

Managing the Data Deluge

Digital data is pouring into your company: Get it organized or risk getting soaked

By Pam George

This article is the first in a four-part series.

How hard would it be for your company to pay a \$1.65 million fine for failing to retain e-mail records? That's how much the Securities and Exchange Commission fined Morgan Stanley for this transgression back in 2002.

After paying the \$1.65 million, would you have taken steps to correct the problem? Four years later, Morgan Stanley agreed to pay \$15 million for failing to produce tens of thousands of e-mails during the 2006 SEC probe of conflict of interests among Wall Street analysts.

Most company leaders want to avoid getting into trouble with the SEC, the courts or any other fine-levying entity. But despite your best efforts, you could one day get hit with a lawsuit. It could be for sexual discrimination, insider trading, or failure to fix a flawed product - and it could be completely unfounded.

But no matter the case, opposing counsel will demand all the records related to the case, including emails, and you'd better be able to locate and produce them - fast.

Need another compelling reason to get a grip on your digital content? You may need it to prove compliance with the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA).

And on a more fundamental level, if your company is typical, it is drowning in a deluge of digital data. If that data were properly organized, it could not only keep your company out of trouble, it could improve your business.

An escalating problem

In the late 1980s and 1990s, when the computer became a desktop staple, data began to accumulate. Not only did we increasingly create it, but we also started saving it, letting it sit on hard drives and servers. Each passing year brought more and more content.

"The amount of data we create has grown exponentially," says Tom Dugan, Owner and Founder of Philadelphia-based Recovery Networks, an offsite backup provider.

The nature of data has also evolved. "You've got this tremendous boom in video and multimedia business content, which must be indexed, searched, found, managed and archived over time," says Douglas Neary, Managing Principle, Collaboration & Compliance Solutions for LiquidHub in Wayne.

Blogs and discussion threads are also fair

game. "If a company allows employees to put comments out there, it might need to produce what employees are saying at any point and time," Neary notes. "With social networking now in the workplace, there are half a dozen new ways that people communicate. The genie is out of the bottle."

The data deluge goes beyond information that the company produces. It also includes all the information coming into the company, and it includes business-related data stored on employees' home computers.

The problem isn't limited to the data itself. "Over the last 20 years, companies have accumulated data in different data sources," says Anatoliy Chudnovskiy, Business Intelligence & Data Warehouse Practice Leader for Prime Technology Group in King of Prussia. "Right now they have not only one database, they have two, three or more."

When companies acquire companies, they also acquire that firm's data, backup tapes and archived items. Fred Diers, Vice President of E-Discovery and Compliance Practice for The Judge Consulting Group in Conshohocken, says one company absorbed so many backup tapes through acquisitions that it shelled out \$8 million to figure out what was on them.

Not all this data is worth saving, yet companies are loading up their servers or paying for storage. And in this economy, with today's soaring energy prices, that costs money.

Discovering e-discovery

Diers knows firsthand what it's like to sift through data for information pertinent to a case, such as the wrongful firing of an employee or records related to a product's development.

"We have to go in and figure out where the information is and look at the subpoena to find out what's being asked for," he says.

In the past, companies produced paper records for lawyers to comb through, a process known as "production," he says. With the growth of electronic records, that process has been dubbed e-discovery.

An unorganized system creates a staggering amount of work for the investigator. Tim Devlin, a Principal at Fish & Richardson, a Wilmington law firm, recently had a case for which the data collection ran into the terabytes.

Who foots the bill? The defendant. "One client last year was averaging \$4 million per case just to pay someone to find data," Diers says. "They're paying outside counsel \$450 an hour to go through what is mostly garbage."

Laptops exacerbate to the problem. "In order to collect everything relevant, you have to collect more irrelevant information," Devlin says. "You cast a wide net."

Large companies with multiple locations may have no idea where all the backup and archival information is stored in each city. But as Morgan Stanley demonstrated, the "I-don't-

Future articles in the Data Deluge series will cover these topics:

Part 2: Policies and procedures

Managing electronic records starts with defined policies and methodologies. For help, many companies turn to the gold standards set by the Department of Defense. This article will pay particular attention to e-mail policies and best practices, which have become critical.

Part 3: Tools and technology

Many applications are available to help companies manage data and harness its power for analysis, forecasting and decision-making. What

technologies are right for your company? Can you launch electronic records management within your budget?

Part 4: Storage and Security

Storage has long been associated with backup. Today, it's also about archiving. The flood of data has made a secure, organized archive a necessary part of records management. Many experts recommend a three-tiered system that addresses critical and non-critical information and the speed with which it must be retrieved.

know" approach does not work. Defendants come off appearing as though they're hiding something.

Claiming that you don't have the proper tools to search, index and find the materials may not reduce your e-discovery burden. "The plaintiff might say, 'But your honor, referential searching is a five-year-old science. They didn't automate it, but they should have,'" Neary says.

Companies that don't anticipate problems are ostriches with their heads in the sand, he continues. "Right now, organizations are waiting and reacting to compliance and e-discovery problem situations, instead of planning in advance."

Many of Diers' clients are doing just that, especially in the wake of the 2006 amendments to the Federal Rules of Civil Procedure, which specifically address e-discovery. Companies must be able to state where pertinent information - paper or electronic - is kept.

Creating a standard to meet the standards

To be sure, legislation has helped fuel the need to manage data. The Sarbanes-Oxley Act of 2002 introduced major changes to the regulation of financial practice and corporate governance.

HIPAA, enacted in 1996, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.

Title 21 CFR Part 11 of the Code of Federal Regulations focuses on FDA guidelines for electronic records and electronic signatures. The guidelines define criteria for the records' trustworthiness, reliability and equivalency to paper records. Drug-makers, medical-device manufacturers and biotech companies are just a few of the businesses required to implement controls.

Complying companies must prove they can track and maintain their data, says Michael McKinley, Chief Financial and Operating Officer for Allied InfoSecurity, a Conshohocken-based company that provides information security consulting and outsourcing.

You never know when you'll need what Neary calls a "snapshot in time." Take, for instance, the announcement of a merger, which understandably unleashes a flurry of stock activity. "Maybe in 30 days, the SEC says, 'You know, there was trading around that



Douglas Neary of LiquidHub

time that we don't like," Neary says. The SEC then demands all communications from the merger and acquisitions team - including emails, phone logs and online chats.

The situation is similar for the company whose product is under suspicion. The business must produce all the public positions regarding that product, including product safety bulletins and correspondence, he says.

Companies must preserve data within reasonable standards, some of which are dictated by law and some of which are dictated by the company itself.

That standard is only defensible if it's an established policy and you are abiding by it and enforcing it, McKinley says. Everyone has to be on board. Consider the lawyer who maintained that he deleted e-mails every day, only to learn that his secretary regularly went through his folders, placing deleted e-mails on a shared drive. "It could have led to a libelous situation," Diers says.

You're still culpable even when you hire a contractor to maintain, manage or store data. "You can make sure a third party contractually abides by the same security standards that you do," McKinley says. "But although you can outsource the activity, you can't outsource the responsibility."

Unleashing the power

Although it's a start, it might not be enough to simply organize data so it can be easily searched and protected. "In the future, the multiple ways it needs to be searched, indexed and found is the real striking change," Neary says.

For instance, a system with cross-referencing



Fred Diers of The Judge Group



Tim Devlin of Fish & Richardson

might allow searchers to both comb through customer invoice data and discover if a certain employee also accessed internal pricing tables at the time of invoicing.

Managed content in a data warehouse, meanwhile, becomes a powerful resource. A data warehouse facilitates reporting, analysis, forecasting and decision-making. "It is a comprehensive view of the organization," Chudnovskiy says. Business intelligence tools let users understand the company, measure its performance, improve relationships with stakeholders and create profit-making opportunities, he says.

Despite the clear case for records management, more than 85 percent of CIOs in a 2007 Accenture survey are nowhere close to employing an enterprise-wide content management strategy. Eight-five percent of the responding companies were either not building content management applications or they were building vertical or departmental solutions.

"Records management needs to be a core capability of a company, and that means the collection, indexing, protection and presentation of the information," Neary says. "What's our policy? What are the training procedures? And what's the technology? If you're not able to respond, your failure to do so could be very expensive proposition for you."