Trends to watch

How to keep your documents secure and under wraps

INTERVIEWED BY JAYNE GEST

David Cramer
Manager, Business Development,
Legal & Professional Services
Blue Technologies

216.271.4800, ext. 2561
dcramer@btohio.com

Security is a growing concern for all employers, but law firms and professional services organizations are at the forefront of this, as these businesses adopt security tools and practices that change how sensitive and/or confidential documents are stored, created and shared.

"New security models in document management systems and security features that are applied directly to the document have grown in popularity in legal organizations," says David Cramer, manager of Business Development in Legal and Professional Services at Blue Technologies. "And it's certainly something that may trickle down into other verticals and be utilized by other businesses."

Smart Business spoke with Cramer about corporate document security trends.

WHAT'S NEW WITH HOW DOCUMENTS ARE STORED, INCLUDING WHO HAS ACCESS?

In the past, document management systems have been set up under an open security model. Everyone with access can see any content that resides the system — even if it doesn't deal with their particular client or workload. Sometimes this is called an optimistic security model.

Now, some law firm clients are saying, 'We don't want this particular matter to be visible to anyone outside of the team of attorneys, paralegals and legal assistants that are working on it. Nobody else in the firm should have access.' Therefore, businesses may need to implement a pessimistic or need-to-know security model by adding security functions through their current document management vendor or layering a third-party security solution over the document management system.

Corporate customers, such as those in financial services and health care, may require professional services to go through an IT audit to be sure security measures have been applied, including restricting content. While these audits aren't new, some corporations are asking for verification of specific practices.

Large organizations also have started moving away from an open security model in their document management system. They're restricting content within different departments, such as the corporate legal department and/or compliance.

HOW IS SECURITY BEING ADDED TO THE DOCUMENTS THEMSELVES?

Document cleaning tools — created after a savvy Microsoft Word user used metadata to discover Microsoft's annual report was created on a Mac computer — are growing in popularity. If an older document is repurposed, these tools clean the metadata, so people cannot see prior edits. Any document that goes outside of an organization can be cleaned via a desktop computer, laptop or mobile device before it's sent over email or through a secure file sharing tool. This cleaning can be done automatically or by giving the sender an option to clean or not clean the document.

Another useful tool is safe sending, which is used to prevent the Outlook oops — sending a message to the wrong person because a different email address popped in when the sender started typing the recipient's name. If an employee is sending an attachment to an external party, the email would be flagged, and a dialog box would pop up and ask, 'Here is the email address it's going to, is that correct? Yes or no.'

WHAT ELSE WOULD YOU LIKE TO SHARE?

It's important to remember the human factor. Last fall, a large law firm drew criticism because an employee didn't utilize the proper technology — in this case, redaction software. Someone transferred a Word document to a PDF, blackened the language in the PDF and filed it with a court. When a reporter requested the document, copied the language and pasted it into Word, the redacted language became visible. In the world of business, it's not only having the right technology tools; it's training to ensure true user adoption is adhered to throughout the organization.

In addition, some vendors are using artificial intelligence (AI) to monitor cybersecurity attacks and determine if it's an external or internal threat. The AI examines technology users to understand their patterns and workflows and flag abnormalities — behavior changes like downloading a massive number of documents — so administrators, security, compliance, or risk officers can further investigate. ●