Records Management & Regulatory Compliance

Finally on the Front Burner

By Peter Mojica, Vice-President, Product Strategy and Management AXS-One Inc.

Peter Mojica

Peter Mojica is vice president of product strategy and management for New Jersey-based AXS-One, a leading provider of records compliance management software. Mojica is a thought leader in the fields of records management, corporate compliance and risk mitigation, and speaks at numerous industry events annually.

Mojica has more than 18 years of information technology experience, primarily in the financial industry. He brings a broad range of sales, technology marketing, and information technology management expertise to AXS-One.

At first glance, it's difficult to see how much has changed in records management and regulatory compliance in the past couple of years. Naturally, some new laws and regulations have been introduced and older ones have continued to evolve, particularly in the multinational context. More companies are putting compliance-related policies in place, and some are taking the trouble to enforce them. And while a few technologies have improved significantly, many still can't do what's needed. But without a close look, it might be hard to tell what's truly different and what's needed now.

In the real world, however, just about everything is different. There's a new urgency in the air, and they can feel it all the way to the boardroom.

Once confined to the back of the business section, issues related to records management and regulatory compliance now dominate the headlines. Either directly or indirectly, these issues have caused companies to be levied huge financial penalties, been the reason for executive turnover (even through prosecution and conviction), led companies to actively enforce policies that have long been in place, been the recipient of significant budgetary resources and, perhaps most importantly, become a companywide priority rather than one essentially relegated to the IT department.

Unfortunately, the stories are often negative. Earlier this year, a financial services conglomerate was hit with a huge fine, in part because it couldn't guarantee that it had turned over every relevant e-mail. In its own defense, the company clearly tried hard to track down all the relevant content. Yet backup tapes kept turning up in closets, yielding more e-mails that had to be combed through. Eventually, the judge lost patience.

Only a few months earlier, in another case involving a major financial services firm, it was found that despite counsel's instructions, employees had deleted some relevant e-mails while the defendant had withheld others. The judge subsequently instructed jurors to presume that the withheld information was prejudicial.

In that case, the jury awarded the plaintiff a total of $29 million in damages—a staggering amount by any measure. In the more recent example, which involved very different litigation, the fine reached $1.45 *billion*.

It's important to remember that in both these cases, the companies caught in the court's headlights were hardly novices; they had billions in reserve, sophisticated executives in the boardroom, high-priced counsel on the payroll, stringent e-mail and content retention policies in place and an expensive technology infrastructure. It could almost be argued that these companies were doing everything *right*. Yet both were essentially caught flat-footed.

The judgments sent shock waves down Wall Street, and perhaps throughout corporate America, as many other enterprises came to the sobering realization that they, too, might be helpless to comply with the same directives.

So what's going on here? How did things go so wrong?

First, let's accept that the content universe looks very different than it did even five years ago. There's a lot more of it, and new mandates for having to keep and manage it over a long period—and destroy it at a precise time—have changed everything.

Take e-mail: No one could have predicted how this would become the cornerstone of business communication. IDC estimates the average number of e-mails sent *each day* will hit 36.2 billion next year. Then there's instant messaging. It's now on just about every business desktop, yet many public corporations have virtually no policies or means of IM retention. Overall, from an IT perspective, organizations don't have true archiving policies, while on the business side, companies can't figure out what they need to keep, for how long and in what ways.

Second, it's obvious that requirements such as Sarbanes-Oxley, the SEC, HIPAA and others are just the tip of the iceberg. The most sensible mandates—for example, that e-mail shouldn't be used for private communications—are also the least practical. What corporations need instead is a global hierarchical data archival and retention management system that governs both the technologies and the users involved. This should be done strictly according to regulatory requirements, risk measures and other corporate mandates that allow an organization to build clear lines between risk, profit, systems and people. But in the real world it's never so neat. Just as government regulations continue to evolve and litigation tries to zero in on the "smoking gun," corporations work to implement policies and technologies that make sense, protect the corporation while maintaining investor confidence and manage it all without overwhelming those responsible for compliance, legal issues and information technology. That's a hard balance to find even at the best of times.

Third, it's vital to remember that no two industries are exactly alike. What do the regulations governing your particular business require relative to your corporation's information? That's not an easy question to answer, since many corporations have found a competitive advantage in developing complexity across their diverse systems: more integration, more customized applications, etc. However, with respect to compliance, this complexity creates challenges in audit ability and controls. Bottom line: simpler is better.

Finally, since technology is the foundation of many of these processes, don't forget what these systems can and can't do. Many of the technologies that now make up the IT infrastructure in corporate America were developed when compliance issues were not a top priority, and when content didn't come in as many types as it does now. This is a critical weak spot.

At the most basic level, many companies continue to back up content when they should be archiving, managing and destroying it. They surely learn the difference when there's a court order mandating a huge search at short notice. On a broader scale, the archival systems many companies have in place simply can't handle the kind of search and retrieve functionality needed to quickly respond to requirements that a judge might deem routine. Going further, even fewer technologies can deliver a comprehensive platform for addressing the global issues surrounding archival, compliance and legal discovery with the flexibility to address "what's next."

Testing the Limits

Measuring Your Company's Compliance Readiness

Like most organizations, you take compliance seriously. The more complicated reality is that even with general policies and some technologies in place, many organizations aren't doing enough or enough of the right things to protect themselves for the growing risks associated with managing electronic records.

Here's a quick test to gauge your company's compliance readiness. No one's looking over your shoulder, so be honest. Score it any way you like, but we recommend a scale of 1 to 10 points on each answer, with a 25 for the bonus question.

1. Do you classify data contained within business systems in such a way that it is easily accessible—for example, by retention periods per data types?
2. Do you have compliant non-destructive media in place?
3. Does your electronic archiving policy include content generated via e-mail, IM and MS Office?
4. Are the archival policies explicit per groups?
5. Do you have a supervisory review process for e-mail/IM communications for some/all users?
6. Do you have checks and balances for all of the above?
7. Are you able to suspend retention cycles/put records on legal/litigation hold and electronically manage your legal case holds?
8. Do you run tests for records recovery, including audit logs?
9. Is all your data that needs to be compliant—for example, relating to financial transactions—readily accessible online for back-office reconciliation and other front-office business functions?
10. Is senior management (CEO, CIO, CFO, CCO, corporate counsel) actively involved in your company's compliance and IT alignment strategies and operations?

And for the bonus question:

Does your company have the capability to rapidly develop value-added front office applications (for example, dynamic web publishing, portal integration, decision systems support) from its compliance data?

Compliance Readiness Scorecard:

- 80 Congratulations: Your company is a leader in the field
- 70 Very good: Your company has an excellent state of readiness
- 50 OK: Your company is toeing the line
- 30 Not good: Your company is at high risk for non-compliance
- 20 Bad: Your company needs to drastically overhaul its compliance practices

Best Practices

Of course, there are still plenty of things organizations can do. Despite the very different terrain, many of these best practices haven't changed much. Maybe it's because compliance is like old-fashioned investing: It's all about the fundamentals.

Exhibit real leadership: Failure to ensure true and effective records management and regulatory compliance represents a failure of management. Even the best policies and technologies won't work without companywide adoption and buy-in, and it is management's job to get it.

Make compliance and governance a no-brainer: Wise companies will build and support a high-visibility compliance competency training program that has the authority and resources needed to develop, implement and enforce participation across all levels. Roles, responsibilities and accountability must be clearly defined.

Keep it transparent: Make it as easy as possible for employees to retain, preserve and archive all the necessary content, but also ensure that your company has the ability to detect policy violations and do what is legally required if and when that happens. The problem won't go away if you don't.

Prioritize the content, not the content type: The medium doesn't matter; the fact that one relevant piece of content was in e-mail form while another was in an SAP report makes no difference in the final analysis.

Put the right tools in place: Conduct a thorough needs analysis and ensure that the technology can do the job. The infrastructure must be scalable; it must have the ability to handle multiple content types; and it must have the capacity to meet the records management and regulatory compliance tasks that come down the pike today, such as global risk and e-mail search-and-retrieve.

Stay ahead of the curve: Accept that we are in the midst of ongoing paradigm shifts in the way we perceive our technological infrastructures, as well as the applications and data they are designed to deliver. Technology evaluation is routine in most corporations, but balancing it with compliance needs is a new twist. That's why many companies often believe that their backup processes are sufficient; measured against compliance directives, they're usually not. For example, a compliance and archival strategy with data expiration policies is a huge waste of time if the expired data continues to exist on multiple back-up tapes, as well as at disaster recovery sites.

These processes have to be reviewed with an eye toward managing both the regulatory requirements and the risk associated with the content. Similarly, the underlying operating systems might allow security breaches that, in addition to other problems, violate compliance policies. Bottom line: The entire technology infrastructure, from the smallest applet to the largest server, needs to be assessed along strict compliance metrics. At the same time, it's vital that companies implement both continual process improvement and reliable audit capabilities. We're long past the point where silos can continue to grow virtually unchecked, each with its own domain. Build a single platform that can be expanded, then evolve when necessary. This will allow technologies, processes and business needs to keep pace with incoming regulations and changing market conditions.

No company will ever say it *doesn't* take records management and regulatory compliance seriously. Now, most of them actually mean it. Still, there's no absolute scale of corporate compliance, just as there's no completely right or completely wrong way to do things. Far from being just another chore for the IT shop, compliance needs to be embedded in the corporate DNA. That's when things happen the way they should. ▮

AXS-One Inc. (AMEX: AXO) is a leading provider of high-performance records compliance management solutions. The award-winning AXS-One Compliance Platform enables organizations to implement secure, scalable and enforceable policies that address records management for corporate governance, legal discovery and industry regulations such as SEC17a-4, NASD 3010, Sarbanes-Oxley, HIPAA, USA PATRIOT Act and Gramm-Leach-Bliley. It delivers digital archiving, business process management, electronic document delivery and integrated records disposition and discovery for e-mail, instant messaging, images, SAP and other corporate records. Visit AXS-One at http://www.axsone.com.