Data Security in the E-discovery Process

E-discovery can be complicated, time-consuming and expensive—and so can proper data security. Here's how to merge the two and get the most bang for your buck.

Ease the Pain of E-discovery

E-discovery may be a dirty word among IT executives, but a more aggressive use of records management tools can help alleviate the pains and cost.

BY KEVIN BEAVER

***COMPLIANCE* IS OFTEN** deemed a dirty word in IT circles. But I have another 10-letter word that's just as dirty: *e-discovery*. This one word arguably creates the most angst among IT executives today. But there is a way to soften that angst with two other words: records management.

I have a lot of firsthand experience with e-discovery-related projects, so I can attest to the level of effort they require of a variety of people in IT roles. Similarly, in my expert-witness work, I've seen how quickly certain e-discovery requests are made by attorneys. The whole process of e-discovery is often brutal, extracting its pound of flesh from an enterprise, regardless of the resources it has to devote to it.

What used to be a cash cow for a select few e-discovery firms with the right tools has gone mainstream. There are numerous e-discovery and records management applications to help reduce the pain and cost associated with discovery requests. According to Stamford, Conn.-based consultancy Gartner Inc., the market for e-discovery software will reach $1.5 billion this year. Vendors such as EMC Corp., Optical Image Technology Inc., StoredIQ Inc. and Messaging Architects offer an array of archiving, e-discovery and information management solutions focused on records management.

The increase in data breaches, bribery and insider abuse underscores the need for such tools. Without them, it's practically impossible to search through hundreds of gigabytes of electronic records for the relatively small subset of data that's needed. If you don't have some semblance of electronic records management and something bad happens that leads to e-discovery, you're toast.

short

THE IMPORTANCE OF RECORDS MANAGEMENT

Looking at the bigger picture, records management is deeply entrenched in various business, compliance and IT processes. Given the amount of information you have, combined with the complexity of your information systems, the only reasonable way to manage these aspects of electronic data is with a good records management tool.

One of the greatest risks to any business is a lack of knowledge about what electronic information is, and the hard fact is that many businesses have little or no control over data classification and retention. These two factors are a dark cloud hovering over an enterprise, threatening to burst into a raging storm. You would be wise to lean on records management tools for help.

That said, as much as these tools can help, they are hardly a panacea. Longer term, you will have to streamline your management processes as well. If you really want to get records management and e-discovery down to a science, you will have to tweak both your business processes and the culture inside your organization. This will require:

- Obtaining and maintaining buy-in from members of upper management (which should be easy, since it's their rear ends on the line);
- Putting the necessary policies in place (classification, retention, labeling and disposal come to mind);
- Getting the word out on what constitutes business records (this is the tough part, but it has to be done);
- Holding people accountable for their actions when missteps occur (creating the understanding that labels such as "Internal use only" and "Archive after 90 days" mean just that); and
- Working with legal counsel periodically to ensure that your system is kept current (there's nothing worse than an outdated records management system that creates more problems than it solves).

Getting management and employee buy-in is half the battle. One of my clients struggled with this very issue for years. After being acquired by a larger company, which already had an efficient records management infrastructure and environment in place, things started to come together.

The typically slow-moving bureaucracy that haunts larger enterprises often hinders information security and risk management efforts. But we can all learn from the finely tuned records management processes many such businesses utilize. They're continually faced with e-discovery and compliance burdens, so records management has become second nature to them.

It would be wise to look into these solutions. If you need help justifying

their cost, many vendors have already done the research for you. The money saved in one e-discovery request can pay for a solution tenfold. Why not take that leap and invest in the right tools now, before you really need them? Things are only going to become more complex. ■

Kevin Beaver is an information security consultant and expert witness, as well as a seminar leader and keynote speaker at Atlanta-based Principle Logic LLC. Write to him at editor@searchcompliance.com.

JB: too much to cut?

E-discovery Gets Smart

The e-discovery software market is growing due to more stringent governance, risk management and compliance regulations—and it's creating smarter solutions.

BY ADRIAN BOWLES

THE PAST DECADE has seen increasing demands on enterprises of all sizes, and in all industries, to be prepared to produce specific business records in defending themselves against prosecution. Data from many systems under IT control may be required to satisfy regulators and the courts charged with enforcing privacy, security, governance, environmental and trade/tariff rules and regulations.

Most of the attention to e-discovery in the popular press is focused on emails—the proverbial "smoking guns" in regulatory cases. But data stemming from various areas of an organization may be requested in a legal proceeding. As the demand for better archiving solutions has increased alongside the overall growth of enterprise data, it's not surprising that e-discovery software is growing as a market.

To make sense of the requirements, the Electronic Discovery Reference Model (EDRM) has become the de facto reference used by vendors, consultants and buyers of e-discovery software products and services. EDRM is organized by projects, each of which comprises working groups. The v2 reference model includes:

- **Identification:** Identification and certification of electronically stored information (ESI) sources that may be relevant to discovery requests.
- **Preservation and collection:** Decide what to preserve and for how long. Litigation hold is a stipulation to preserve records—paper and ESI—that may be required in a legal action. Knowing what may be required by rule and practice is essential to a preservation policy and to subsequent collection efforts (which may involve people or an automated system to find and produce records).

- **Processing, review and analysis:** These are the heart of e-discovery software, and the steps where specific legal functionality and knowledge/rules must be applied. The defending enterprise must determine, according to laws, rules, guidelines and precedents, which data (including metadata) must be produced for opposing counsel. Core search technologies of today may soon be augmented by smarter processing in the future.

- **Production:** Extraction and preparation of relevant data.

- **Presentation:** The display of ESI in formats suitable for review by people charged with their evaluation: courts, counsel, juries, etc.

As noted, the processing/review/analysis steps require more legal knowledge than the rest. Therefore, it is natural that specialized vendors have emerged to address those steps, and just as natural that more traditional database archiving vendors have adapted their wares—or at least their marketing—to address the ancillary steps.

When asked about the plethora of vendors approaching e-discovery from a database and archiving standpoint, Parity Research founder Gary MacFadden noted, "the e-discovery space is immature...you see a lot of hammers looking for nails."

One product manager noted that the technology his firm developed for database archiving has found favor as an e-discovery aid because there is a big push from risk and compliance managers for live archiving. As a result, they are able to apply the same type of data retention strategy to records management and compliance.

IT has traditionally focused on price and performance of database archiving solutions when making buying decisions, based on criteria such as frequency of retrieval and storage costs. The new emphasis on collection, search and review can complicate purchasing, but it can also help free up the budget. When the transaction system is the system of record that may be subject to review under the Sarbanes-Oxley Act, those faced with the possibility of fines and incarceration are more inclined to fund appropriate expenditures for adequate improvements and controls.

The new emphasis on collection, search and review can complicate purchasing, but it can also help free up the budget.

Vendors with strengths in the key processes, such as Autonomy Corp., Clearwell Systems Inc., Recommind

Inc. and ZyLAB North America LLC, now face giants such as EMC Corp. (Kazeon Systems Inc.), IBM (OpenPages Inc., PSS Systems Inc.), Informatica Corp., Oracle Corp., SAP AG and Symantec Corp. as formidable competitors in the e-discovery space.

While the market shakes out, it's common for IT managers to look first to their traditional suppliers (enterprise software and hardware vendors), while legal, compliance and risk managers are wooed by the new breed of e-discovery solution providers. IT often has direct responsibility for software acquisition and operations, while the other stakeholders have more visible liability for compliance and legal actions.

This may set up a somewhat uneasy relationship and budget conflict. We are seeing new mandates from risk management and compliance managers, but funding still comes primarily through IT. One vendor suggested that this makes the buying cycle shorter, but the implementation cycle may actually take longer due to increased scrutiny and participation from new stakeholders.

For now, risk management and compliance professionals should be prepared to look beyond immediate regulatory concerns to include e-discovery policy choices when evaluating all enterprise software purchases. IT executives, meanwhile, should familiarize themselves with the new players at the heart of e-discovery, either as possible solutions or to challenge their incumbent enterprise solution providers to provide comparable functionality. There will no doubt be further consolidation in this space, but the courts won't wait, and neither should IT. ■

For now, risk management and compliance professionals should be prepared to look beyond immediate regulatory concerns to include e-discovery policy choices when evaluating all enterprise software purchases.

Adrian Bowles has more than 25 years of experience as an analyst, practitioner and academic in IT with a focus on IT strategy and management. He is the founder of SIG411 LLC, an advisory services firm in Westport, Conn., and director of the Sustainability Leadership Council. Write to him at editor@searchcompliance.com.

Avoiding the Breach

Web-based vulnerabilities are often simple to exploit because no one's watching. To protect your data, expand the scope of your incident response and Web forensics.

BY KEVIN BEAVER

WHEN WE THINK about computer forensics and incident response, it's often in the context of workstations and servers—items at the OS level, and rightly so, as that's where many Web security breaches take place. From malware infections to password cracking to lost or stolen laptops, there's often plenty of information right inside the operating system to help create a forensic timeline. But there's an area of Web forensics and incident response that we don't hear about as much: websites and applications.

Why is this? There are several reasons:

1. The assumption that a firewall and Secure Sockets Layer for Web encryption are all that's needed.
2. The assumption that your managed security services provider is taking care of things.
3. The assumption that your last Web security scan didn't turn up anything, so all's well.
4. The assumption that your business doesn't have anything the bad guys would want.

In many cases, Web-based systems have remained out of the spotlight. Perhaps it's because of the complexity of Web systems and all of the components involved? When you experience a Web security breach, there are numerous systems that may need to be analyzed. These include routers, network firewalls, Web application firewalls, Web servers and database servers. This shouldn't keep Web systems off your incident response radar, however. Given vulnerabilities as prevalent as cross-site scripting, Web-based malware and weak passwords, you have to ensure that your Web environment isn't taken for granted. After all, you can't respond to what you don't acknowledge.

When I refer to *Web environment*, I don't mean just your main website and your public-facing Web applications. Instead, I'm referring to every critical Web system you have, both externally facing and on your internal network. In my security assessments, I often find the greatest risks are to internal Web systems such as financial applications, intranet portals and system management interfaces. Some common Webcentric vulnerabilities I find are in core processing systems and ATMs in banks, firewall and storage management systems, physical security closed-circuit television monitoring systems and Microsoft SharePoint systems.

The one thing that's easy to forget is that it's often easier to abuse these critical internal systems because, after all, everyone's "trusted" if they're on the internal network. There's nothing to worry about, right? Nope. You do have stuff to worry about—especially when it comes to the governance and compliance of critical business systems.

The reality is, Web-based vulnerabilities—both public-facing and internal—are, more often than not, simple to exploit because no one's watching. There's little to no logging, limited system monitoring and no real accountability. If something happens in such a scenario, who's to blame? How are you even going to perform a forensics analysis when you don't have any visibility into the environment or controls in place generating data to analyze?

Some common Webcentric vulnerabilities I find are in core processing systems and ATMs in banks, firewall and storage management systems, physical security closed-circuit television monitoring systems and Microsoft SharePoint systems.

Cast a broader net and expand your scope for incident response and Web forensics. Otherwise, your Web-based systems are sitting ducks and your hands are going to be tied when the unimaginable becomes reality. ■

Kevin Beaver is an information security consultant and expert witness, as well as a seminar leader and keynote speaker at Atlanta-based Principle Logic LLC. Write to him at editor@searchcompliance.com.

CSI: Compliance

Computer forensics is perceived as a science rarely used by compliance officers, but that's just not the case.

BY KEVIN BEAVER

COMPUTER FORENSICS technology is an emerging field involving security incident and data breach investigations. The general perception is that computer forensics is a highly specialized area that businesses rarely tap into. In reality, it can be used in a wide array of circumstances—in fact, anyone working in or around IT, legal, compliance and human resources departments can benefit from learning more about computer forensics technology and the impact that it has on the overall information risk management process.

Computer forensics technology involves securing, collecting and analyzing digital evidence related to computer security incidents, data breaches and similar abuses of computer systems. Depending on the circumstances, law enforcement officers can perform the detailed technical and operational procedures associated with forensics investigations. Most computer forensics investigations require either commercial or open source software to uncover and preserve the details of what took place during the event in question.

What's the difference between computer security and computer forensics?

There are information system controls and security assessments for those who take security seriously, and forensics tools and techniques for those who don't. Computer security is proactive and involves the management of information risks before something happens. Computer forensics is reactive and is something you do after a breach.

The prospect of a security breach is very real, no matter how proactive you are and no matter how tightly things are locked down. Experienced compliance officers and security managers have systems for both the proactive and reactive components of managing their information systems.

How does computer forensics technology tie into incident response?

Incident response is the act of responding in a systematic and methodical way to internal and external security breaches. Forensics is a component of incident response that outlines how breach investigations are actually carried out through a number of tools and techniques.

There are various types of incidents or breaches that may warrant a computer forensics investigation, including:

- External attackers performing an SQL injection against a Web application to siphon data out of the database;
- External attackers breaking into an unsecured wireless network and gaining access to the internal network;
- Rogue employees copying sensitive information to an external hard drive to take off-site and share with a third party;
- A careless employee leaving an unencrypted laptop computer in his car, and the computer is then stolen.

The general assumption is that all security breaches are known and visible, but that's not always the case. Certain controls such as activity monitoring, audit logging and password lockouts can aid in both detection and forensics investigations when a breach occurs. The important thing is to ensure that the lack of an incident-response plan doesn't leave a hole in your information risk management and compliance strategies. It's also important to realize that certain breaches may go undetected for a period of time, especially if the proper controls aren't in place.

Is a formal forensics analysis needed for every suspected or known security breach?

It depends. This needs to be discussed in advance by your security committee. Management, legal, IT and compliance executives need to be involved in such decisions. You may not know if a formal investigation is required until you gather more information post-mortem.

> Not every breach is serious. It is a good idea, however, to approach each one as though it is.

Not every breach is serious. It's a good idea, however, to approach each one as though it is. You have to determine which systems were compromised, what was accessed, and whether such information is covered by what laws, regulations and contracts. Regardless of what's compromised, you'll want to step back to determine what needs to be improved in order to prevent the same occur-

rence. Your business may also be bound by data breach notification laws that require you to contact everyone whose personal information was compromised, or even suspected of being compromised.

You may also determine that the incident warrants getting law enforcement involved. A good rule of thumb is to get law enforcement involved if you're unsure. It pays to know your local law enforcement agency's cybercrime division. Knowing an independent forensics investigator or forensics firm would also be helpful.

How do I integrate computer forensics technology with my compliance program?

Forensics is an aspect of information security, just like compliance. The two areas are intertwined and need to fall under the umbrella of your overall information risk management program. The best advice is to not go at this alone. You don't want to bear the burden of making the critical business decisions associated with compliance, forensics and information risk management all by yourself. This will come to light when something bad happens and a regulator, auditor or judge pins you down and wants to know the reasoning and business justification for why you did or did not have controls and response procedures in place. ■

Kevin Beaver is an information security consultant and expert witness, as well as a seminar leader and keynote speaker at Atlanta-based Principle Logic LLC. Write to him at editor@searchcompliance.com.

SearchCompliance.com

Data Security in the E-discovery Process is produced by CIO/IT Strategy Media,

Jacqueline Biscobing
Managing Editor

Rachel Lebeaux
Assistant Managing Editor

Linda Koury
Director of Online Design

Kevin Beaver
Adrian Bowles
Contributing Writers

Ben Cole
Associate Editor

Scot Petersen
Editorial Director

FOR SALES INQUIRIES

Theron Shreve
Senior Product Manager
CIO/IT Strategy Media Group
tshreve@techtarget.com
(617) 431-9360