

# Data protection

How to take control of your data before it controls you

**A**re you aware of where all of your data resides? Do you know if you have too much? How about your retention schedule? Any idea as to the risks this data represents?

If you're like most businesses, it's as if a giant barrel of data was poured out and, naturally taking the path of least resistance, has found its way into every nook and cranny in your network. For years, companies have dealt with the proliferation of data by adding infrastructure. The server is slow? Add RAM or upgrade the processor(s). We are running out of storage? Space is cheap, so just add a server or a drive. Archive it, you know, just in case we need it some time. Inexpensive hardware has helped companies postpone the need for an effective and sustainable approach to data management.

*Smart Business* learned more from Dan Mallory, an IT audit and assurance manager with Habif, Arogeti & Wynne, LLP, about why businesses need more than piecemeal hardware additions to track and store their data: They require a solution that will address the risks and opportunities that this flood of data presents.

## Why is data management such a critical business issue at this time?

According to a recent report in *The Economist*, the estimated amount of data generated in 2010 compared to the amount of data generated in 2005 represents a 700 percent increase. Chances are, if you could measure it, you would find a similar trend occurring in your business. (Have you purchased more storage recently?)

While the average business is struggling to cope with all this data, few have made fundamental changes necessary to effectively control the flood of data hitting their business. The effects and risks of the proliferation of data are very significant. Some are obvious, such as the inefficiencies (e.g. search, application performance) brought about by storing much more data than necessary for much longer than necessary. Others are not as obvious, such as the risk this data represents. In addition, the introduction of cloud computing has uncovered new risk as your data is moved to the Internet and/or shared with other cloud apps and vendors.



**Dan Mallory**  
IT audit and assurance manager  
Habif, Arogeti & Wynne, LLP

## How should companies address data management concerns?

The first step in protecting data is to understand where it's captured, stored and shared. The output of this identification stage should be twofold:

- A map depicting the life cycle of personally identifiable information (PII) in and out of your organization
- An understanding of your inherent risk. This exercise should not be taken lightly. It's quite possible that your copy machines could contain thousands of digitally stored documents that get passed on when the machines are disposed of or repurposed at another company.

Here are a few other key elements of an effective data management program:

- Data with class. Step two involves classifying the data and records identified during the assessment. The classification should be used to build retention and security around your data. Keep in mind you're looking to identify what sensitive data your company possesses, capture and maintain the minimum necessary and place it on a fortified island.
- Know thy regulations. Requirements vary greatly depending on your industry.

**DAN MALLORY** is an IT audit and assurance manager with Habif, Arogeti & Wynne, LLP with more than 10 years of experience providing data-centric solutions and consulting to a variety of business and industries. He also has expertise in document management with deep knowledge in the data privacy sector having developed privacy management plans for firms concerned with personally identifiable information. He can be reached at (770) 353-7182 or dan.mallory@hawcpa.com.

Reference resources are aplenty, however, [www.aicpa.org/privacy](http://www.aicpa.org/privacy) is a great place to start, as it has industry specific information as well as both federal and state regulations.

■ Risk assessment. Armed with the knowledge of what data your business is capturing/storing/sharing, its classification and the regulations associated with that data relative to your industry, your risk map (including inherent risk and prioritization) becomes much easier to identify.

■ Control your risk. From a risk management perspective, one could say the opposite of risk are controls that come in the form of policies, procedures, system controls and even insurance. These risks come in a variety of forms (e.g. regulatory, reputation, litigation, etc.) all of which should be evaluated when considering the proper control used to mitigate the risk.

■ Trust but verify. Your monitoring program will need to ensure compliance with privacy policies and procedures, commitments, applicable laws, regulations and service-level agreements. Contracts should be reviewed and the results of such reviews reported to management.

■ The human firewall. Any successful data management program will involve a significant amount of employee awareness. No system is 100 percent secure, and informing your users of the importance of data and data security will create the final barrier between your data and the outside world.

## How do good data management practices translate to solid business practices?

Continuing to do what you've always done will only lead to increased costs, staff inefficiencies and significant risks of leaked or breached PII, resulting in loss of reputation and potentially crippling litigation. Traditional methods of throwing hardware at the problem will not deal with the core issue, and solving it requires a fundamental change in the way data management is dealt with, encompassing a rigorous, disciplined approach starting at the top. It won't be easy, however the result will not only be compliance but increased efficiencies and, in general, simply stronger business practices. <<