Flyer

opentext™

Information Governance—Challenges and Solutions

In this modern information age, organizations struggle with two things: having too much electronic data, and how to govern all that data. Each year, the speed of information accumulation (velocity) increases, and the associated problems continue to grow. Large amounts of electronically stored information (ESI) drive up the cost of storage, raise the costs and risks of NetIQ eDiscovery and regulatory noncompliance, negatively impact employee productivity, and raise the prospects of intellectual property theft and increase the chance of Personally Identifiable Information (PII).

Seven Primary Information Governance Challenges and Solutions:

1. Information Management
2. NetIQ eDiscovery
3. Regulatory Compliance
4. Security and Privacy
5. Storage Management
6. Defensible Disposition
7. Productivity

Here are seven of the top challenges companies face when it comes to information governance, and the solutions to those challenges.

1. Information Management

Information management requires the organization, retrieval, acquisition, security, and maintenance of all information—electronic and hardcopy—within the organization. Remember that country-specific data retention laws, the number of possible data storage repositories, and the breadth of potential data formats can further complicate and increase your costs.

In the past, one solution was to implement an enterprise content management system by which to store all of the electronic data. However, ECM solution software was not necessarily user-friendly, and users found ways to circumvent the rules (i.e., underground archiving) or by storing data on individual devices and storage media, thus creating silos of data.

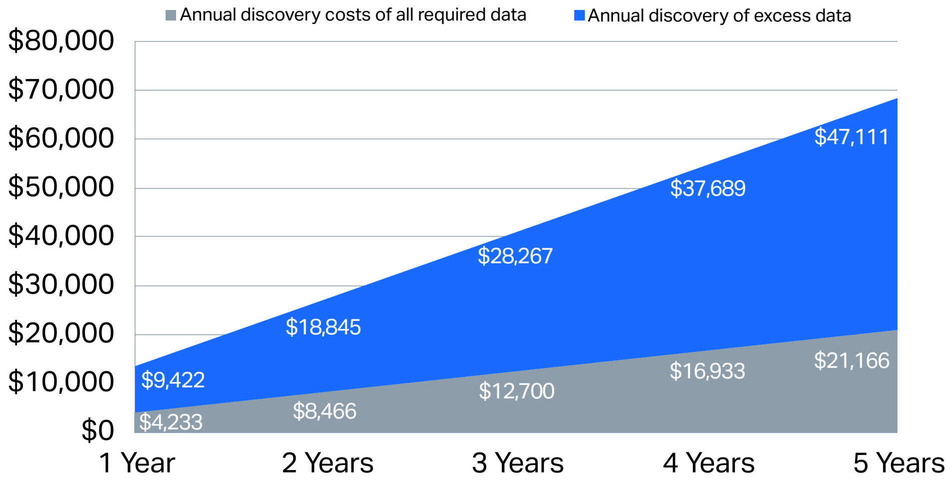
The Solution

To achieve true enterprise-wide information governance, organizations must implement information management automation. This solution removes the responsibilities of data storage and backup tasking from the users and ensures that your organization has enterprise-level information management.

2. NetIQ eDiscovery

The costs and risks of NetIQ eDiscovery by OpenText™ are greatly increased when your company does not properly manage its information. When faced with a lawsuit, and when you cannot find the information requested within the time allotted, or when the relevant information isn't available, your costs can increase exponentially. And there are those organizations that tend to over-collect data for an NetIQ eDiscovery request. The increase in costs comes from attorney's fees, when they must review all of the collected data to determine the relevant data to the lawsuit.

Discovery Costs and Estimated Savings per Employee



Over-collection can add millions of dollars to the cost of defending just one case, while an under-collection situation could cause you to lose the case before it even goes to trial due to spoliation and hidden evidence.

The Solution

An effective information governance program is the key to reducing both the cost and risk of NetIQ eDiscovery because it means that when the time comes, your organization will be able to retain the correct data for the correct time period. Furthermore, because your organization is using the right software, the performance of NetIQ eDiscovery will be quick and easy, which means that costs will be reduced as well. This graph shows the cost of discovery over time for one employee. The gray shaded area shows the cost of discovery for the data that should be kept because of litigation hold, regulatory retention, or value to the business (31%). The blue area of the chart shows the cost of discovering unneeded or valueless data. The main point is that retaining data that is not subject to retention by law or to the running of the business can pose a huge cost liability in NetIQ eDiscovery.

3. Regulatory Compliance

No matter what country you're in, you can be sure that there is some form of regulatory requirement on keeping records that directs what organizational information must be kept and for how long. Information subject to these retention requirements should be treated with care, much like information subject to NetIQ eDiscovery, due to potential penalties and fines for not following the laws. Data subject to compliance requirements that is not managed and retained per regulations can trigger government information requests. These requests can quickly transform into expensive legal proceedings, fines, and can include jail time.

The Solution

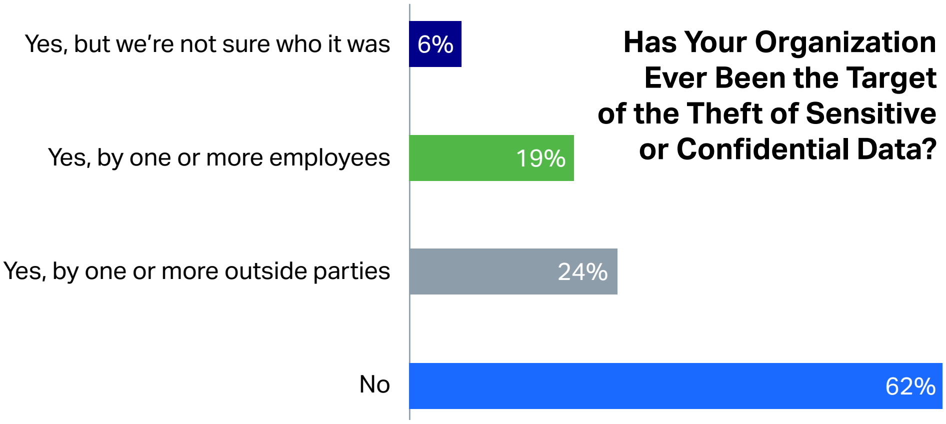
Implement an information governance software solution that automatically stores the electronic records required by the regulations in your industry. For example, an enterprise information archiving solution can tie directly to electronic communication systems (email, social media, and mobile messaging) and file systems. A proper archiving system also has search, publishing, and NetIQ eDiscovery tools. This ensures that your data is stored automatically and without end-user management.

4. Security and Privacy

Information security and privacy issues are closely related to the Regulatory Compliance challenge that organizations face.

"With 60,000 external e-mail messages and 300,000 internal email messages a month, Retain provides us exactly what we need. The investment has already paid for itself in the 500 GB reduction in space on our SAN. We were nearing capacity on the SAN. A huge amount for an organization our size. Plus, our users now have 100% access. It has really reduced the amount of time IT spends doing email discovery."

PAUL RUDIN
Network Administration
Grand Bank & Trust of Florida


Has Your Organization Ever Been the Target of the Theft of Sensitive or Confidential Data?

Many governmental regulations have requirements for handling and retention of certain types of information under the organization's control. There are at least two types of sensitive data that organizations should take pains to control and secure: employee and customer Personally Identifiable Information (PII) and Intellectual Property (IP).

Inadvertent release of a customer's or employee's social security number, bank account number, health information, or tax information can trigger lawsuits, massive costs, and penalties, as well as negative publicity for the organization. Intellectual property represents potentially huge amounts of investments by the organization. IP leaks through theft or inadvertent disclosure can cost the organization millions (or billions) of dollars, loss of market share, loss of shareholder equity, and ongoing negative publicity. More than one-third of the organizations surveyed have experienced theft of sensitive or confidential information.

The Solution

Similar to the solution outlined for the regulatory compliance, organizations must implement software to ensure proper information management and security. The archiving solution that your organization implements must comply with security and privacy requirements, including those outlined in HIPAA, SOX, FINRA, and other regulations. When choosing an archiving solution, it is essential that you verify that the solutions meets its security and privacy needs.

5. Storage Management

Because of the increasing data velocities and volumes, IT departments are regularly forced into purchasing additional storage resources to keep up with the demand. Even though the price of storage continues to fall, the volume and velocity of enterprise information continues to outpace the price reductions. An issue associated with growing storage volumes is the cost of effectively backing up, finding, managing, and using retained information cost.

The Solution

To decrease storage costs and volume, organizations must implement information management automation. Automation removes the responsibilities from the users to handle their own electronic records and will ensure that your organization has enterprise-level information management.

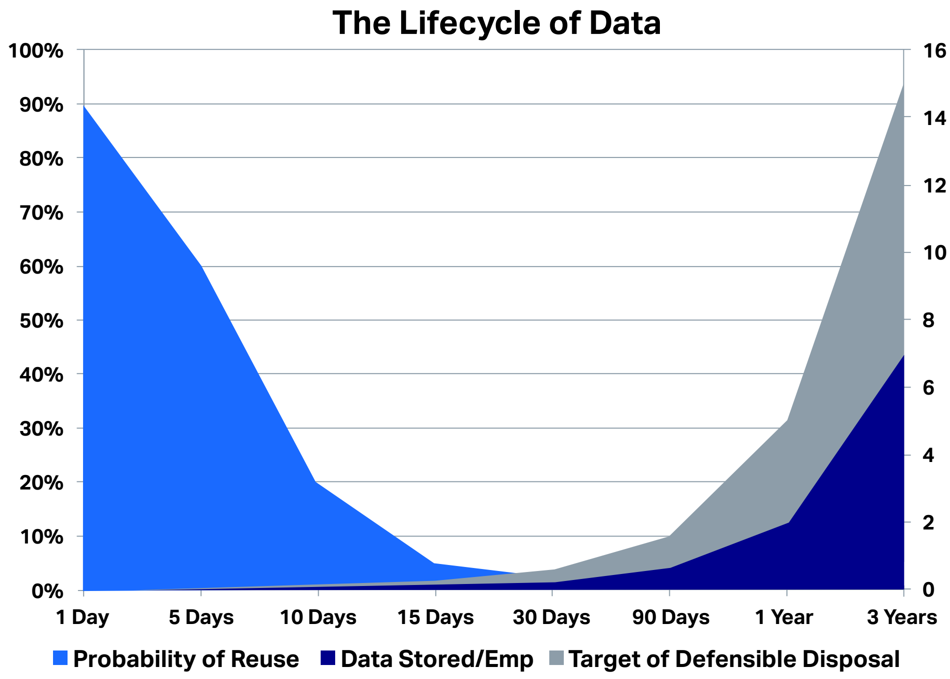
6. Defensible Disposition

The Compliance, Governance and Oversight Counsel (CGOC) conducted a survey in 2012 and revealed that on average 1% of organizational data is subject to legal hold, 5% is subject to governmental regulatory retention requirements, and 25% has some business value. This basic breakdown in data value concluded that approximately 69% of any organization's retained data had no obvious business value and could be disposed of without legal, regulatory, or business consequences.

This graph shows several data points related to this theory. The blue shaded area represents the probability of reusing data as it ages. Examples of this are the potential reference or reuse of email messages. For most employees, the need to search for and review an email message older than two weeks almost never occurs. Because of this, it should not surprise anyone that the probabilities of overall data reuse drop off rather quickly, approaching 1% after just 15 days. This figure also shows both the growth of information per employee over time as well as the information that, according to the CGOC, should be retained (green shaded area). The data balance (grey shaded area) represents the data that can be disposed of without negative consequences to the business. Osterman Research found that only 46% of organizations have a defensible disposition program in place.

The Solution

There are two keys to defensibly disposing of information. First, ensure the disposal process



is part of an up-to-date documented policy. Second, only dispose of information that is not subject to any current legal holds or government requests. Timely defensible disposal of information reduces the risk of future involvement in a future legal case or government information request, reduces the cost of NetIQ eDiscovery review and storage, and raises employee productivity. Defensible disposal is an important variable when calculating the ROI of an information governance program.

7. Productivity

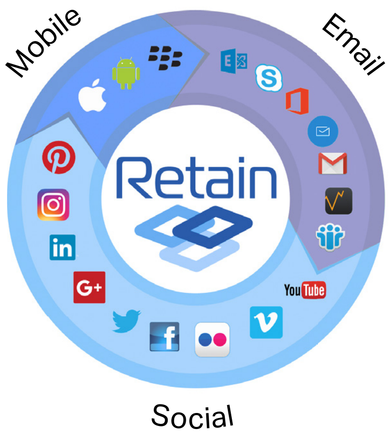
As information grows within the organization, employees spend more and more time managing individual work files, email and other content. This is time that could be better spent on the employee's actual job function. In fact this management has been estimated to consume between two and eight hours per week for each employee. In addition to this basic information management, additional productivity can be sucked up from inefficient search practices and data recreation when retained data cannot be found.

The Solution

Good information governance practices and solutions to support these practices increase productivity by reducing the amount of time employees spend managing their information.

The Retain Unified Archiving Solution

OpenText™ Retain Unified Archiving meets the information governance needs for electronic communication of organizations of all sizes and in all industries. Retain Unified Archiving provides multi-platform unified message archiving of all email, social media, and mobile communication data for case assessment, search, and NetIQ eDiscovery and can be deployed on-premises or in the cloud.



Connect with Us
OpenText CEO Mark Barrenechea's blog

Learn more at
www.microfocus.com/opentext