I've Seen the Future of ECM, and It's Not ECM

By Joe Shepley | *Dec 21, 2015*

Published by CMSWire http://www.cmswire.com/information-management/ive-seen-the-future-of-ecm-and-its-not-ecm/

The balance of power in ECM is shifting away from IT and records management and towards information security.

Information security makes for a far better owner of enterprise content management (ECM) than records, IT or legal — all of which have been the owners du jour among talking heads like me over the last 15 years. All of the latter failed to gain the organizational support needed to institute the meaningful organizational change that allows ECM to flourish.

The Business Case is Already Made

Without the executive support and funding, ECM perennially seems to land as the number three enterprise priority … except that every year, number one and two change without ECM ever moving up (or getting done). There are a lot of reasons for this, not the least of which is that most people have no idea what ECM is.

But in my opinion, ECM has trouble gaining funding and support because IT and RM haven't built compelling enough business cases for it. Worst case, they rely on fuzzy things like time saved searching for and working with documents, often using very generic and amorphous terms that executives don't buy. Or in the best case, they tie ECM's value to tangible business improvements, but scare execs with the complexity of the organizational change required. Execs would much rather fund more straightforward initiatives that "do more of what we already do" than a big transformation.

At most large organizations, CISOs already have funding and support — and this funding and support is earmarked for managing information to keep it secure. Traditionally this meant building a better moat to keep bad actors out and more effective monitoring to keep the crown jewels inside the firewall. But over the last 12 to 18 months, I've seen CISOs shift to include managing information more effectively to reduce the severity and impact of breaches when they do happen. More on this in a minute.

Orange Jumpsuits, Pink Slips

The other reason why the CISO is a better owner for ECM than IT or RM is that their success (or failure) can determine whether the CEO will be wearing an orange jumpsuit … or at least be handed a pink slip.

No CEO ever went to jail or got fired because people spent too much time searching for documents. And so when the CISO tells their CXO peers that something needs to be done, it has a much higher likelihood of getting done than when RM does. And even though IT has the CIO or CTO at the top, at most organizations, it's a struggle to get the CIO/CTO to understand ECM, let alone get them to stick their neck out with the rest of the C-Suite to get it funding and support. Which is why it's perennially a number three priority.

Rubber Hits the Road

I had some vigorous debates about my thoughts on the CISO's role in ECM after the last post, so I know people may be wondering what a CISO-owned ECM would look like. To give you a better idea, let's walk through some of the core scenarios in how a CISO would address ECM

Let's assume this is a F1000 organization that has sensitive data (PHI, PII, intellectual property, etc.). Any CISO worth their salt no longer believes that they can prevent all breaches — in fact, most will tell you that it's not a matter of if, but when … and that they're likely being breached as we speak, but just don't know it yet. Instead, their effort to protect corporate information has two prongs: defend (build better walls, moat) and minimize impact. It's the latter that has the significant overlap with traditional ECM, because the best way to minimize the impact of a breach is to have less sensitive data in the first place (and to know what you have and where so you can understand the extent of the breach quickly).

Given this, the CISO will be concerned to determine where sensitive data is stored, so that they can: 1. manage it better where it is or 2. move it somewhere where it can be better managed. In the process, they also want to remove redundant, obsolete and transitory (ROT) information because it makes their job of managing sensitive content harder. Managing sensitive data better has typically meant making sure access rights are aligned with policy, applying information rights management (IRM) or data loss prevention (DLP) to prevent end point breaches, but it can also include giving users a better interface with more robust capabilities so that they use the proper system rather than resorting to workarounds.

In addition, the CISO will be concerned with making sure their organization has a rationalized portfolio of applications, because the more systems you have, the more risk you carry.

Here's why: picture the typical F500 P&C insurer or financial services organization, where you are likely to find at least 500 to 1000 enterprise applications in place (in some organizations this number will be much, much higher). A significant portion of these are aging, homegrown dinosaurs that, even if we could render them secure by today’s standards, would require a tremendous amount of effort to do so. And beyond the effort to secure them, having this many applications in play makes breach detection difficult because you have so many systems accessing data on a regular basis — it’s harder to determine when one of them has been hijacked by a bad actor than if you had a more rationalized portfolio.

The Final Word

More debate is needed about whether the CISO is the right owner for ECM. But what's clear to me now is that ECM, as it’s traditionally been done by IT and RM, can make a huge impact to the CISO’s efforts to minimize the impact of breaches by helping them manage information more effectively. And the CISO, unlike RM and IT, often has the organizational support and funding to get things done. This could explain why I’m seeing more ECM projects happening with the CISO as sponsor or key stakeholder. To me, this makes the case for the CISO owning ECM a case worth making.

About the Author

Joe Shepley is a strategy consulting professional living and working in Chicago. In his current position as Vice President and Practice Leader at Doculabs he focuses on helping organizations improve how they manage information using technology and processes.

Submitted by Ruth Edge, Cardinia Shire Council