SearchCompliance.com E-Guide

E-discovery: What you Need to Know

In this expert E-guide, you will explore the importance of e-discovery through key tips and how you can assure you do not have e-discovery gaps in your information management process. These tips include: Getting your IT orgainization under control, coordinating with departments to understand your data retention policies, and accurately assessing the capability and effectiveness of your contingency plan. Also, learn the do’s and don’ts from two large corporations around their experiences with e-discovery and document retention.

SearchCompliance.com E-Guide

E-discovery: What you Need to Know

Table of Contents:

Data security: The missing piece of e-discovery (but not for long)

How State Farm saves millions on electronic data discovery

E-discover the gaps in your information management process

Electronic discovery critical to health of company, IT org

Resources from Google

Data security: The missing piece of e-discovery (but not for long)

Angelo Mozilo, Countrywide Financial Corp.'s former CEO, had already earned a "rep" as an inveterate emailer before the Securities and Exchange Commission (SEC) launched an investigation into allegations that he engaged in insider trading and misrepresented the financial condition of Countrywide. Mozilo, after all, was the author of a heated reply to a struggling borrower that called customer complaints about subprime loans "disgusting."

That email was a public relations disaster for Countrywide, but internal emails by Mozilo that describe Countrywide loans as "toxic" and Countrywide itself as "flying blind" may be far more damaging, now that the SEC is investigating whether he and his company misrepresented its condition to investors. The case is just the latest to underscore the growing importance of e-discovery in the courtroom.

Corporate legal departments are responding with stricter policies on document retention and more formal procedures for responding to discovery requests. There are also new tools, including electronic content management systems for storing documents and e-discovery software for analyzing information in those documents. Despite all that, experts say there's an elephant in the e-discovery living room: data security, in the form of porous networks, sophisticated hackers, malicious insiders and the specter of altered electronic records.

Data security on corporate networks and computers on which discovery takes place is of growing concern and will demand much closer attention in the years ahead, forcing e-discovery and electronic records management firms to forge closer ties to IT security vendors.

Foundation for admissibility

Document integrity isn't new to the courts or discovery. In the United States, the Federal Rules of Evidence lay out the authentication and identification parameters by which various types of evidence -- spoken testimony, documents and recordings, verbal testimony -- can be made admissible in court. While the courts, in a handful of decisions, have laid the foundation for admissibility with electronic documents, they are ill-suited to promulgate uniform standards and have been slow to adapt to changes in technology, noted Virginia Jo Dunlap, a senior consultant at Electronic Image Designers Inc., a consulting firm specializing in electronic content management and e-discovery.

"The law is set up to address the issue of original paper. There's just not a good foundation of how to work with electronic information," Dunlap said.

So, while the process of determining the admissibility of typed or written documents in court is well established, the process of authenticating electronic documents such as email is less clearly defined. The fact that such documents often aren't signed and may exist in various versions and locations on corporate networks makes authentication for the purposes of admissibility even more challenging, Dunlap said.

Craig Carpenter, general counsel at e-discovery vendor Recommind Inc., said he thinks the issue of document and data integrity -- the possibility that concerns about the security of electronic data might undermine its admissibility -- is going to be a major area of interest in the not-distant future. However, he added, the full impact of the security question hasn't hit the legal world or the enterprise content management (ECM) and e-discovery markets yet. "We're in the first half of the first inning, here," Carpenter said.

Recommended practices

With no clear guidance from the courts, the content management industry is taking the lead in setting best practices on issues like authentication. Recently, AIIM International, a standards group representing the ECM industry, released an updated version of its AIIM Recommended Practices. The new version adds a section that provides guidance on creating "trusted" ECM systems to store documents in a way that ensures that "all electronically stored information can be considered a true and accurate copy of the original information received."

AIIM recommends a number of measures to ensure system integrity, including hardware and storage media that prevent unauthorized additions, deletions and modifications of documents and data. The guidelines are designed to give IT departments and CIOs a frame around which new ECM implementations or modifications to existing systems can be built, said Dunlap, who helped draft the trusted system guidelines.

Dunlap noted that IT security and e-discovery have grown up independent of each other. While IT security companies like Symantec Corp., McAfee Inc. and Check Point Software Technologies Ltd. focused on keeping computers and networks safe from worms and viruses, e-discovery vendors focused on managing large volumes of case documents -- hard copies at first, but increasingly electronic documents in various formats and from an increasingly diverse range of sources.

Consolidated solutions

That's slowly changing. Legacy data identification and cleanup is a pressing issue in the e-discovery world, in what might be seen as a precursor to better data security. At the same time, companies like EMC Corp. and Symantec are bringing technology for storage, data security and content management together under one roof. Even rank-and-file endpoint and network security vendors are making big investments in data encryption technology and leak detection to help customers comply with a raft of new and toughened data security and privacy regulations.

E-discovery vendors like Recommind already partner with those vendors on solutions that combine e-discovery and content management. In the long term, executives like Carpenter envision a convergence of tools for systems management, information management, compliance and e-discovery behind a single pane of glass -- especially if IT security vendors become convinced that corporate legal departments concerned about litigation are better equipped to drive purchases than IT departments concerned about data security.

Carpenter said a bigger, but necessary, first step in aligning network and data security with ECM and e-discovery will be overcoming institutional barriers within corporations. "Today, the e-discovery manager has nothing to do with the IT security manager or data loss prevention. He has nothing to do with questions about whether a person has access to a file or server, and he doesn't care about that," Carpenter said.

As with so much in the legal world, however, such attitudes may disappear with the first seven-, eight- or nine-figure judgment in a case that hinged on the security of a litigant's network or content management system and the admissibility of the files and data stored there.

Restoring another backup tape to find that lost email made me go Google.

Searching for email through traditional backups is time consuming and costly – and displaces important work on other projects. But when you're responding to a discovery request or compliance audit, you don't have a choice. You have to restore and seek, until you find.

With secure, hosted Google Message Discovery, you'll change that. You'll perform email searches in minutes without having to restore any backups. Built on Google's cloud platform, Google Message Discovery provides unlimited storage, flexible retention, and the ability to hold specific messages for as long as you need.

Make your existing email infrastructure more secure, compliant, and productive. Try Google Message Discovery – part of the integrated suite of Google security and archiving services, powered by Postini.

www.google.com/postini

Google™

How State Farm saves millions on electronic data discovery

State Farm Mutual Automobile Insurance Co. takes what many would argue is a counterintuitive approach to electronic data discovery (e-discovery). The U.S.'s largest insurer of homes and automobiles keeps anything that might matter: emails, 100% of the email attachments of its claims officers, paper and electronic documents dating back 25 years, even the latest iterations of its human resources Web pages. The voluminous cache, meticulously imaged and coded, is stored centrally in an active system that is searched regularly as litigation arises

"For us it is not about cost but more about lowering risk. We have a lot of litigation all over the country," said Tim Crouthamel, section head of litigation support for State Farm's corporate law offices.

But saving basically everything in a centralized platform has also saved millions of dollars for the Bloomington, Ill.-based insurer, as evidenced in the wake of Hurricane Katrina. Crouthamel said the company was midway through the implementation of its centralized live repository when the hurricane hit. To recover data related to the Katrina litigation from just 1% of the hard drives cost State Farm $30 million. The long-term cost of archiving email for all 30,000 or so claims officers? Something around $1 million.

"Who knows what it would have been if we had searched everything we preserved, which, knock on wood, we haven't had to do," said Crouthamel, who spoke at last week's LegalTech event in New York.

Making documents available all the time

State Farm is not in the legal business. But litigation sure is a big part of its business. The insurer has approximately 150,000 pending lawsuits. It employs hundreds of law firms, all of which in the past answered litigation requests in their own way from their own collections of documents. After the explosion of bad faith cases in the 1980s and 1990s, State Farm wanted a workflow process that would allow it to respond to cases in a consistent and efficient manner, Crouthamel said. It did not want to have to school each one of its law firms in its data retention policies. With the advent of electronic data discovery laws, the need for a centralized platform became more urgent.

"We knew we have certain kinds of litigation across different departments. We asked what are the documents that we use over and over again," Crouthamel said. Why not "put them up in a platform where we can reuse the documents and the work products in an efficient manner?"

The company installed a dedicated staff at its corporate headquarters that does nothing but e-discovery. It brought the supervision of class action lawsuits in-house, ensuring State Farm speaks in a single voice on legal actions that affect the enterprise. It hauled in the many discrete document collections built up by its field law firms. And then it paired with e-discovery platform vendor CaseCentral Inc. in San Francisco to build a central repository, or master library, of carefully coded documents to populate its hundreds of thousands of lawsuits, minus the duplication and inconsistency common to the paper world.

This aggressively proactive process is not just about managing the past or materials requested in litigation. Any new document that could conceivably be requested in a legal hold is put into the repository by State Farm's cadre of "gatekeeper" paralegals, ready if necessary to populate the company's many lawsuits.

"We're trying to take the duty-to-preserve issue off the table," said Crouthamel, who refers to the company's re-engineering of its document management as "optimizing our e-discovery supply chain."

"It's kind of hard for the government to make a conspiracy argument against you when you have all the email and attachments of the people they are talking about as targets sitting there and ready to look at," Crouthamel said. The insurer's disciplined process elicits something approaching awe from other lawyers.

"I think State Farm, more than any other corporation I have seen, gets long-term enterprise evidence management better than any other firm I have talked to," said John Woods, a Washington-based partner at Hunton & Williams LLP, who advises companies on internal investigations, business crimes and complex civil litigation.

But Woods, who participated on the panel and does not do legal work for State Farm, said companies with more typical litigation exposure might well find this approach a tough sell in hard times.

"You have made a philosophical choice that you are basically going to save everything, but your volume of litigation is atypical and probably your risk is atypical," Woods said to Crouthamel.

The main message for companies, Woods said, is that whatever electronic data discovery process they implement should be easily explainable to outside counsel required to sign off on the process.

"I know a lot of companies very focused on saving only what needs to be saved. The tension point is that you can do whatever you want, but I [in the role of outside counsel] am going to ask some questions about how you got there."

E-discover the gaps in your information management process

So you passed your recent compliance audit. Your documentation and technical safeguards are in tip-top shape. You even have management on your side, providing reasonable money and support. All's well in the world of security and privacy -- that is, until your business gets sued and receives an e-discovery request.

Suddenly, the strong controls and leadership you have in place might not seem so robust. Electronic discovery, and more specifically information classification and retention, is arguably the biggest IT-related weakness in any given organization. Regardless of the size of your business or what industry it's in, you likely have some gaps in your information management process that could have some pretty serious consequences.

When asked how they inventory, store and dispose of electronic information, many IT leaders respond with "I don't know," "We're working on it" or "Legal handles that." The majority of information management scenarios I see in my work are lax, at best. Many people simply keep all electronic information indefinitely. It seems easier that way, but it usually only serves to help the opposition in a lawsuit. On the other hand, I have seen scenarios where lawyers who weren't up on compliance and technology just assigned random retention periods for electronic information. Even worse, the people in IT and compliance who needed to know about these policies were out of the loop. Nothing was getting done.

Many e-discovery cases have shown that the courts don't take too kindly to sloppy information management practices such as a lack of retention periods and inconsistent policy enforcement. There's a general false sense of security around e-discovery. Management and IT admins often assume that they'll just be able to do some quick searches and find whatever's needed when the time comes. The reality, however, is that electronic information is scattered about in every nook and cranny of the business. From decommissioned servers to off-site tapes to laptops and beyond, information that could be fair game in an e-discovery request is everywhere. Finding information -- especially if it hasn't been properly labeled, classified and stored where it should be -- can be an insurmountable situation if you get in a pinch and need the information quickly.

"Dig your well before you're thirsty." It's an ancient Chinese proverb that fits nicely into the context of e-discovery. By this, I mean get management's support and clearly define roles and responsibilities in the information management process so everyone is on the same page and can hit the ground running when needed. For example, the IT team will be responsible for the technical components, legal counsel for defining what to keep and for how long and so on. You also need to determine what information you have and where it's located, and clearly define the business's policies and procedures for information retention and disposal. Your security/governance/compliance committee would be perfect for all of this. Some companies even have a dedicated e-discovery coordinator who's responsible for this stuff 24/7. Just do something. Check out the Electronic Discovery Reference Model for further information on widely accepted practices in this area.

Finally, automating information classification and retention is essential for keeping e-discovery-related costs down. They say necessity is the mother of invention. Once lawyers and IT staff have to sift through everything manually to satisfy an e-discovery request, they'll see the value in information management products from companies such as StoredIQ and Kazeon.

E-discovery is a beast that's easily controlled if you make the right choices. As with information security assessments, if you're going to effectively manage IT risks and keep all aspects of compliance in check, you have to ensure electronic information is managed in the right ways by the right people using the right tools and some good old-fashioned common sense.

Electronic discovery critical to health of company, IT org

Not responding to an electronic discovery request is just as good as an admission of guilt, and this downfall lies squarely on the shoulders of the IT organization. In the well-known case of Zubulake v. UBS Warburg LLC, UBS could not produce potentially incriminating emails critical to the case, and the courts actually ruled that it was more likely than not these emails existed. This had damaging effects on UBS's case. Likewise, in United States v. Philip Morris USA Inc., Philip Morris was fined $2.75 million for continuing to delete emails after a notice of litigation was issued.

Cases like this have instantiated a tidal wave of fear in organizations, and just as they did in response to the Sarbanes-Oxley Act, organizations have seemed to overreact, overcorrect and overspend. And, as with Sarbanes-Oxley, I'm now hearing electronic discovery used as a blanket excuse to justify IT processes and spending that serve no business purpose. Continue down this road, and you won't need to worry about a lawsuit because there will be no company left to sue.

So how do you put these e-discovery concerns to rest for good? Well, you can't. E-discovery is like a reckless teenager; you do the best you can, then cross your fingers and hope nothing happens. Here are three key tips, though, that will get you 80% there. Don't worry too much about the other 20% -- that's where the cost starts kicking in and it's not really necessary.

No. 1: Get your IT organization under control

This is going to sound a lot like the advice I give for Sarbanes-Oxley because it equally applies. The first step is to get your own act together. If you're not organized, get organized. If you're already organized, stay organized.

Know everything about your data. Know where all your servers are and their purpose. Know what's in every database, and maintain tight data governance control. Understand both your transactional systems and your data warehouses. Know every detail about every transformation that your reporting systems make to rearrange your data.

Know where your data is at all times, from the time it gets created until the time it is destroyed. Know how your data is backed up, where your data is stored, and how long it is stored there.

For the purposes of e-discovery, the focus should be on email and instant messaging; however, e-discovery should not be the driver. Get everything documented and organized because this information is vital to a properly running IT organization.

No. 2: Don't do anything special for e-discovery purposes.

Coordinate with finance, legal and other departments to clearly understand what your document retention and destruction policies are and make sure you do your part to comply. I once led the development of a compliance data warehouse that had a policy of keeping everything online for 11 years -- and destroying anything older than that. The destruction is just as much a requirement as the retention.

Do everything you need to do to support your corporate policies (i.e., Sarbanes-Oxley, privacy, etc.) as they pertain to your business function, but don't make special accommodations in your normal business practice purely for e-discovery purposes (except for tip No. 3, below). You cannot anticipate what a potential lawsuit may require from an e-discovery standpoint, and the law does not require you to be clairvoyant.

No. 3: Hope for the best, but plan for the hold.

A litigation hold means things are about to get interesting. When there's even the anticipation of a lawsuit, your legal department will mandate that you stay your information destruction process. Litigation holds override any and all other retention policies. This is a contingency that you absolutely need to plan for and execute flawlessly. You must have the capability of altering your systems so information can be retained longer than usual.

I suggest organizing fire drills with your legal department to accurately assess the capability and effectiveness of your contingency plan. Have legal create a mock lawsuit, and go through the motions as if it were real. Focus first on email and instant messaging then branch out to other forms of electronically stored information like Microsoft Word and Excel documents. The first time through you will invariably find weaknesses in your system: This is normal. Continue executing drills until you know for sure you can react properly when it's the real thing.

E-discovery can turn into an e-nightmare if not handled properly. However, by running an efficient and lean IT organization and having a good litigation contingency plan, you can rest in confidence that you've done your diligence in the matter. Start discussions today with your legal department, about assessing your capability to support them.

Resources from Google

Postini Services

[To learn more about Google email security and archiving services please visit.]

[To contact our sales team please visit]

[To learn more about all of the enterprise IT solutions offered by Google, please visit]

About Google:
Google email security and archiving services, powered by Postini, enable organizations to make their existing email infrastructure more secure, compliant, and productive. The services protect against spam and messaging threats as well as provide content filtering and encryption for email. The archiving service stores email messages in a central archive with search capabilities to locate messages quickly. As a service, there is nothing to install or maintain, so organizations can simplify their IT architecture and lower costs.