10 Plain Truths About Risk Manage

By Marcia Jedd

Locking down enterprise content, in many respects, is as elusive as herding silverfish. While managing risk has always been one aspect of good document and records management; today, reducing risk around enterprise content—from security breaches to e-discovery—is the heady stuff of headlines. More is at stake than ever before for not having a strong grip on risk management, given the high costs associated with e-discovery in a litigious and regulated world.

Lack of a solid risk management plan, combined with poor ECM project planning and implementations, are top reasons why ECM systems and corporate initiatives leave data vulnerable, says Arvind Krishna, senior principal with ECM Advisory Group. "Risk management is really a process. It's about proactively balancing the operating and economic costs of protective measures to protect ECM systems and content."

Blame most of the failure of ECM endeavors in this area around bad strategy, says Kyle McNabb, principal analyst with Forrester Research. "Discovery is a huge pain point. Discovery only materially impacts a small portion of people throughout the organization, yet technology is intended to be used by large masses of people and that's where the disconnect is."

McNabb says many enterprises are at crucial decision points around figuring out or otherwise improving upon their enterprise-content risk management strategies and policies. "Many focus on going and fixing the risk problem and they soon realize just trying to focus on risk may not help them improve the bottom or top line or deliver a better customer experience," McNabb says. Rather, most enterprises, he says, are realizing they need to integrate risk

What's in your risk management-enterprise content tool kit? More than IT and dusty policies, experts say. How to identify and mitigate risks and develop a path to proactive risk management

ment for Enterprise Content

management activities into enterprise-wide drives to do things like improve productivity or deliver a better customer experience.

"Most organizations realize they have to define what's reasonable to them," McNabb says, adding, "A lot of legal groups we speak to are getting involved. Technology and the way we use it is changing dramatically and enterprises can't keep up. Unfortunately, the enterprise IT environment will be in a catch-up mode for the foreseeable future."

Given these challenges, what can the enterprise do to identify and mitigate risks around mounting volumes of enterprise content while developing a path to proactive risk management? Here are some ideas from the experts.

#1 Know your drivers in assessing content risk.

First, Krishna says it's important to look at the business drivers for ECM systems. These tend to fall into four major areas:

1. Compliance and risk reduction
2. Collaboration and workflow capability to increasing individual and group productivity
3. Business continuity and disaster recovery
4. Improved efficiencies and customer service through reduced operating costs

Specifically in relation to risk reduction, Krishna points to the adoption of IT security principles such as those by the government's National Institute of Standards and Technology that advise putting in place controls around management, operational, and technical areas. Technical controls like encryption and firewalls receive attention though inadequate operational controls and the day-to-day administration of technical controls often create vulnerabilities. Strong management controls are needed to tie all the aspects of security together. "Security threats can certainly expose vulnerability in a system," Krishna says, noting the importance of having proper user authentication processes in place.

#2 Identify risk.

Risk can come from anywhere: catastrophic, political or financial events, situations that affect company reputation, customers acquired or lost, etc. Risk around enterprise content is something that's always been there, says Frank Wu, managing director of Protiviti, a risk consulting firm, but awareness is escalating at higher levels within the organization, "There's a growing sense of awareness around risk management and what to do about it."

Risk is pervasive in most aspects of a business, Wu says, noting that sources of uncertainty arise from the business environment and business processes, both affecting the viability and execution of the business model. As well, there's always going to be uncertainty around decision-making when relevance and reliability of information isn't solid.

Highly regulated industries, for example, are most concerned with risk around compliance. "If you try to chase changes in the rules, you'll always be playing a game of catch up," Wu says. Any organization, he says, needs to look at how risk is addressed in company policies and generally speaking, IT, legal, and operations should all be able to agree on what the top risks are and how to mitigate them. "You must have the right policies and the people must understand the processes around risk. The right systems and data are needed to support processes."

#3 Analysis outreach.

First, identify potential areas of risk, do the analysis and determine the expected value of those events. "If the event were to occur, what impact would it have," Krishna asks. "Organizations have to manage risks by being proactive about the potential risks facing them. Have brainstorming sessions with your team on potential risks," Krishna says.

Consult with your office of general counsel to help identify risks, advises Rich Baily, vice president of Xerox Business Process Services, "Find out where most risk is coming from and address those concerns with whatever policies you put in place. Most of the discussion has been around e-discovery and records management as it relates to e-discovery and compliance concerns, but do not ignore disaster recovery and business continuity in risk mitigation." That broad view of risk will ultimately allow the organization to develop a policy around risk management. "Then, implement it and implement it consistently," Baily says.

#4 Business process improvements.

Frame your development of risk management practices around how it can improve business processes, Baily says. Roll up business process initiatives, such as implementing a new online enrollment system for a healthcare organization, within the broader context of risk management.

Many organizations, from the institutional to small, private companies, are seeing the light in going toward an all-electronic environment, away from paper. While well-documented policies and procedures around records management certainly help manage and mitigate risk from the legal and business continuity standpoints, many organizations need help in that area today.

Records management often gets short shrift in project planning because the dollars don't flow there, Baily says, make the business case that the project supports improved processes and savings. "When you can implement a records management process or system that also supports a line-of-business and makes it more efficient, then multiple dollars can be found. You need business owner input and ownership."

Business process improvement—and likely the reduction of any e-discovery costs—comes with the territory of good records management. "If your records retention schedule hasn't been updated in the last two years, or if you don't have one, hire a qualified consultant to update or create one for you," says Anne Tülek, president of Access Sciences, an ECM and RM consultancy.

#5 Calling in records pros.

Hire a company with appropriate professional liability insurance and a suite of knowledgeable team members—not an independent contractor, Tülek says. "Law firms have recently entered this market en masse, while information management firms have been doing this kind of work for quite a while."

Again, in-house or outside legal department should be involved. "Regardless of who does it, have your legal department validate the schedule. The balancing act here: buckets large enough to allow you to have a reasonably low number so that people will actually use them versus buckets that are grouped in a way such that items with similar retention duration requirements are together, so that you don't keep things for longer than you reasonably need to."

Getting a grip on risks around enterprise content ***doesn't happen overnight.***

No matter the type of ECM system, Tülek says risk management capabilities and enterprise content strategies need to happen within the context of ECRM, enterprise content and records management, an emerging practice. "Very few initiatives are happening without a concurrent or highly integrated ECRM software suite in the project priority mix."

As all good records managers know, Tülek cautions the enterprise to avoid excessive archiving, which is a good reminder on managing risk, too. "Archive only what you need. This implies that you have practices and systems in place to know what you need, which gets back to the apparent Catch-22: how to stop the bleeding on proliferation of unmanaged content and storage versus how to draw a line in the sand to carve a path forward for effective management of information."

#6 Study user behavior: people first.

Increasingly, risk management policy and practices must be set within the context of people and how they work. This means putting the greatest effort into integrating risk management policy into how people in the enterprise use content, McNabb says. "Look at how they use content, documents, spreadsheets, etc. Then look to define policies that complement how people work and mitigate risk concerns."

Don't overly rely on software tools, McNabb cautions. "For a lot of organizations the driver of these initiatives often sits in IT in what usually results is 'let's go beef up infrastructure, the tools.'" For example, if management has a policy on purging emails and R&D needs to go back through emails from years ago for their product development purposes, then management might want to either change its policy or have R&D create their own repository for those emails.

#7 Departmental approach still rules.

Traditionally, the enterprise has been concerned with high value content that's departmental in nature—engineering drawings for instance, notes Mike Alsup, president of Gimmal Group, an ECM integrator firm.

"And it was less about unstructured content on shared drives and email—that's where the real vulnerability is about compliance today." While Alsup says that department or functional approach shouldn't be overlooked today, you still need to manage these systems in an integrated fashion.

Indeed, many enterprises have gone away from jumping on the one-size-fits-all approach of single ECM systems. Baily says: "Now companies have come to the realization that doesn't have to be their approach. You don't need monolithic ECM systems. Departmental applications are still important," he says.

With departments in mind, make sure you have ERM (enterprise records management) technology to support the company's electronic records management needs, Tülek says. "Even if you have an up-to-date retention schedule, invest in getting people out into your business units and departments who can help them translate their work processes into meaningful information buckets," Tülek says, noting categories will vary by department and organization culture. "Some will want lots of specificity; others will want large, sweeping buckets. Help the groups translate what you create for them into their email management system, shared-drive folder structures, and desktop filing systems."

#8 Email, king among unstructured content.

Email is perhaps one of the biggest threats around locking down content because of the sheer volume and lack of being tethered to ECM systems. There's also the dimension of whether users should be required to file documents to repositories, Alsup says, which raises questions around the tools and support that need to be offered to users.

Experience has shown users aren't able to reliably archive their email while the volume of email is sure to overwhelm auto-classification systems, Alsup says. "If it takes three minutes to classify an email, they'll just delete it." And instant message archival is another open mine field.

Whether or not content is tied to an ECM system, educate users and help them understand what a record is, Tülek advises. Given email's high volumes, it remains the most popular target of ECRM-related technology initiatives currently. " For email, provide employees with guidance on how to organize their email into three or four buckets based on what they think the status of the information is, whether record, working document, might become a record, or trash."

Both Alsup and Tülek cite Microsoft Office SharePoint as helpful to compliance, e-discovery, and otherwise corralling enterprise content, rendering user interfaces and content storage. "The vast majority of our clients are dedicating resources to the design and implementation, or the control and redesign of this tool, as most of them are Microsoft shops," Tülek says, noting for better and in some cases, for worse, these enterprises view it as a way to quickly enhance their IT capabilities for managing information.

Tülek adds discovery management tools and hold-order-management automation are on the minds of corporate counsel. "These are high priorities for companies looking for quick course correction on the collection process and the management of collections," she says.

#9 Years in the making.

Getting a grip on risks around enterprise content doesn't happen overnight. While one year to eighteen months is often a typical timeline for ECM initiatives through the implementation phase, for organizations making major drives to integrate risk management into new or improved content systems, expect a far greater amount of time.

McNabb says: "When you really pay attention to the business context, the way business processes and people work, IT leads to better policy definition and this means much longer implementation and rollouts." He says most companies need a minimum of three years and even up to five or more years to see the broader implications of risk management built into ECM systems and business processes.

#10 No single cure-all.

There is no one-stop-shop approach to risk management of content from a consultancy or system, experts say. "Risk consultants tend to focus on the risk side. System integrators haven't really built up the skills in a holistic view of risk management," McNabb says.

Wu says: "Depending on the size and industry of the company, more organizations have the risk management hat being worn by multiple senior executives and in some specific environments; they'll create a focus or titles directed toward that."

In their quest for effective development of risk management practices—those that are thoughtfully integrated with enterprise content and records management (ECRM)—many organizations actively seek expert help. "There are a lot of organizations really looking for outsiders to tell them how long to keep paper or electronic versions of documents," Baily says.

While content and records management with the watchful, big-brother eye of risk management is a necessary but tough pill to swallow, enterprises are taking measures today. Some enterprise may view it as a necessary evil, but others can find opportunity and even competitive advantage with proactive risk management. "There's huge upheaval going on around the topic but the truth is, people want it," Alsup concludes.

Marcia Jedd (www.marciajedd.com) is a Minneapolis-based marketing consultant and writer.