

Growing pressure for data classification

Jay Cline

March 22, 2007 ([Computerworld](#))

A storm is brewing over the silicon fields of corporate data — and companies that don't classify their data are going to get rained on. Why? Three reasons. New security-breach notification laws being considered around the world will compel multinationals to know where their most sensitive data is. The recent implementation of a U.S. Supreme Court decision on e-discovery allows for fines to be levied against companies in federal litigation that don't know where all their data is. And the decentralization of corporate data to mobile devices is heightening the risk of not having business-continuity plans that risk-rank critical data.

If you're one of the 65% of companies [polled by Computerworld last year](#) that don't routinely classify their data, you'll want to forward this list to Legal and IT to help inject some urgency into the situation:

- Data classification for breach response. U.S. state laws on security-breach notification have been so successful in prodding companies to shore up their information security that Congress, and legislative bodies in Canada, Europe and Australia are now considering adopting similar measures. To comply with these laws and prevent these breaches from happening in the first place, companies are starting to inventory all their data that trip these notification triggers. (See [Data Confidentiality Classifications](#) table below.)
- Data classification for e-discovery. Last December, amendments to the Federal Rules of Civil Procedure recommended by the Supreme Court concerning the discovery of "electronically stored information" came into effect. Under the new rules, companies need to produce all relevant information much earlier in the litigation process and may be fined stiff penalties for stumbling across new information during a trial. To avoid these penalties and reduce the cost of e-discovery, companies are finally

starting to implement comprehensive data-retention policies that routinely destroy old records. (See [Data Retention Classifications](#) table below.)

- Data classification for business continuity. The growing popularity in U.S. corporations of data-leak scanning software has shown them just how much of their data is flowing outside their organizations. Employees are increasingly e-mailing company files to their home e-mail accounts and storing them on their handheld devices and laptops. To ensure that a company can recover its operations in the event of a large-scale disaster, there has never been a greater need for companies to have a handle on where all of their mission-critical data is. (See [Data Recovery Classifications](#) table below.)

I can just hear the groans on the other end of your e-mail. "Three classification schemes? Are you crazy? This would be too expensive, and employees would never get it."

That's what I thought, too, until I came across companies that have put this into practice. I can't mention their names, but they've found basic data classification to cost less than any of their enterprise-technology implementations. And their employees intuitively understood the data classes after a minimal amount of training and awareness. In one company, 75% of employees could accurately identify the company's data classifications after just three months of an awareness campaign.

It all comes down to two basic messages companies need to inculcate in employees from Day One on the job:

1. Don't store **privacy-restricted** or **mission-critical** data on your laptop, mobile device, home computer or personal e-mail account.
2. If you have **official company records**, you need to store them in a special share-drive directory, since your personal drive and e-mail account will be routinely purged.

This isn't rocket science. And with these basic rules understood across your company, you can build out more rigorous security, retention and business-continuity programs over time.

You could do that, or bet that your company will never experience a publicized security breach, federal trial or large-scale physical disaster. As the Information Age converges with the Age of Terror, these kinds of bets will increasingly determine the outcome of careers and fortunes.

Jay Cline is a former chief privacy officer of a Fortune 500 company and now president of [Minnesota Privacy Consultants](http://www.minnesotaprivacyconsultants.com). You can reach him at cwprivacy@computerworld.com.

Data Confidentiality Classifications

My review of over 30 publicly available classification schemes for data confidentiality found that most chose minor variations of the four classes below. The most mature schemes mapped these classes with the data-security controls those organizations required to protect each class of data.

Data Class	Criteria	Examples
Public	Public exposure would not harm the company or individuals	Information posted to a company's public Web site
Internal use	Public exposure would not significantly harm the company or individuals	Information posted to a company's intranet Web site
Confidential	Public exposure could harm company business	Proprietary trade secrets
Privacy-restricted	Public exposure could harm a person's privacy	Social Security numbers and credit card information

Data Retention Classifications

Companies attempting to implement enterprisewide records retention are often stymied by their employees' inability to understand all of the different categories and retention periods their records may be subject to. A more effective strategy is to adopt a few simple categories, such as those below, and accommodate department-level variations on an exceptions basis.

Data Class	Retention Period	Examples
Regulated record	7 years	Financial statements
Historical business record	3 years	Completed client contracts
Temporary nonrecord	1 year	E-mails

Data Recovery Classifications

It's far too expensive for most companies to design business-continuity plans that immediately recover all their data in the event of a disaster. A more cost-effective approach is to classify data, systems and business processes into categories such as

those below, prohibiting employees from storing mission-critical data on home computers or mobile devices.

Data Class	Time to Recover	Examples
Mission-critical	Immediate	E-commerce Web site data
Urgent	Within 72 hours	E-mails
Nonurgent	Within 30 days	Client contracts; employee information