

The True Cost of Information Risk

By Craig Carpenter, General Counsel and VP Marketing, Recommind, Inc.



Craig Carpenter

Craig Carpenter, general counsel and vice president of marketing, oversees all aspects of marketing at Recommind. He has extensive experience in the enterprise software, information security and e-discovery industries, and is a frequent speaker and panelist. Carpenter is also an adjunct faculty member at the University of San Francisco where he teaches graduate classes on high-tech marketing, content management and digital rights management (DRM).

Let's face it: when it comes to electronic data, especially email, most of us are pack rats. We are loath to delete anything, no matter how old or utterly useless it might seem, for fear of not being able to find a document or message in the (highly unlikely) event we need a key piece of information. When the email administrator knocks on our office door or cube wall, our justification is elegantly simple: we should be able to keep as much email as we want because "storage is cheap." And to the untrained user this maxim seems accurate, as storage costs continue to fall. But while "more data" may be better for the creative types, it is most definitely not welcome to those of us living in the risk management, compliance and/or e-discovery worlds. What is increasingly apparent is that as data volumes soar, the "information risk" associated with this data rises in parallel, forcing enterprises to completely rethink how data is created, stored, shared and retired on all of their systems.

Storage Costs: the Ultimate Red Herring

Storage is indeed cheap. With 1 gigabyte thumb drives given away for free at trade shows and 1 terabyte external drives retailing for less than \$400, disc space on which to store myriad types of data continues to proliferate—to the tune of 60% data growth every year (*source: IDC Research*).

According to storage vendor EMC, this represents 45 gigabytes of data for every person on Earth, whether or not they happen to use a computer. This in turn feeds our insatiable appetite to create, share and save data in increasingly large chunks (remember when an MP3 seemed like a large file?).

But how relevant are direct storage costs in the context of risk management? As it turns out, not very relevant at all; in fact, they are a mere fraction of the overall costs of managing enterprise data. At the exact time the direct cost of storing data is decreasing, the indirect costs associated with managing this data are skyrocketing.

Indirect costs can include data center space costs (as storage devices require rack space in which to live), energy costs (whose rise is accelerating) and personnel costs (more devices require more techies to manage them), all of which are rising to varying degrees. But the real growth in costs can be traced to two drivers: costs of compliance and litigation-related costs.

From more humble beginnings, compliance costs have increased dramatically over the past six years—coinciding with seminal legislation including Gramm-Leach-Bliley and Sarbanes-Oxley (SOX) in the wake of the Enron and Worldcom meltdowns. SOX compliance alone has cost US businesses some \$32 billion since 2002, with 2007's price tag a cool \$6 billion (*sources: AMR Research; IDC*). Not to be outdone, the cost of identifying, preserving, collecting, processing, reviewing, analyzing and producing data for litigation (otherwise known as e-discovery) is even larger at \$12 billion and growing to \$22 billion by 2011 (*source: IDC*). The average e-discovery event—including regulatory investigations and lawsuits—costs \$1.5 million with the average \$1 billion revenue US company facing more than 500 lawsuits at any given time (*sources: Network World; Gartner Group*). The main factor driving these costs? The amount of data which must be collected, reviewed, analyzed and produced. And therein lies the problem.

A ballpark rate for e-discovery costs is in the range of \$2,000 per gigabyte of data, so a case with 200 gigabytes of data will generate \$400,000 in e-discovery costs. But this is where the data growth phenomenon, driven by ever-cheaper storage costs, comes into play: With data volumes growing 60% every year, e-discovery costs are by definition growing commensurately—and quickly outstripping legal department budgets set up to handle these issues. These costs have become so significant that they are increasingly forcing enterprises to rethink their approach to data creation, sharing, storage and deletion.

A New Way to Think About Data

Risk managers, compliance officers and litigation managers are taking increasingly active roles in the management of the data lifecycle within their companies. Historically, these groups' concerns may have fallen upon deaf ears, but with information risk occupying more and more of enterprise budgets, they are increasingly finding an interested audience at the executive and board level. In the past, these groups have collectively viewed data—inasmuch as they viewed it at all—as the province of individual users who are allowed to do what they wished so long as they stayed within the bounds of HR guidelines. Today, however, many enterprises are seeking to get the most out of their data while simultaneously getting (and keeping) their "information house" in order.

First, rather than putting data into separate silos, many are making all or nearly all data securely searchable to those who have appropriate access rights, as this allows risk managers to figure out what data is where while simultaneously increasing the utility of corporate data. Second, many enterprises are deleting redundant data in an effort to gain control over exploding data and storage centers. Another benefit of this "deduplication" exercise is that it helps enterprises identify what data should be kept, which allows them to start retiring data which should *not* be kept—which is important to effectively respond to investigations and lawsuits. Finally, enterprises are building and scaling their IT infrastructure with risk-management needs squarely in mind, including records management, e-discovery, compliance and knowledge management. Although these efforts have just begun for most, with so much potential risk at issue proactive enterprises will find themselves with a distinct advantage over their laggard peers. ■