opentext™

WHITE PAPER

Promptly detecting insider threats: Best practices for law firms and corporate legal departments to mitigate the financial impact of a data breach

This position paper explores the nature of security threats and, in particular, insider threats, including the weak links in security that arise at the document or content level. It discusses industry rules and regulations governing data security, including the ethical obligations around content security, and provides security measures that allow organizations to promptly detect threats, escalate warnings and eliminate access at the document level when a breach is detected.

opentext™

Contents

opentext™

Lawyers are, unfortunately, notoriously poor at managing data security. According to the American Bar Association's 2018 Legal Technology Survey Report, 23 percent of respondents indicated that their firms had experienced a data breach.[1] Given the increasing recognition of these risks, 48 percent of law firms had been subject to a data security audit at the behest of at least one corporate client over the preceding year.[2]

Data breaches and cybersecurity threats targeting both law firms and legal information residing within corporations are a major challenge facing the legal profession, both in terms of liability and professional responsibility. As custodians of sensitive and high-value information, legal professionals amass volumes of sensitive client information. This includes strategic plans, regulatory filings, intellectual property,

employment contracts, privileged communications, case data, nonpublic personal information (NPI), personally identifiable information (PII) and other sensitive and confidential data—making both law firms and their corporate clients vulnerable targets for hackers.

Yet, news stories of organizations suffering a data breach take months or years to break. The average time for organizations to detect and resolve data breaches is about nine months. Though external threats get much of the press, what tends to be less public are the threats from within—when insiders steal or misappropriate sensitive or valuable company data. This is because they are often undetected until months or years later, if at all, though they comprise a majority of cyberattacks. The average time it takes for a company to identify that a data breach has occurred is estimated at 197 days. Another 69 days elapse, on average, before a breach can be contained. Those companies that manage to speed their response time save considerably. Companies that contained a breach within 30 days saved an average of more than $1 million.[3]

Security threats from without and within

Organizations typically possess a wide array of information that may be of interest to external hackers or internal bad actors, including:

- Customer information, including PII, broader categories of personal data and financial information, such as credit card numbers.
- Information about the organization's finances, including details about potential sales or mergers.
- Protected health information (PHI) pertaining to customers or employees.
- The organization's intellectual property, trade secrets or proprietary information.
- Information about pending or likely litigation, legal claims or regulatory inquiries.

The security of this data can be compromised in several ways. External data breaches are the most well-known and easiest to prevent. They occur when an unauthorized individual infiltrates a data source and extracts valuable, sensitive or proprietary information. These breaches may be perpetrated by individual cybercriminals, groups of hackers or even foreign governments. They may occur through physical access to a mobile device, computer or network or remote access over an inadequately secured network connection. Ransomware attacks, malware and phishing attempts fall within the category of active external threats.

1 American Bar Association, 2018 Legal Technology Survey Report. (2018)

2 LOGICFORCE, Law Firm Cybersecurity Scorecard. (2017)

3 ibid

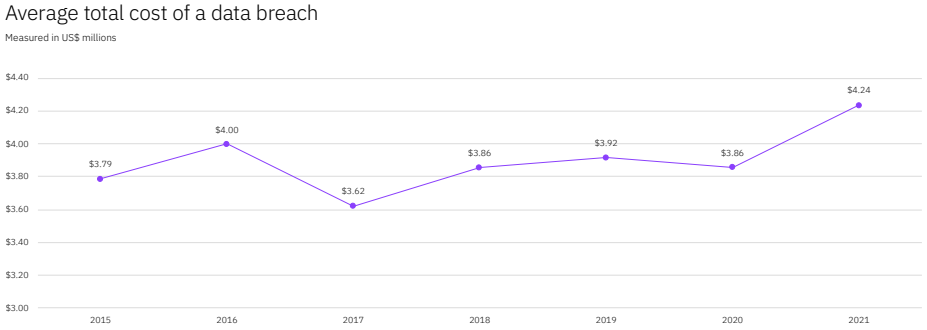
A type of threat that is common but harder to detect are internal threats. Information may be compromised by insiders: employees, contractors or vendors who have been granted some access to the organization's data but whose interests are not aligned with those of the organization. Those insider attacks frequently evade detection since insiders come bearing valid credentials and are often expected or even required to access sensitive data during their work.

In 2021, the average cost of a data breach was highest for healthcare organizations for the 11th year in a row. Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5-percent increase.[4] In this industry, the most prevalent mistake is sharing sensitive information with the wrong person, though improper disposal of secure data. Misplacing data assets is also a significant risk. Publishing errors and misconfigurations of software that lead to exposure also abound. Beyond these unintentional blunders, the intentional misuse of data, whether motivated by convenience of access or malice, is also a risk factor.

But the healthcare industry is not alone. Insider threats are on the rise across the board. Among IT professionals in all industries, 59 percent of those surveyed in a recent report stated that their organizations had experienced an insider attack over the previous year.[5]

Regardless of how they occur, data breaches are enormously costly. The survey found that the average total cost of a data breach increased by nearly 10 percent between 2020 and 2021, the largest single-year cost increase in the last seven years.[6]

Estimated cost of a data breach

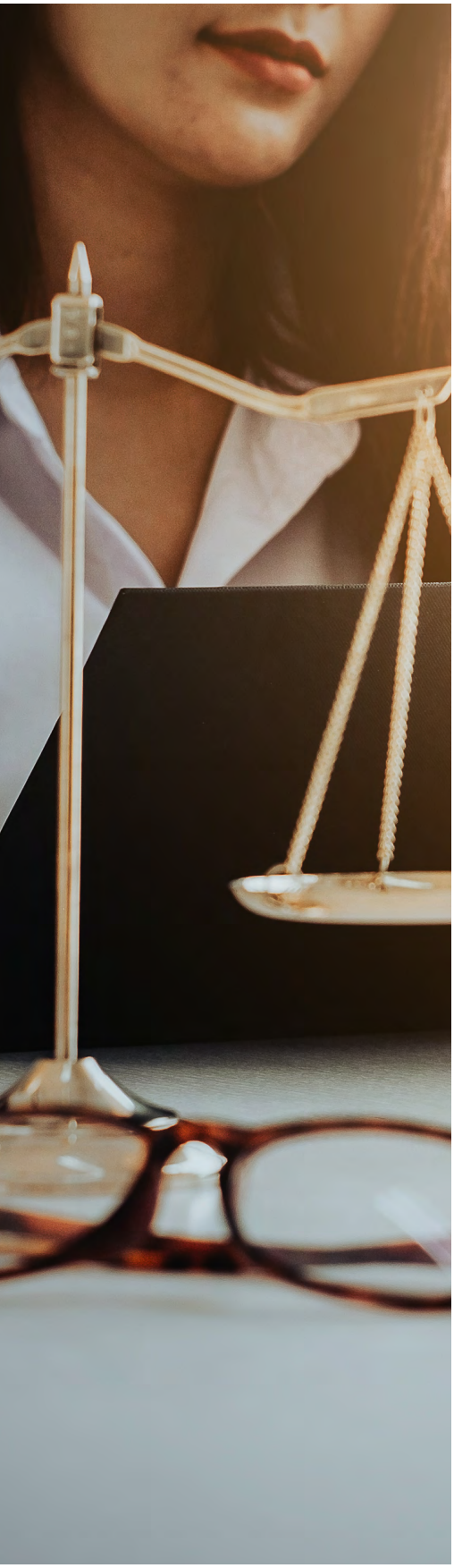


Source: Ponemon Institute, Cost of a Data Breach Report. (2021)

4 Help Net Security, 2021 was the most prolific year on record for data breaches. (2022)

5 Bitglass, 2019 Insider Threat Report. (2019)

6 ibid



External demands for enhanced security measures

Legal professionals face pressure from all sides regarding security measures. That pressure stems from three major sources. First, a complex array of laws, rules and regulations, including the recently updated American Bar Association (ABA) Model Rules, as well as ethical opinions interpreting those rules, both of which impose various security requirements and create liability for noncompliant organizations. Second, the courts, through their opinions, take organizations to task for their failures. Finally, the court of public opinion and the competitive stakes imposed by clients and customers who will take their business elsewhere to ensure that their data is protected, which increases the pressure to a boiling point.

Note that the following discussion is meant to be illustrative rather than comprehensive. A given organization may be subject to stricter legal requirements than those catalogued here. It is best practice to analyze compliance separately under every applicable law or rule.

Legal requirements for data security measures fall under several categories, including data privacy protections, industry-specific rules for healthcare and financial information and breach notification rules.

Data privacy protections

As of 2018, all 50 U.S. states, plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands, had enacted data breach laws, some of which are more robust than others. But the current hotbed for data-related legislation is focused on expanding consumers' data privacy rights.

Recently, there has been vigorous interest in data privacy and the protection of a broader category of "personal data," as the European Union's General Data Protection Regulation (GDPR) came into effect. It was quickly followed by similar efforts, such as the California Consumer Privacy Act (CCPA). While these requirements are, so far, geographically restricted—applying specifically to residents of European countries and the State of California, respectively—they dramatically increase the scope of previous data protection laws.

GDPR: The GDPR espouses an incredibly broad definition of "personal data." Beyond the prior notion of PII, personal data now encompasses any information that might be used alone or in combination with other data to identify a specific individual. Thus, personal data includes not just names and identification numbers, but also IP addresses and demographic labels. The GDPR also imposes notification requirements, demanding that organizations report data breaches to a supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of" the breach.[7] The regulation imposes a harsh penalty for the failure to protect personal data: up to €20 million or four percent of annual global turnover, whichever is higher.[8]

7 General Data Protection Regulation art. 33.

8 General Data Protection Regulation art. 83(5)

CCPA: California law requires businesses that own, license or maintain Californians' personal information to provide reasonable security for it. The law defines "personal information" as an individual's name, Social Security number, driver's license number, account numbers, medical information, health insurance information and usernames and passwords. The CCPA strengthened this law, effective Jan. 1, 2020, giving California consumers the right to access, delete and opt out of the sale of their personal information.[9] It also creates a private right of action for breaches involving Californians' personal data. Violations will be punishable, with a penalty between $100 and $750 per incident, plus actual damages and injunctive relief.[10] The California Attorney General may fine violators an additional $7,500 per violation in cases of intentional non-compliance.[11]

Industry-specific rules

Industry-specific cybersecurity provisions, such as the ones summarized below, often include requirements that companies promptly disclose the existence of any data breaches to affected or potentially affected customers.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) requires that organizations dealing with PHI implement physical and technical security protections to safeguard that information. The HIPAA Privacy Rule sets the standards for protection of medical records and health information.[12] The Security Rule, which guides the Privacy Rule's implementation, declines to prescribe any specific technological approaches, noting that "determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for their specific organization."

HIPAA's Breach Notification Rule requires that an entity that has experienced a breach must notify affected individuals within 60 days after the breach has been discovered

FINRA: Similarly, in the Financial Services industry, the Financial Industry Regulatory Authority (FINRA) requires that, "Every broker, dealer, investment company and [registered] investment adviser … must adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[13] As with HIPAA, FINRA's guidance does not dictate the precise methods by which organizations should protect their data.

GLBA: The Gramm-Leach-Bliley Act (GLBA) requires financial institutions and those that collect non-public personal information to explain their information-sharing practices to their customers and to safeguard sensitive data. This includes any personally identifiable financial information that is not publicly available, such as names, addresses, income, account numbers, payment history, purchase history, balances and the fact that an individual is a customer or consumer.[14] The GLBA mandates that financial institutions must "develop, implement and maintain a comprehensive information security program that … contains administrative, technical and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities and the sensitivity of any customer information at issue."[15]

9 Cal. Civ. Code tit. 1.81 § 1798.81.5.
10 Cal. AB-1130 § 1798.29.
11 Cal. AB-375 § 1798.105.
12 45 C.F.R. Part 160.
13 17 C.F.R. § 248.30.
14 16 C.F.R. § 313.3(n).
15 16 C.F.R. § 314.3.

opentext™

"The average time it takes for a company to identify that a data breach has occurred is estimated at 197 days. Another 69 days elapse, on average, before a breach can be contained. Those companies that manage to speed their response time save considerably. Companies that contained a breach within 30 days saved an average of more than $1 million."

Source: LOGICFORCE, Law Firm Cybersecurity Scorecard. (2017)

FERPA: The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. FERPA does not require educational institutions to adopt specific security controls. However, it does require them to use "reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective."[16] Violations of FERPA can lead to an institution losing its federal funding.

New York DFS: In New York State, to take one regional example, the Department of Financial Services (DFS) has established a cyber regulation that requires financial organizations to create a "robust cybersecurity program … designed to protect consumers' private data." In line with other regulations, the DFS cybersecurity rule avoids "being overly prescriptive so that cybersecurity programs can … keep pace with technological advances." However, it does draw some bright lines, mandating the use of multi-factor authentication, as well as encryption for data both in transit and at rest.[17] New York's DFS cyber regulation requires breach notification to the state superintendent within a remarkable 72 hours from the determination that a qualifying "cybersecurity event" has occurred.

American Bar Association Model Rules of Professional Conduct and formal opinions

In two recent ethics opinions, the ABA Standing Committee on Ethics and Professional Responsibility explained that lawyers not only have the duty to safeguard client data, but also must notify a client if their confidential information has been exposed through a data breach. These formal opinions follow Model Rules 1.1 (duty of competence), 1.6 (confidentiality of information), 5.1 (responsibilities of a partner or supervisory lawyer) and 5.3 (responsibilities regarding non-lawyer assistance), which all address how lawyers should handle the risks that accompany the benefits of using technology. Lawyers must study potential security measures for client data access and disclosure, implementing appropriate safeguards that may include the use of secure internet access to information, such as a virtual private network, complex passwords, firewalls and antivirus, anti-malware and anti-spyware software, security patches and updates, remote disabling and destruction features for mobile devices and data encryption. Finally, lawyers should closely supervise the conduct of third parties that handle client data, taking "'reasonable efforts to ensure that' the non-lawyer's 'conduct is compatible with the professional obligations of the lawyer.'" Some of these steps may include an audit of the vendor's security policies and practices and a review of the vendor's cybersecurity credentials.[18] The Standing Committee issued Formal Opinion 483, providing new guidance on a lawyer's ethical obligations after a data breach. Not only must lawyers monitor for potential breaches, they must also take steps to stop any breach and mitigate any damage that results. The opinion does not prescribe any particular actions, though it suggests that a best practice is adopting an incident response plan to guide the breach response. Finally, the opinion clarifies that a lawyer must promptly notify their clients, and potentially their former clients, of data breaches.[19]

16 45 C.F.R. § 99.31.
17 45 C.F.R. § 99.322 23 NYCRR 500.
18 American Bar Association Formal Opinion 477R, May 11, 2017.
19 American Bar Association Formal Opinion 483, October 17, 2018.

"The overall number of data compromises (1,862) is up 68 percent over 2020; the new record number of data compromises is 23 percent higher than the previous all-time high (1,506)."

Source: Identity Theft Resource Center, 2021 Annual Data Breach Report. (2022)

Court opinions

State and federal courts have penalized—or at least opened the door to penalizing—organizations for damaging data breaches in a variety of different ways. In an appeal before the Pennsylvania Supreme Court, the court held that an "employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system." Further, it ruled, "recovery for purely pecuniary damages is permissible under a negligence theory" so long as the plaintiff could establish a breach of a common-law, rather than contractual, legal duty.[20]

Many data breaches turn into class actions or multi-district litigations (MDLs). Indeed, of the 206 MDLs listed as pending on the Judicial Panel on Multidistrict Litigation's April 15, 2019 docket report, 15 directly involve corporate responsibility for damages related to data breaches. These include heavily publicized data breaches involving Yahoo!, Equifax, Uber, Marriott and Ashley Madison.[21]

Not all cybersecurity cases involve damages to the party whose data was disclosed. In another recent case, the plaintiff moved for spoliation sanctions under Federal Rule of Civil Procedure 37(e)for the defendant's failure to preserve evidence after the defendant lost "most of the information" that the plaintiff had sought in discovery due to a "cyberattack that affected its servers and personal workstations." The court pointed out that according to the advisory committee notes for Rule 37, "the rule calls only for reasonable steps to preserve." In fact, the rule specifically mentions that a "malign software attack" might be the type of uncontrollable event that could cause an excusable loss of evidence. However, the defendant wasn't automatically off the hook: the courts may still evaluate a party's anticipation of risks and any steps taken to protect discoverable information from loss. In this case, the court determined that it did not yet have enough information to ascertain whether the defendant had, in fact, "adequately protected against the risk of such an attack.[22]

Client and customer demand

Finally, corporate clients are insisting that their law firms (and their in-house counsel), maintain solid security practices for their most sensitive and valuable information. With a wide range of law firms and alternative legal service providers competing for the business of an ever-more-sophisticated and demanding client base, the competitive pressure to enhance data security should not be underestimated.

Remote work and digital transformation

Remote work and digital transformation due to the COVID-19 pandemic have introduced new challenges regarding security and increased the average total cost of a data breach. According to a Ponemon Institute report, remote work was a factor in causing a data breach for 17.5 percent of companies and the average cost was $1.07 million higher in these cases, compared to those where remote work was not a factor. Organizations that had more than 50 percent of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50 percent or fewer working remotely.[23] More than two dozen organizations experienced multiple data breaches last year, which is a result of increasing levels of remote work putting greater amounts of data at risk than ever before.

20 Dittman v. Univ. of Pittsburgh Med. Ctr., No. 43 WAP 2017 (Pa. November 21, 2018).
21 U.S. Judicial Panel on Multidistrict Litigation, MDL Statistics Report—Docket Type Summary, April 15, 2019. 27
22 Western Power, Inc. v. TransAmerican Power Prods., Inc., No. H-17-1028 (S.D. Tex. June 7, 2018).
23 Ponemon Institute, Cost of a Data Breech Report. (2021)

Detecting and pre-empting internal data threats with legal enterprise content management (ECM) security

All told, there is a tremendous push for organizations generally—and legal professionals in particular—to expand their data security measures. These efforts include two prongs: protecting against data breaches and insider attacks on the front end and enabling the prompt detection of intrusions should prevention measures fail. These complementary approaches reflect the dual focus of legal data protection requirements. They demonstrate a clear preference for protecting not just computer systems, but also the discrete data within those systems, through encryption both in transit and at rest. In addition, they monitor and promptly detect breaches and suspicious activity, without which there can be no timely notification.

Many organizations have focused their security enhancements on additional device-level security measures. This includes firewalls, password requirements and biometric screenings, in addition to ongoing efforts to eliminate the human-error component associated with many security lapses. Increasingly though, law firms and their clients are benefitting from adding a second layer of security at the document level. By combining these approaches, organizations can close security gaps and protect their informational assets against threats both external and internal.

Within law firms and corporate law departments, content management systems offer an easy way to insert document-level security measures, shielding and locking down sensitive and valuable Intellectual Property and company information from all forms of unauthorized and improper access. As newer legal requirements—such as provisions encouraging or requiring document encryption—demonstrate, this dual-layer protection is a best practice that will soon become a standard expectation.

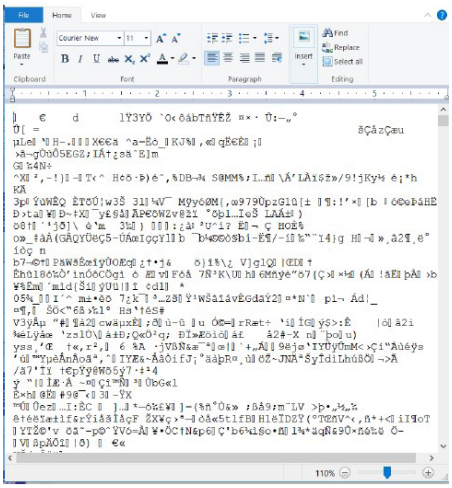
Guidelines for implementing legal content management security measures

The following best practices will enable law firms and corporate law departments to close the security gap left by strictly device-level measures using enterprise content management (ECM) systems.

Ensure the ECM incorporates standard security features

While most modern ECM platforms incorporate basic security features, users should verify that they are using those baseline measures. Confirm that an ECM provides:

- Two-factor authentication to log in to the ECM platform itself.
- Individual, document-level authorization for user access, sharing, editing and viewing of documents.
- Metadata security protection.
- Protection during information transmittal via secure socket layer (SSL) protocols.



Maximize document security with encryption at rest

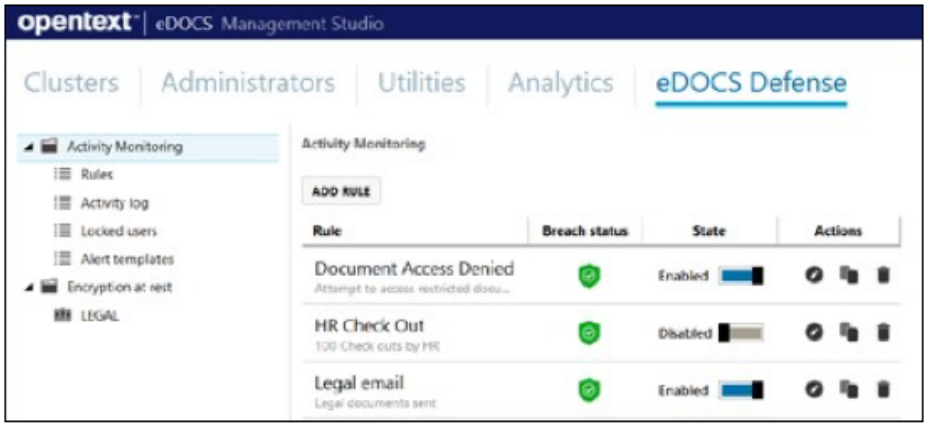
With encryption solely at the device level, sensitive information can still be viewed via server, opening the door to unauthorized document access by system administrators who have access to back-end databases. By encrypting individual documents at rest within the ECM, users can close that door, ensuring that not even high-level administrators can gain access to document contents without authorization from the ECM user interface.

Below is an example of encryption at rest at the document level and what IT or unauthorized users see when looking at a document directly in the database.

Document-level encryption protects content both on premises and in the cloud and continues to protect content that is backed up onto external media. This protects back-up data in house and ensures that content remains encrypted and inaccessible should a back-up device be stolen or hacked.

Proactively monitor for internal threats

Even authorized users can engage in unauthorized document access. That is the very essence of many insider data breaches. ECM activity monitoring detects these suspicious access patterns and sends customized alerts to designated individuals. This minimizes the time between improper data access and its detection, limiting the damages of such a breach. ECM activity monitoring can also automatically lock down sensitive documents, preventing access when an authorized user attempts to violate a rule or engages in unusual activity, perhaps by deleting multiple documents or accessing documents outside of business hours. Finally, activity monitoring includes creation of document audit trails, enabling organizations to reconstruct what happened during an attempted breach or inappropriate document access.



Configure realtime alerts to monitor unusual activity and lock potential abusers out of the system to avoid an additional data breach.

opentext™

Resource links

Protect your organization against a data breach with eDOCS Defense (vidyard.com)

eDOCS Defense | OpenText

Legal Enterprise Content Management | OpenText eDocs

Conclusion

With a growing number of data breaches initiated internally and an ever-widening regulatory landscape demanding heightened data protection, device-level security is no longer adequate to provide the tight levels of security that law firms and corporate legal departments need. Fortunately, legal professionals can now raise a secondary wall of defense against unauthorized document and email

access from internal and external threats, using document-level security protections in modern ECM designed for legal users. ECM security measures, such as document-level encryption and activity monitoring, allow users to both protect documents and emails from unauthorized access and detect unusual or potentially suspicious document activity, even by authorized users.

OpenText™ eDOCS Defense

OpenText eDOCS Defense, a document security module available within the OpenText™ eDOCS platform, enables organizations to encrypt sensitive documents and emails at the document library level, ensuring that only users authorized to access specific documents can view that content. While device-level encryption provides a back door through which users with server access can read or even copy sensitive information, leading to internal breaches, eDOCS Defense provides document-level encryption at rest, protecting valuable content on premises, on back-up media and in the cloud.

Even with authorized users, eDOCS Defense provides comprehensive activity monitoring that further mitigates the risks—and the costs—of an internal breach. Instead of waiting an average of nearly 200 days to discover that a breach has occurred, eDOCS Defense allows organizations to maintain document audit trails, immediately detect suspicious activity and initiate customized templated alerts. These alerts are flexible and configurable, allowing notification of designated individuals at various stages—such as 50 percent, 80 percent or 90 percent—of a potential breach. eDOCS Defense can also automatically lock down sensitive information, preventing authorized users from accessing content should they breach a rule or engage in suspicious activity as defined by the organization.

Because hackers work relentlessly to breach increasingly sophisticated security measures, data owners must work every bit as hard to stay ahead of them. eDOCS Defense adds the second layer of document-level security that valuable content deserves, protecting against both external and internal threats and detecting suspicious activity to limit any damage.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact