No company can afford the backlash associated with a data breach.

It’s not just the fines, it’s also the monumental impact to the company’s reputation and potential hit to customer loyalty that can ultimately prove difficult for even the largest organizations to overcome.

Unfortunately, data breaches and ransomware attacks are seemingly regular events with new occurrences continuously making headlines. In fact, in the first 10 months of 2017 alone there were a reported 1,120 breaches and more than 171 million records exposed — a significant jump from the 36.6 million exposed records in all of 2016.

As such, it’s time for organizations to step up their approach to protecting enterprise data. This can be a daunting task considering the complexity of today’s operating environment. After all, organizations of all sizes are far more mobile — often relying on a bevy of apps capable of generating and accessing mountains of data, often stored within the cloud. However, no matter where data exists — in private or public clouds or both — a comprehensive enterprise content management (ECM) strategy will protect both data and users.

Significant pressures exist for the business to comply with tight regulations and standards monitoring access, generation, and long-term data retention policies — especially for organizations operating in industries such as financial services.
healthcare, and telecommunications. As hackers become increasingly sophisticated and the number of attacks continues to climb, the risk of non-compliance also becomes a growing concern.

Companies need to be able to retain and effectively secure data in accordance with compliance and regulations. They must also manage the support for new regulations that require the retention of complex business records — often containing structured and unstructured data in the same records — to comply with privacy and auditing requirements. The issue only compounds for global organizations that operate in countries where failing to comply with regulations such as the General Data Protection Regulation can prove catastrophic.

THE ROLE OF ECM

ECM is a holistic approach to data management. It incorporates storing, sharing, utilization, and management of all information across departments within an organization. By integrating strategy and technology, it brings together structured and unstructured data, which then empowers team members to work efficiently.

For ECM solutions to play a meaningful role in compliance, they must have robust security that encrypts data and prevents unauthorized access. For instance, ECM solutions should adopt leading standards for security in records management such as the Department of Defense (DoD) 5015.2 standard for records management. This ensures rules-based authentication with delegated administration, while enabling different lines of business to effectively manage user access independently when necessary, so that personally identifiable information, for instance, stays under the proper department’s control.

The ability to track and manage access is critical. The ECM solution should enable information from multiple applications to be accessed by authorized users both inside and outside the organization.

And the right ECM solution, while meeting compliance, access, and security requirements, will not slow efficiency, productivity, and collaboration. This is not an easy ask, considering the complexity of today’s world of information sharing among cross-departmental teams, both inside and outside the organization.

The effective integration of software and hardware into one content management solution will fully protect and secure data, while also improving user access and workflow efficiency.
CASE IN POINT: A MED DEVICE COMPANY’S EXAMPLE
A Midwest medical device provider offers a good example of how an integrated ECM solution can come together to meet compliance and security standards, while improving workflow and productivity.

The company was searching for a HIPAA-compliant way to manage confidential document flow. It needed a digital imaging solution that could track users, simplify workflow, and keep confidential information secure. While security and confidentiality were understandably top priorities, the medical device provider also wanted a comprehensive solution that was easy to use, especially when it came to emailing scanned documents.

The company ultimately implemented new multifunctional printers (MFPs), as well as an ECM solution that limited access to authorized users, and that simplified the scan-to-email process. As a result, it now has a means of effectively tracking usage, automatically populating e-mail fields, while granting access only to authorized employees via RFID cards.

HOW KYOCERA CAN HELP
As a total document solution provider, KYOCERA offers a portfolio of services and solutions to streamline output management. Well beyond providing hardware solutions, KYOCERA empowers organizations with ongoing management, optimization, and lower document costs — all designed to reduce IT department workload and minimize environmental impact. Its solutions turn otherwise complex data and document workflows into simple, efficient processes.

Peter Fretty is a freelance writer and editor, who specializes in technology and market development.