VERITAS

Restore Order: Information Management in the Federal Sector

A white paper for…

Federal IT practitioners and stakeholders responsible for defining or deploying their agency's information governance and eDiscovery policies, or backup and service continuity/disaster recovery strategies.

Table of Contents

Introduction 3

Part One: Information Governance 3

- **Data Growth: Moderation is a Must** 3
- **Defensible Deletion: Know When it's Time to Trash Data** 4
- **Compliance and Security** 5

Part Two: Information Availability 6

- **Downtime is Money** 6
- **Service Continuity and Disaster Recovery** 7
- **Add it Up: Business Impact Analysis** 8

Part Three: The Benefits of Information Management 9

- **Cut Your Costs** 9
- **Information Over Infrastructure** 10
- **Gain Visibility to Drive Insight** 10

Conclusion 11

- **Three Truths (Honest)** 11

Introduction

It's time for a little order.

Agencies have too much information, so they throw it into data centers like old clothes into a closet, vowing to organize it another day.

That day is here. Information management solutions help agencies sort through the data clutter. Federal IT leaders face numerous challenges – tight budgets, inefficient legacy systems, meeting Federal mandates – and Information Governance and Information Availability programs often are a lower priority. That's beginning to change because agencies understand that Information Governance and Information Availability reduce risk, increase efficiency, and save money. A progressive approach to information management helps agencies get data under control.

Don't wait – restore order.

Part One: Information Governance (That Thing that Only Lawyers Used to Talk About)

"Information governance… should incorporate all the tools needed to better manage information. Implementing an IG strategy will help unlock the value of data and improve decision making."
– Information Governance Initiative

Data Growth: Moderation is a Must

"As technology magnifies the ability to generate ever more data, Information Governance has presented itself as a critical component to overall organizational health."
– Samantha Lofton, Chief Risk and Information Governance Officer, Ice Miller LLP

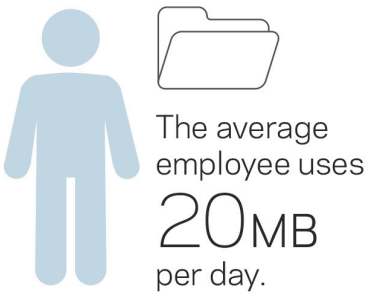
Veritas understands that data represents an agency's most valuable – and most abundant – asset.

The digital universe is doubling in size every two years and will multiply 10-fold between 2013 and 2020 – from 4.4 trillion gigabytes to 44 trillion gigabytes.[1] Agencies are no exception. They have an insatiable appetite for data, storing an average of 2.63 petabytes at any one time.[2] That's 167 times the information in all the books in the Library of Congress.

That's a lot to keep track of, and the sheer volume of data has the potential to slow agencies down if they let it.

[1] *The Economist.* "Building on the Data Lake" April 7, 2015. http://gelookahead.economist.com/data-lake/
[2] *Informatica.* "Big Data for Government." 2013. http://international.informatica.com/Images/02340_big_data_government_eb_en-US.pdf

The average employee creates, sends, receives, and stores conservatively 20 megabytes of data per day.[3] That includes structured data like spreadsheets and data in XML files. It includes unstructured data – data that has no fixed field – in the form of email, email attachments (which are often duplicated), Word documents, and PowerPoint presentations. And it includes video and images – from work and non-work sources like social media sites.



By 2017, 79 percent of all data shipped will be unstructured data, according to IDC.

Data doesn't just grow quickly, it also grows old quickly. Once data has aged 10 to 15 days, its probability of ever being looked at again approaches 1 percent.[4] Keeping data around is an idea that can grow as stale as information itself.

Defensible Deletion: Know When it's Time to Trash Data

"Data deletion carries a potentially high ROI, but pressing the delete key is much easier said than done."
– Alan Dayley and Garth Landers, Gartner Analysts

We are conditioned to keep all data because we believe it will be useful… sometime. Some day. Maybe.

Agencies are no different, and they struggle to overcome the "store everything" mentality.

Accumulation is easier than organization.

But progressive agencies have learned a valuable lesson about data – less is more, and "delete" is not a bad word. Why keep what you don't need? Clean out the clutter and harness the power of information.

It turns out an overwhelming amount of data that agencies and organizations hold on to has no legal, regulatory, or business value. The Compliance and Governance Oversight Council conducted a survey in 2012 and found that 69 percent of an organization's stored information is redundant, outdated, or trivial (ROT). It doesn't add value to an agency.

Practicing "defensible deletion" will allow agencies to shed ROT data. More data does not equal more value, so there is no compelling reason to retain all data. Defensible deletion is at the heart of that approach.

[3] *Information Governance 101.* "The Lifecycle of Information – Updated." May 20, 2015. http://informationgovernance101.com/
[4] Ibid.

Agencies shouldn't be afraid of deleting data. Rule 37(e) of the Federal Rules of Civil Procedure gives agencies the latitude to delete information provided they establish a documented retention policy.[5]

Old habits are hard to break, and data proliferation continues unabated throughout many agencies. Rather than save all data, agencies must figure out how to manage data appropriately so their most important asset doesn't also become their biggest, costliest burden.

Compliance and Security

"Part of the reason eDiscovery is so expensive is because companies have so much data that serves no business need. Companies are going to realize that it's important to get their information governance under control to get rid of all the data that has no business need... in ways that will improve the company's bottom line..." – Judge Andrew J. Peck, U.S. Magistrate

Data has a direct impact on an organization's compliance efforts.

It costs $18,000 to conduct eDiscovery for every 1 gigabyte of data, according to Gartner's eDiscovery report. The 2012 RAND Report, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery,* found that the document review process consumes more than 70 percent of every eDiscovery dollar.[6]

Agencies are dealing with increasing numbers of international, Federal, state, and local regulations that are driving the need to better manage information. Examples of these regulations include SEC 17, FINRA 3010/3011, Solvency II, Dodd-Frank, FAR, HIPAA, the Gramm-Leach-Bliley Act, and Sarbanes-Oxley.

More regulations often mean higher costs, but properly maintained data requires less searching and gathering by staff and less review by counsel.

Keeping data also has security implications. Improved Information Governance policies mean agencies keep less data. That translates into reduced exposure – less data means there is less for hackers to steal.

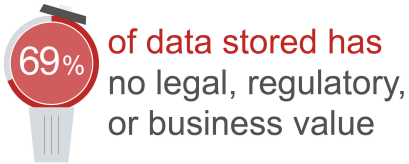
The historic hack at Sony Pictures represents an important example. The theft resulted in the disclosure of thousands of personal emails that simply didn't have to be retained. Wikileaks has built a searchable database that allows anyone to search through all the emails, and sift through the company's digital dirty laundry.

[5] Cornell University Law School. "Rule 37. Failure to Make Disclosures or to Cooperate in Discovery; Sanctions." https://www.law.cornell.edu/rules/frcp/rule_37
[6] Rand Institute for Civil Justice. "Where the Money Goes."

The pitfalls are numerous, but agencies can avoid those digital hazards by adopting Information Governance policies that allow them to:

- **Gain visibility and expose risk.** The best way to do that is by understanding an agency's information ecosystem – determining the age of information, its location, and ownership. Understanding the risk profile of information allows agencies to shift from the "store everything" mentality to a value-focused perspective

- **Take action and execute decisions.** Once agencies gain visibility into their information footprint, they must take action. Ultimately, the choice is between retention, protection, and deletion. By leveraging critical insights into the value of their information, agencies can assign classifications, deploy policies, and initiate cleanup. With 69 percent of enterprise information having no legal, business, or regulatory value, it is imperative that agencies clean up their information footprint – sooner rather than later



- **Assume control and ensure governance.** Information Governance doesn't occur overnight – it happens when agencies bring together the right people, process, and technology. Stakeholders must develop sustainable policies that outlast a single project. Technologies that integrate and automate will drastically reduce the manual effort required to manage the Information Governance workflow and improve an agency's ability to mitigate information risk

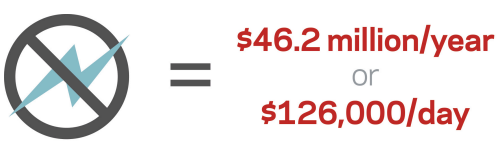
Part Two: Information Availability

"Successful and responsible organizations must have the ability to identify, locate, and retrieve the records and related information required to support its ongoing business activities… Having the right information available at the right time depends upon an organization's ability to nimbly search through enormous volumes of information." – Association of Records Managers and Administrators

Downtime is Money

"…it's inevitable that the time will come when you'll need to recover from a disaster, and fast."
– Aberdeen Group

Avoiding downtime is crucial, and no agency or organization is immune. A 2013 study found that 91 percent of data centers experienced an unplanned data center outage over the previous



two years.[7] The cost of downtime adds up fast. Over a 12-month period, outages at 67 data centers cost a combined $46.2 million – or $126,000 per day – according to the study.

Productivity also takes a hit when agencies and organizations experience downtime. IT downtime costs businesses, collectively, more than 127 million person-hours per year—an average of 545 person-hours per company—in employee productivity.[8]

On the opposite end of the spectrum, real-time access to information boosts productivity to save the average Federal worker more than 800 hours per year.[9]

When it comes to downtime, it's a matter of "when" not "if." So agencies and organizations must be prepared. Human error, natural disaster, or an IT-related failure can be the culprit. So can cyber attacks, and 2015 may well be remembered as "the year of the hack." It is unlikely the trend will improve in 2016 and beyond.

The red flags are more numerous than ever – the Office of Personnel Management, Veterans Affairs, and Internal Revenue Service all have been the target of recent attacks – and all agencies are in a state of heightened awareness.

But no matter why it occurs, downtime is a financial stumbling block that agencies must do their best to avoid.

Service Continuity and Disaster Recovery

"In many organizations, it may seem as if the only goal of backup and recovery is to backup and save as much data, content and system images as possible. But the real goal of backup and recovery is to avoid downtime, data loss, and regulatory issues. With that goal in mind, the main focus of backup and recovery should really be recovery." – Aberdeen Group

Veritas understands agencies are "always on" and require constant access to data and applications. But agencies with poor Information Availability policies waste time by trying to gain access to data and applications. They also run the risk of losing their information when downtime occurs. Too often they rely on rudimentary backup and recovery approaches. Data and applications are too valuable to leave in the hands of run-of-the-mill backup and recovery solutions.

One out of 10 organizations say they need greater than 99.99 percent application availability, and that's why service continuity represents the best approach to maintain access to information.[10]

[7] Ponemon Institute and Emerson Network Power. "Data Center Outages." http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/infographics/documents/ponemon-infographic-cost%20of%20downtime-r11-13-final.pdf
[8] CA Technologies and Coleman Parkes Research Ltd. "The Avoidable Cost of Downtime, Phase 2." May 2011. http://www.arcserve.com/us/lpg/~/media/Files/SupportingPieces/ARCserve/avoidable-cost-of-downtime-summary-phase-2.pdf
[9] *MeriTalk.* "The Drive to Thrive." August 2014. http://meritalk.com/drivetothrive
[10] *Tech Target*. "Trends in high availability and fault tolerance." http://searchcio.techtarget.com/podcast/Trends-in-high-availability-and-fault-tolerance

Service continuity means making sure the applications an organization relies on are highly available. When it's done right, service continuity means users never even notice when there's a disruption or downtime. That's because all data and applications have been replicated – not just backed up – and everything is stored safely at a disaster recovery site.

Continuous replication is a critical component for agencies to avoid losing information during long disruptions. While many agencies know they need mature service continuity and disaster recovery solutions, these important initiatives often get overlooked or passed over in favor of other IT programs.

But information management has come a long way in a short period, and Information Availability is easier than ever. As agencies consider service continuity and disaster recovery, it's vital that they include three elements in the solution they choose:

- Automation is a key pillar of a meaningful service continuity and disaster recovery plan. Manual processes increase costs and reduce efficiency. A fully automated approach allows agencies to manage large enterprises with limited staff and resources and keep pace if data and the number of IT systems continues to grow
- Simplicity also represents a key pillar, and agencies must drive out complexity so they can adopt solutions that work with any IT platform – not just Linux or Windows. Limiting options means limiting effectiveness. Eliminating point products in favor of an enterprise-wide approach helps keep it simple
- Agencies also must test their strategies so they can predict the outcome of a disruption and know what's at stake. That's why predictability is the third pillar of an effective service continuity and disaster recovery plan

"Be prepared," may be the Scout Motto, but agencies would do well to embrace that timeless aphorism. These days, preparation requires much more than backup, which represents a one-size-fits-all approach, but no two agencies are alike.

Add it Up: Business Impact Analysis

"The BIA becomes the foundation of the plan you will build for your recovery. This is the process that will determine what needs to be recovered and how quickly. It is one of the most difficult tasks to perform and one of the most critical to get right."
– Kelley Okolita, author, "Building an Enterprise-Wide Business Continuity Program"

Being prepared also means agencies must arm themselves with information so they can determine the appropriate course of action. Conducting a business impact analysis before forging ahead will help agencies compile the insight they need about their data and applications. The analysis forces agencies to determine:

- What are the most critical applications?
- What data sets are most critical?
- Where do those applications and data reside?
- What do Service Level Agreements say about data and applications and what are the expectations for the delivery of those services?

Agencies also must take time to understand their recovery point and recovery time objectives. This is a truly deep dive that will allow agencies to figure out:

- How long it will take to get data and applications up and running again
- How current the data and applications will be once they are up and running again

An analysis can also enable agencies to consider the many different scenarios that could result in downtime. No service continuity and disaster recovery initiative is complete without the comprehensive internal review that a business impact analysis provides.

Part Three: The Benefits of Information Management

Cut Your Costs

Holding onto data can cost a lot of money.

It costs organizations an estimated $5 million a year to store 1 petabyte of data.[11] Some agencies believe they are addressing the problem by off-loading data into the cloud to cut costs. But cloud storage encourages agencies to retain data. What would you do with $5 million saved through defensible deletion? Think dollars and sense.

Other agencies “tier” their data – rank its value and then store it accordingly. This approach recognizes that not all data is equal. But it also encourages data hoarding and data fragmentation, or the dispersion of data

[11] Veritas. “Information Governance: Fighting Back Against the Exponential Data Curve.” http://docs.media.bitpipe.com/io_12x/io_123875/item_1157099/GA-EB_information-governance-fighting-the-exponential-data-curve_0515.pdf

and applications across tiers, data centers, and clouds that make information increasingly complex to manage.

Hoarding data is not a strategy, and agencies shouldn't waste money holding on to ROT data that provides no value.

Information Over Infrastructure

Of every $10 spent on infrastructure, $6.20 is spent to maintain it – that's 62 percent of spending. Infrastructure represents a lost investment, and agencies can't afford to waste their resources spending on infrastructure to store data they don't need.

No Federal project can overlook the potential impact on an agency's bottom line. Mandates like the Federal Information Technology Acquisition Reform Act (FITARA) give chief information officers (CIOs) the leverage to implement cost-saving approaches. That's because it requires CIOs to have a significant role in IT investment decisions and oversight of those investments.

Data-driven policies can help CIOs meet those cost-cutting goals by setting priorities, shedding data, and then reducing infrastructure. CIOs have the power to end the "store everything" approach and save money.

Gain Visibility to Drive Insight

"Information is the oil of the 21st century and analytics is the combustion engine."
– Peter Sondergaard, Senior Vice President at Gartner and Global Head of Research

Big data is all the rage. Agencies want and need to derive insights from their information assets – because they need to learn to make better decisions as well as become more agile and productive. That's why President Obama hired the administration's first Chief Data Officer, Dr. DJ Patil, and why Federal agencies are following suit.

Smart data management and analysis are the keys to deriving the big data insights that can help agencies become smarter and apply predictive analytics so they can understand what consumers want and need – even before they know themselves.

By 2020, the percentage of useful data could grow to more than 35 percent, mostly because of the growth of data from embedded systems. And, Federal agencies seem to be ahead of the curve, with 60 percent saying their agency is analyzing the data they collect.[12]

[12] *MeriTalk*. "Big Data, Big Brains Beacon Report." April 2013. http://www.meritalk.com/big-data-beacon.php

Availability drives insight. That means knowing where data is. It means being able to access data when you need it. It means faster access and retrieval. High-value data needs to be kept separate from run-of-the-mill information. It needs to be stored in advanced disk storage for quicker retrieval.

But data growth has led to haphazard storage and data fragmentation. Progressive agencies leverage the power of their information to learn more, gain time, and save money.

Conclusion

Three Truths (Honest)

Information Governance and Information Availability help agencies overcome data chaos. Veritas empowers agencies to recognize the business value of information management. That's the easy part. The hard part is the cultural shift required of agencies – they need to overcome the "store everything" mentality.

They need to embrace "defensible deletion." Agencies that take an information-first approach are becoming masters of their data – not controlled by their infrastructure. They understand the "three truths" of information management:

- Data isn't the same as information, and agencies shouldn't treat them the same. High-value data requires storage in advanced disk storage for quicker recovery
- More data doesn't mean more value
- And information is more important than infrastructure

Proper Information Governance policies allow agencies to get the most value out of their data, cut costs, improve efficiency, and avoid that risk – financial, legal, security, productivity, and reputational.

Agencies must apply Information Governance policies to records management, compliance, storage and archiving, risk management, and eDiscovery. And they must understand that storing data that has no value costs a fortune.

Proper Information Availability policies ensure that agencies can access what they need, when they need it, wherever it resides. Wasting time and money trying to access data is both expensive and frustrating. Agencies must apply Information Availability policies so they aren't hobbled by downtime.

Take control of your information today to help unveil your information potential tomorrow.

Restore order.

For more information, please visit www.veritas.com/solution/government

For specific country offices and contact numbers, please visit our website.

Veritas Technologies LLC
Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1 (650) 527 8000
1 (800) 721 3934
www.veritas.com

© 2015 Veritas Technologies LLC. All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.