In partnership with

VERITAS Symantec

Rethinking Your Information Governance Strategy

Use an information governance plan to get a hold of government's 'data explosion'

Rethinking your information governance strategy

Use an information governance plan to get a hold of government's 'data explosion'

Government's digital paper trail is growing by the day, and digital records, such as email, make up the bulk of an agency's archive. "These stored records are causing a 'data explosion' in recordkeeping," says Stephen Watts, Federal Architect for Archiving and eDiscovery at Veritas Technologies Corporation. "And, it's causing many federal leaders to rethink their information governance strategy, a plan that can define records management policies and procedures."

According to a recent report from the National Archives and Records Administration, half of federal agencies are at a moderate or high risk of mismanaging records. Meanwhile, federal leaders are working towards a looming deadline: December 31, 2016. That's when agencies must comply with President Barack Obama's Managing Government Records Directive (M-12-18), a mandate that makes both permanent and temporary email records accessible in an electronic format.

The countdown to compliance can feel nerve wracking, Watts says, but agencies need to rethink their strategy because adding more storage simply is not a sufficient methodology anymore.

"The long-time adage of storage is cheap, so let's add to it, is no longer the case," he says. "We recently found that one petabyte [1,000,000 gigabytes] of data costs an organization about $5 million a year to manage. People used to think that storage was the solution, but really it's about defining your archive retention and information governance strategy."

In order to meet compliance and create a robust archive that can be quickly and efficiently searched, leaders should ask three, key questions:

1. **What kind of data do I need to look for?** Federal leaders need to know where the data was stored, when it was stored, who stored it, and what metadata was associated with it.

2. **Can I take action on my data?** Once you have the information, the data has to help agencies take action on things such as retention schedules and defensible deletion policies.

3. **Can I search my data quickly and efficiently?** Agencies must be able to produce records for audits, investigations and public records requests. Federal leaders need to identify the right records in a timely and efficient manner.

Over the course of the next week, you'll hear from Stephen Watts and his colleague, Phil Yaccino, Public Sector Architect for Information Governance at Veritas, on effective strategies for an information governance strategy. This course will guide you through processes, like email modernization, records archiving and retention and eDiscovery.

69%

Of information holds no business, legal, or regulatory value at all.

"Really, your information governance strategy drives discoverability. It helps you discover information, so that you can really learn from and manage records efficiently," Watts says. "You have to constantly be thinking about it because information governance is constantly evolving."

Enabling email modernization and automation

Finding the email in the haystack

"When government first started using email for daily correspondence, most assumed it was a communications tool, but federal leaders now consider email to be a digital record," says Stephen Watts, Federal Architect for Archiving and eDiscovery at Veritas.

Email volumes continue to grow, which makes searching for and identifying an email record similar to finding a needle in a haystack. Most government agencies are now on a path to email modernization, either for compliance purposes or to efficiently manage digital records.

One key piece to email modernization is automation, Watts says, a process that classifies and manages the vast amount of email records automatically. Many federal agencies are working toward Capstone Compliance in an effort to achieve email modernization. According to the Capstone directive, agencies should be able to:

- Ensure all email records are scheduled
- Prevent unauthorized access, modification, or deletion of records
- Make sure all records in the repository are retrievable and usable
- Consider whether emails and attachments can be associated with related records
- Capture and maintain required metadata associated with each record

But agencies can't keep everything. Watts offers the following advice on how to determine which records to preserve and move toward modernization.

Scope of Email Records

First, federal leaders will want to determine the scope of email that is subject to recordkeeping. Consider if managing email at the account level is suitable for your agency. Do you need to retain all employee email? With certain tools, agencies can establish permanent and temporary email accounts, creating classifications for individuals within an organization.

"If it's someone in a general counsel's office, they would be defined as permanent, while a facilities maintenance worker might have a temporary email account. By doing this, you can vary the rules and limit the amount of email records that you need to be focused on," Watts says. The goal is to determine what should be kept versus the unimportant employee chatter.

Imagine if you only had to send 5 GB of data to your law firm to review instead of 500 GB and legal – not IT – did much of the work.

The Risk of Keeping Everything

There's an underlying risk and cost associated with keeping everything for forever, Watts says. After deciding upon the scope of records to be preserved, agencies can employ email automation features to save both time and money while maintaining the data archive for retrieval.

Metadata, or basic summary information about a record, is key to automating the archiving process without any end-user interaction. This can be especially useful for actions like defensible deletion, Watts says — a process that determines when an email can be stricken from the archive.

"Defensible deletion allows agencies to delete records based off certain policies or prescriptions. For instance, an agency might only keep records for a specific period of time, and then they will purge those records," Watts says.

'Journaling' for Permanent Recordkeeping

For records that need to be kept forever, email automation can enable "journaling." Think of journaling as the official, true record, Watts says. With journaling, the email system captures an immutable copy of the communication, independent of any end-user interaction.

To begin the process of email modernization and implement strategies for efficient records management, download this whitepaper detailing the steps agencies should take to achieve digital records compliance.

Three steps to an eDiscovery strategy

Knowing the who, what, where, when, and why's of a record

Lawsuits, corporate investigations, Congressional subpoenas, and regulatory audits are increasing. And, according to the Justice Department's Office of Information Policy, the Freedom of Information Act backlog grew by 67 percent last year — close to 160,000 individual public records requests.

In order for electronically stored information to be accessible and ready for a records request, agencies should keep in mind a set of eDiscovery procedures to use.

"When you can answer all the questions that a reporter would ask — who, what, where, when, and why — then you have a solid information governance strategy," says Stephen Watts, Federal Architect for Archiving and eDiscovery at Veritas.

Step 1: Identification and Preservation for Archive Collection

The first step is to identify your records. Agencies need to detect all of their records that need to be preserved and potentially collected. The goal should be for agencies to first identify the custodian of the record, the appropriate date ranges for the record, and the sources of records involved. During preservation, the goal is to institute a "hold," ensuring that potentially relevant and responsive records are not accidentally destroyed, lost or expunged due to meeting retention.

Step 2: Processing, Analysis, and Review of Archive Records

The next step is to process the request, analyze the relevant records, and review each record for any privileged or sensitive information. The processing step refers to the crawling, indexing, and culling of records, including any conversion that enables analysis and review to be done electronically. In the analysis phase, records are reviewed for relevant summary information, such as key topics, people, and timelines critical to the request. Finally, in the review phase, the records are given a detailed look for relevance and privileged information.

Step 3: Production and Presentation of Archive Records

The final phase of the eDiscovery process focuses on preparing and producing the digital records for courts, regulators, or public audiences. Production refers to the process of turning over records in the format requested. It's important to verify that production details, such as form, media, and schedule are negotiated and agreed upon by both parties. Then, an agency enters the presentation phase, which refers to the process of turning over electronic data at depositions, hearings, and trials to elicit further information.

$18,000

The average cost to take just 1GB of data through the eDiscovery process

eDiscovery is a fact of life for government leaders, and yet many agencies still struggle with this critical task. Download this report to see which enterprise information archiving product works best for your needs.

It's important to be proactive and to follow a prescribed framework, Watts says. "It's not a question of if, but when."

Making decisions with your data archive

An information governance strategy requires data insight

Archiving is the first step towards an effective information governance strategy, but to really take hold and gain value from your data, agencies need to be able to draw insight from those records.

"An information governance strategy is much more than just keeping data around," says Phil Yaccino, Public Sector Architect for Information Governance at Veritas. "You have to know what your data looks like, what content information it contains, and the types of records that you have."

Using Data to Take Action

This data knowledge is what helps an agency when it faces something like a public records request or audit. It's also the way agencies can evaluate their records, identifying gaps where further efficiencies can be achieved.

For example, by looking at email records, an agency might be able to reduce storage needs by retaining only essential emails and eliminating transient messages that often make up the bulk of inbox traffic.

Knowing your data can also help save time when it comes to archive discovery, which can be particularly useful in cutting down wait times for things like FOIA requests, Yaccino says. With greater insight, agencies can begin to define their retention policies and schedules, allowing them to take action on things like defensible deletion or the movement of data across servers.

~1.5%

More data does not mean more value.
Target-rich data = ~1.5% of all data

Developing a Records Retention Plan

Data insight hinges on an effective retention plan, or set of rules that are used to govern how long records are kept.

"There is a big risk associated with keeping all your data and not doing anything with it," Yaccino says. "You could put your agency at risk if there's an internal review or public records request. You're saving yourself both time and money if you know your content and store it correctly with retention definitions."

Most agencies struggle with records retention because it requires a coordinated discussion between IT, records management, and legal services. These groups need to come together and decide on things like the record's format, metadata, retention, and value, Yaccino says. "You have to be thinking about your agency's basic and advanced archiving needs, and how they will help lead to greater insight."

Often times a storage problem is not a storage problem at all, but rather a management issue. Download this research note and learn how to get started on an information governance strategy.

Only after this conversation can government leaders look for tools that do the work of searching the network and creating value. "You want to implement archiving tools that can assign and automatically set retention rates," Yaccino says. "And you want to automate the process for how long a record is kept and why it's kept."

Using the right tools to advance your information governance strategy

Without a dedicated information governance strategy in place, federal leaders can spend valuable time and money managing unnecessarily large amounts of data.

"One agency in particular right now has 8 petabytes [8,000,000 gigabytes] of storage, and their management cost is approaching $40 million per year," says Phil Yaccino, Public Sector Architect for Information Governance at Veritas.

Cost is a main driver and so is efficiency. Often, it's the time that it takes an agency to process a record that can cause them to rethink their information governance strategy, Yaccino says. "If you can't turn around a public records request in time, you might be putting your agency at a reputational or legal risk," he says.

To maximize on both cost and efficiency, Yaccino says there are three tools that agencies should consider when it comes to advancing their information governance strategy.

Tool #1: Digital Archive Manager
Archiving tools, such as Enterprise Vault or Enterprise Vault.cloud, give government leaders the ability to efficiently store and discover unstructured data from their digital email records.

"Some agencies have rules and regulations on their data collection and storage. And every agency has their own unique requirement for whether they need an on-premise or cloud solution," Yaccino says. "Whether it's cloud or on-premise, it's about finding the right fit."

1 year

Neuralytix shows that in almost every case, Information Governance initiatives can completely pay for themselves in the first year of deployment.

Tool #2: Data Insight
Drawing data insight from archived records can help agencies improve their information governance strategies by providing actionable intelligence to data ownership, usage, and access controls.

There are a number of advanced analytics tools that can help government leaders gain knowledge into their data. One of them, Data Insight, helps agencies identify each data owner and gives greater visibility into the data, providing historical context into the record, so that actionable steps, such as defensible deletion or retention, can take place.

Tool #3: eDiscovery Platform
An eDiscovery platform can help government see through the electronic discovery process — from collection to production of records requests or audits. An enterprise solution, such as the one powered by Veritas, can bring about greater transparency and control of the electronic discovery process.

Particularly for government, which deals with hundreds of thousands of public records requests each year, there's a real need to deliver information in a timely manner. An effective platform will rapidly cull-down data and automate the records review throughout the eDiscovery process.

"In general, there's a real sense of urgency for government leaders who can't put off their information governance strategy any longer," Yaccino says. "There's a deadline and that means government leaders have to adhere to specific requirements and records requests for the public good."


VERITAS
Symantec