies and legal matters. When companies fail to manage their e-records, they face severe sanctions by the courts, disruption of computer operations, and considerable costs.

Once litigation begins, it is too late for planning. Companies expose themselves to financial risk and criminal charges if their policy for retaining and destroying of e-records is not sound and comprehensive. The pervasive and haphazard use of e-mail and IM make them the greatest source of risk, expense, or embarrassment for companies. Proper ERM procedures based on duties to preserve and disclose e-records are needed to reduce a company's exposure to IS disruption and obstruction charges.

References

1. Arent LM, Brownstone RD, Fenwick WA. E-Discovery: Preserving, Requesting and Producing Electronic Information. Santa Clara Computer and High Technology Law Journal, 2002, 19(131).
2. CNN Money. FBI subpoenas ISP Over SoBig, 2003.
3. Caloyannides MA. Computer Forensics and Privacy. Artech House, Inc, 2001.
4. Editor interview of Michael Prounis. Plan For Electronic Discovery Now— And Avoid "Bet The Company" Mistakes. The Metropolitan Corporate Counsel, 2002, 24.
5. Enneking NE. Managing E-mail: Working Toward an Effective Solution. Records Management Quarterly,1998:32(3):24.
6. Eoannou CL. Briefs Filed in High-Profile Fifth Circuit 'Case about Document Destruction'. Digital Discovery and e-Evidence,2003:3(7):1-2.
7. Flynn JP, Finkelstein SM. Tactic: A Primer on E-VIDE-N.C.E. American Bar Association Litigation, 2002, (34).
8. Flynn N, Kahn R. E-Mail Rules. New York: AMACOM, 2003, 108.
9. Gleim IN, Ray JB, O'Connor EP. Business Law/Legal Studies. Gainsville, FL: Gleim Publications, Inc, 1992.
10. Gordon M. WorldCom Stock Drops to 6 Cents. AP Wire Story, 2002.
11. Grimaldi JV. The Gates Deposition: 684 Pages of Conflict. Seattle Times, 1999.
12. Keena JR. E-Discovery: Unearthing Documents Byte by Byte. Bench Bar of Minnesota, 2002.
13. Melnitzer J. Keeping Track of the Invisible Paper Trail: What Legal Departments Can Learn From Boeing's Experience. Corporate Legal Times, 2003, 15.
14. Neumeister L. Prosecutors Use E-Mails Against Banker. Associated Press, 2003.
15. Nimsger KM, Lange MCS. Computer Forensics Experts Play Crucial Role. The Lawyers Weekly, 2002, 22(2).
16. Palmer G. Forensic Analysis in a Digital World, 2002.
17. Patzakis J. New Accounting Reform Laws Push For Technology-Based Document Retention Practices. International Journal of Digital Evidence, 2003, 2(1).
18. Prywes DI. Discovery of Electronic Records: Preparing for the Inevitable. The Brief, 2002, 31(33).
19. Scheindlin SA, Rabkin J. Outside Counsel Retaining, Destroying and Producing E-Data: Part 1. New York Law Journal, 2002, 227.
20. Scheindlin SA, Rabkin J. Outside Counsel Retaining, Destroying and Producing E-Data: Part 2. New York Law Journal, 2002, 227.
21. Shear KR. Orders Freezing Backups—An Approach that Should Leave Courts Cold. Digital Discovery and e-Evidence,2003:3(7):3-5.
22. Sidor G, Rogers S. Electronic Evidence is Superior to Paper Evidence. The Lawyers Weekly, 2002, 21(44).
23. Sleek S. Good e-Recordkeeping Saves You Money, Protects Your from Liability. Digital Discovery and e-Evidence,2000:1(1):1, 4-5.
24. Smith EB. Wall St. Bloodhounds Track IMs for Clues. USA Today, 2003.
25. Streza R. Discovery Unplugged: Should Internal E-mails be Privileged Confidential Communications? Defense Counsel Journal,2003:70(1):36-41.
26. Tambe JW, Redgrave JM. Electronic Discovery Emerges as Key Corporate Compliance Issue. The Metropolitan Corporate Counsel, 2002, 6.
27. United States v. Trauger. N.D.California, 2003.
28. Varchaver N. The Perils of E-Mail. Fortune, 2003.
29. Withers KJ. Killing the Vampire: Computer Users, Facing Discovery, Attempt to Make the 'Delete' Key Stick. Part I. Federal Discovery News, 2000.
30. Zaslow J. To Fight E-mail Sharing, Firms Try New Rules,Software. Wall Street Journal, 2003.