Storage-as-a-Service: Best Efforts or Best Practice ?

IDG research reveals gaps between information management best efforts and best practice

Compliance and security, litigation readiness and legal discovery, among other things, are driving greater attention to electronic information management strategies, from data retention schedules to destruction protocols. But do CIOs' best efforts meet the real requirements? Recent research reveals that IT professionals understand the fundamentals of managing and protecting data, however key best practices are often not in place.

When it comes to information management, storage and data protection strategies, IT professionals definitely get it. In fact, a recent study by IDG Research Services shows that IT pros recognize what needs to happen to effectively manage and protect data, and they're taking definitive action to that end. However, best practices are still just out of reach.

Specifically, the majority of survey respondents express an appreciation for outsourcing as one of those best practices, touting a host of compelling benefits. Yet only 17 percent are ready to jump aboard the Storage-as-a-Service bandwagon.

"This obvious discrepancy begs very important questions," says Fred Engel, SVP of Engineering and CTO of Iron Mountain Digital. "Are CIOs doing enough to control the in-house costs associated with the exponential growth of information, its distributed nature, and demands for compliance and litigation support? Are they willing to bet their badge on their current in-house information management, storage and data protection strategy as a solid, viable option in the long run?"

Compliance Drives Attention to Information Management

CIOs are certainly spending a lot more time thinking about their information management, storage and data protection strategies. In fact, they've become downright strategic in their thinking, and it's all about compliance and security.

Eighty-seven percent of respondents to the January 2008 survey point to compliance or compliance-related issues like legal discovery, auditors and security as the top drivers for their information retention and destruction practices. The survey, by Framingham, Mass.-based IDG Research Services, polled 100 IT decision makers from organizations with 1,000 or more employees across 15 verticals, with the most respondents working in the health care, manufacturing, government, finance and banking, and insurance categories.

"Compliance is the start, but it is also about controlling the growth of demand for storage," says one survey respondent, a director-level IT professional at a global pharmaceutical company. Granted, storage management, cost control and business imperatives are important, but in this survey, respondents tend to rate them secondary to compliance.

CIOs have retention strategies for all sorts of digital/electronic information, from legal documents to chat logs. But no matter the information, they are strategic in establishing retention schedules, which is most prevalently governed by internal and external policies, the survey found. Tactical reasoning is not the norm, as responding companies tend not to let issues like resource constraints dictate how long data is kept.

94% of survey respondents have created or are in the process of creating written policies.

Research conducted by
CXO Media

CIO
Custom Solutions Group

Sponsored by

IRON MOUNTAIN DIGITAL™

Storage-as-a-Service: Securing the Right Third Party Relationship

When it comes to selecting a third-party storage provider, the IDG survey respondents have some fairly strong opinions. Specifically, they cite the following criteria as most important when considering providers: TCO (78 percent), reliability (61 percent), ease of retrieval (61 percent), compliance rules built in (55 percent), and company health and future outlook (52 percent). Least likely to be considered important are shared liability (25 percent) and product road map (22 percent).

Best practices in the selection process, however, might have CIOs refining their selection criteria away from cost as the overriding factor. With the right partner, total cost of ownership should come naturally, as that provider will leverage the many features and benefits that come with Storage-as-a-Service to deliver bottom-line value. So perhaps CIOs should focus their attention on choosing the provider with the most experience and best infrastructure to help them reach those elusive best practices that keep them up at night.

"Our highest priority is adoption of compliance best practices that assure the treatment of electronic data and the various media it can reside on, like magnetic disk, CD, DVD and solid-state storage, be consistent with the treatment of paper-based data," says Ed Todd, data warehouse manager for Jacksonville, Fla.-based Nemours, a nonprofit children's health care system.

Progress, with Room to Improve

It's abundantly clear that IT decision makers are taking their digital/electronic information management, storage and data protection practices seriously and making strides across the board. In fact, the IDG study illuminates several best efforts toward effective data management and protection. Still, those efforts seem to be coming up short.

1. CIOs are creating policies around retention and destruction.

"As with many organizations, we have a policy for record retention and destruction that was silent on digital data," says Todd. "We are now formulating protocol that parallels the non-digital policy to assure we meet with statutory requirements for retention." Nemours is not alone, with nearly all respondents (94 percent) indicating that they have created or are in the process of creating written policies governing the retention and destruction of electronic information. Still, with such an overwhelming response, one must question exactly how formal and comprehensive those policies are.

Best practices mandate formal, written policies with defined roles and responsibilities, and an equally formal communications process—all unilaterally enforced. Perhaps most important, such policies must be all-encompassing. Policies should extend across the enterprise to include everything, from centralized records in the data center to individual files on the desktop, even when inventory control proves difficult. And they should cover all types of media—for example, physical and electronic records and structured and unstructured data. Finally, policies can't be created as one-time projects, but rather they must be tested, measured, assessed and modified on a continual basis. All said, that seems a fairly tall order for such a high percentage of respondents.

2. Enterprises are treating backup and archiving requirements separately.

Another very encouraging data point is that nearly half of the survey respondents say they treat their archive and backup requirements separately. Yet a full 39 percent still do not distinguish between the two disciplines at this time.

Best practices require CIOs to consider the business implications associated with both scenarios. The backup—versus—archiving decision must be strategic, not a knee-jerk reaction borne of complacency or bad habits learned over time. "Meaning, an IT decision maker responsible for disaster recovery mustn't automatically solve archiving-related problems with backup solutions," says Engel. "And an email database administrator shouldn't fixate on an archiving solution to resolve a business continuity need."

3. The retention and destruction of electronic records have become selective processes.

The majority of respondents are selectively retaining data for a specified period of time. However, nearly 20 percent say they still keep everything indefinitely, or selectively retain data indefinitely.

Could it be that, over the years, nightly backups have inadvertently become the retention practice of record? That's not a selective process, nor does it make for a best practice. In contrast, enterprises need to implement archiving protocols based on the business and legal implications of specific types of data. For example, records that are subject to legal constraints should be retained as required. At the same time, sensitive internal documents—not subject to compliance regulations—must be subject to destruc-

tion policies. Mechanisms must be in place to ensure that obsolete records are disposed of properly and that "holds" or temporary "cease destruction" clauses kick in when necessary.

Todd bases Nemours' retention schedules on compliance requirements. "As a health care provider that also conducts research and physician training, we have to balance the retention of meaningful data to support that research and evidence-based medicine," he explains. "Accordingly, we cannot separate the 'retain versus destroy' issue from the consideration of appropriate privacy (i.e., HIPAA) and de-identification practices."

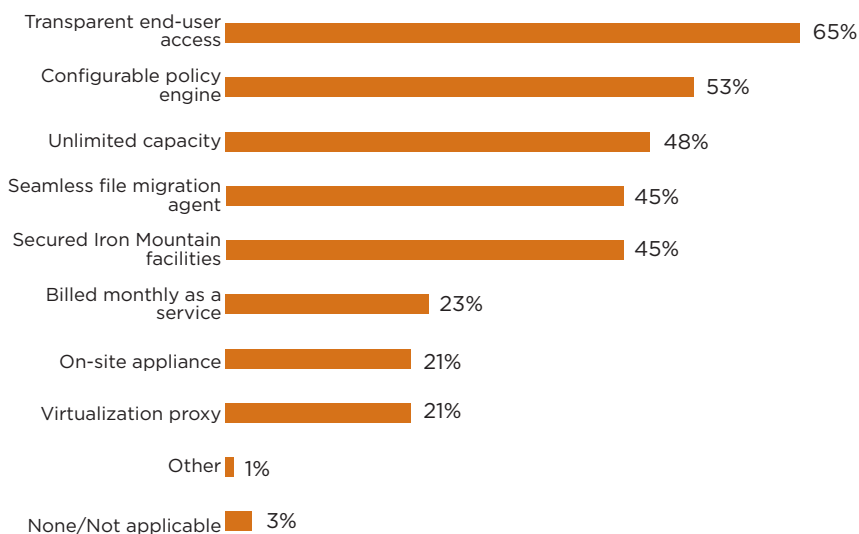### 4. Enterprises are actively investing in archiving technology.

In regard to infrastructure, enterprises seem to be on track, with 62 percent already investing in information archival technology and another 38 percent planning to invest.

That's a positive indication, Engel observes, "Though in another survey conducted by IDG last year, we learned that only 38 percent of enterprises index their data." Indexing is a key best practice in eDiscovery, as the technology is used to locate, analyze and present requested records in a timely manner based on specific criteria, such as subject matter and date. Also, access control based on type of record should be part of the package to control who is authorized to access what, pursuant to predetermined policy.

Moving Toward Storage-as-a-Service

In the end, the greatest challenge for our responding pharmaceutical company IT professional is "designing a system that covers all of the different types of documents in all the different jurisdictions and complies with all of the applicable regulations and guidelines." That's a daunting prospect that suggests CIOs should be weighing options, and perhaps looking at approaches that take the onus of "pulling it all together" off the enterprise, and instead leverage the experience of organizations that live and breathe storage.

Most Appealing Aspects of Storage-as-a-Service model for Electronic Records and Information Archival

Aspect	Percentage
Transparent end-user access	65%
Configurable policy engine	53%
Unlimited capacity	48%
Seamless file migration agent	45%
Secured Iron Mountain facilities	45%
Billed monthly as a service	23%
On-site appliance	21%
Virtualization proxy	21%
Other	1%
None/Not applicable	3%

"If a [third-party] provider can deliver the compliance expertise as a value-add," Todd says, "there may be a great deal of merit to using a provider." And that leads to the most interesting revelation from the IDG research, in that the greatest gap between best practices and best efforts involves outsourcing.

Outsourcing in and of itself is not a new concept, but it is now being applied in a compelling new way to address information management requirements. Storage-as-a-Service, as it's becoming known, is an outsourcing option for which information is selectively removed from an operational system and stored with a third party for electronic archiving and retrieval for a variety of needs including litigation and corporate investigation.

"It's clear from the survey results that IT leaders understand the potential upside to outsourcing their storage requirements,"

says Engel. "So it's no surprise that Storage-as-a-Service is emerging as an overarching best practice in information management."

Storage-as-a-Service enables enterprises to gain the very capabilities they need to bring their efforts to the next level. It can provide data protection and recovery across servers, shared files and even desktops; policy-based scheduled and automated archival and backup; more stringent recovery time and recovery point objectives than in-house programs; and categorization and indexing capabilities for eDiscovery. What's more, enterprises can leverage state-of-the-art technology without the capital investment.

Indeed, the return on investment for Storage-as-a-Service speaks volumes, with survey respondents pointing to a host of risk and cost benefits. The risk benefits are top of mind, with the highest ratings going to simplified legal discovery, long-term protection and enhanced compliance. Interestingly, offloading risk and third-party indemnification rank lower, even though both speak to a very important risk issue. Cost benefits, including improved utilization, reduced complexity, simplified storage infrastructure and less floor space, rank strong as well, but are secondary to risk rewards.
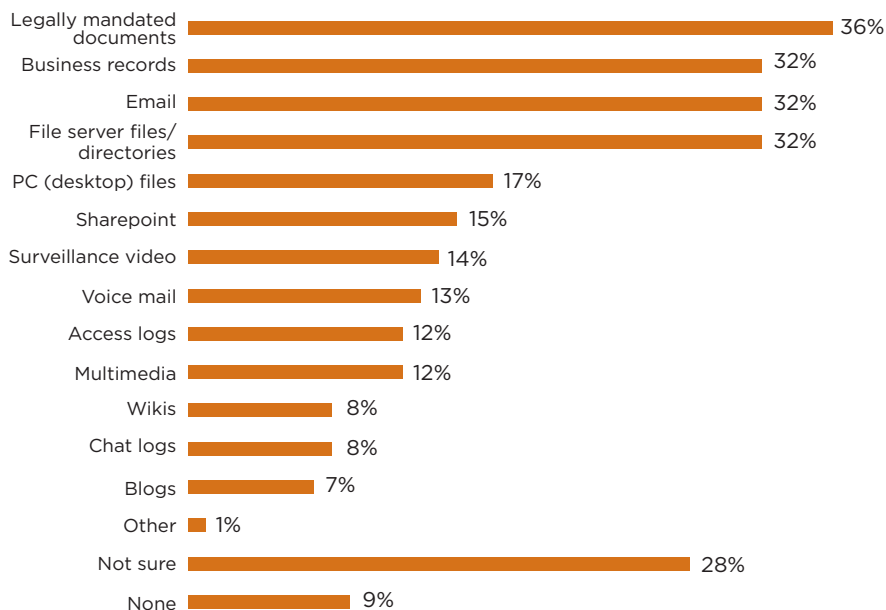
Todd predicts that the cost of storage space will not be the differentiator. "A business continuity provider that also bundles the backup/archive storage and data management expertise could be an attractive package," he says, which makes it a classic "build versus buy" decision.

All that said, less than 20 percent of respondents say they are currently willing to consider Storage-as-a-Service as a viable option for their company's information management needs. That brings to bear some critical questions: Is outsourcing worth greater consideration? Are CIOs willing to admit there could be a better way? And how confident are they, really, in their strategies, now that the benefits of Storage-as-a-Service are understood?

"Most important, with outsourcing, CIOs are free to strategically analyze their backup and archiving needs separately and implement the right information management for their unique business needs," says Engel. "And, of course, their valuable data assets can be safe, private, available and compliance-enabled."

Willing to Allow Offsite Third-Party Management for:

Category	Percentage
Legally mandated documents	36%
Business records	32%
Email	32%
File server files/directories	32%
PC (desktop) files	17%
Sharepoint	15%
Surveillance video	14%
Voice mail	13%
Access logs	12%
Multimedia	12%
Wikis	8%
Chat logs	8%
Blogs	7%
Other	1%
Not sure	28%
None	9%

17% of survey respondents are willing to consider Storage-as-a-Service.

CALL TO ACTION:
To learn more about Storage-as-a-Service, please go to www.ironmountain.com