



Navigating Information Governance: What's Your Strategy?

November 6, 2014

Introduction

Government agencies and private sector businesses are **drowning in information**. In addition to managing the growing variety, velocity, and volume of data, they must:

- Meet government transparency objectives
- Respond quickly to eDiscovery requirements
- Manage Freedom of Information Act (FOIA) requests and internal investigations
- Comply with records management regulations



With data requirements skyrocketing, how can organizations leverage **information governance** to meet this tidal wave head on while ensuring data security?

To find out, O’Keeffe & Company, on behalf of Symantec, surveyed **152** Federal government and **153** private sector attorneys, IT executives, FOIA agents, and records managers to examine barriers to and benefits of achieving true enterprise-wide information governance.

For this study, respondents were asked to frame their responses using the following definition of **information governance**: The activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs.

Executive Summary

- **Today's information governance is inadequate:**
 - Nearly **three-quarters** of respondents' organizations (**74%**) have a formal, enterprise-wide information governance strategy, but just **one in five** say it's very effective
- **Data security is at risk:**
 - Just **37%** give their organizations an "A" for data protection, **28%** for data discovery, and **26%** for data management
 - **Forty-four** percent of respondents say that data security and protection is the single largest information governance-risk their organizations will face if not addressed
- **Organizations must make investments in technology and training:**
 - Respondents believe their organization should take the following steps to ensure effective, enterprise-wide information governance programs: **Improve training (46%), educate end users on the importance of records (46%), and improve technology (43%)**
 - During the next two years, organizations say they are most likely to invest in **security software, document management, data loss prevention, and backup**

Defining Information Governance

Feds and businesses associate information governance with the policies and procedures surrounding data management

In your own words, how would you define “**information governance**”?*

“An integrated approach to overall information management from creation, to use, to disposition”
– **Records manager, Federal agency**

“The laws, procedures, and protocols used to protect electronic information among employees and outside the organization” – **Attorney/Legal Counsel, Large business**

“The oversight, management, and policy surrounding the capture, collection, and access to data” – **IT director/manager, Federal agency**

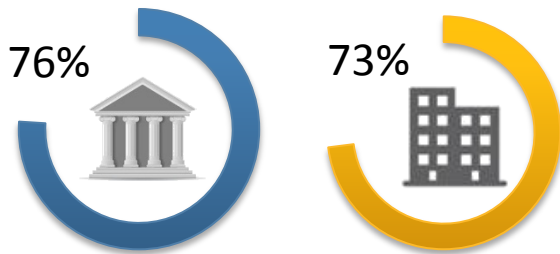


Take Away: No Universal Definition

The State of Information Governance

Three-quarters of Feds and businesses have a formal information governance strategy, yet just one in five say it's very effective

76% of Feds and 73% of businesses have a formal, enterprise-wide information governance strategy

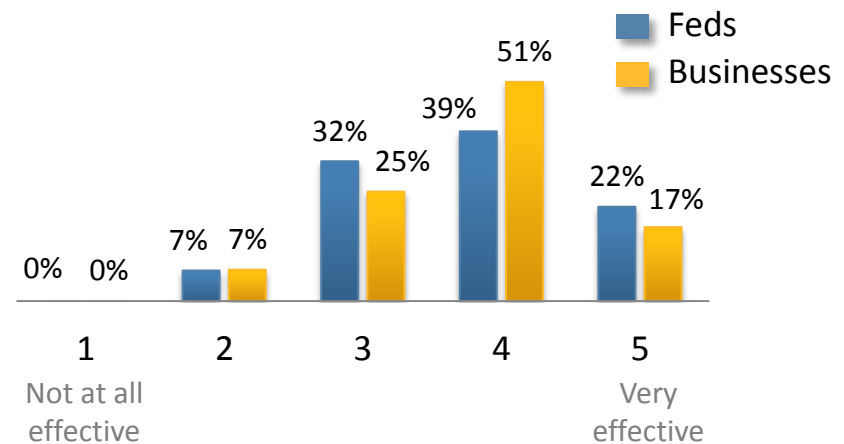


Of organizations who do not, 57% of Feds and 83% of businesses are currently working on developing one

However, having a strategy does not guarantee it's effective – Merely

ONE in FIVE

have a “very effective” strategy



Take Away: Wide Adoption, Limited Impact

Key Program Components

Both Feds and businesses agree that data security is the most important component in an information governance strategy

What are your organization's most important components of information governance?*

Protecting data from cybersecurity criminals and other nation states



 76%  69%

Implementing backup and disaster recovery



 62%  63%

Protecting data from employee theft and loss



 61%  57%

Creating/improving eDiscovery, investigations, or FOIA response process



 39%  37%


Creating/enforcing/improving ongoing records retention



 38%  50%

Deleting old data with no business or legal value



 22%  25%

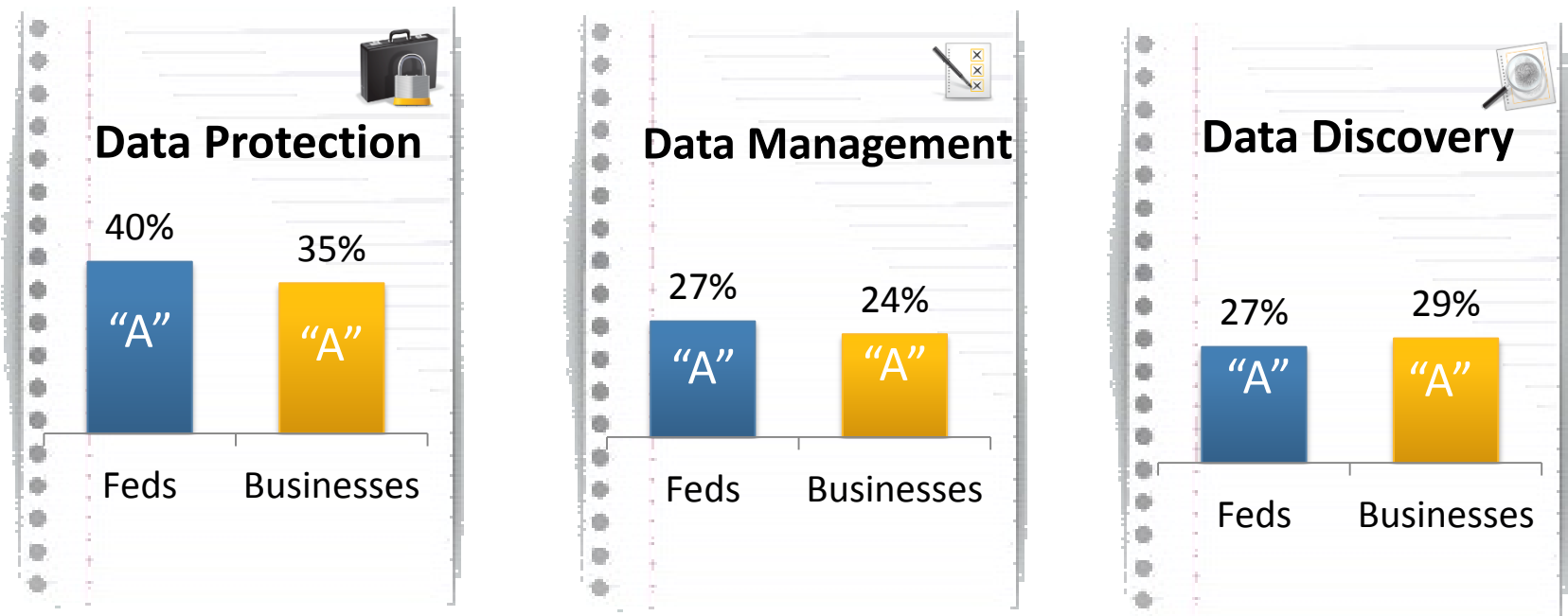
Take Away: Multiple Components for a Solid Strategy

*Percentage who ranked the component in their top three

Grading the System

Despite their focus on data protection, just more than a third of respondents give their organization an “A” in that area

How would you grade the following components of your organization’s information governance program?



Take-Away: Room for Improvement Across the Board

Top eDiscovery Challenges

Organizations consider data processing and filtering to be their top weaknesses

When it comes to eDiscovery and FOIA requests, what are your organization's biggest technology weaknesses?*



Data processing and filtering **38%**



Data collection **36%**



Review **28%**



Applying legal holds **22%**



Early case assessment **21%**



Feds believe their top weakness is data collection. *Businesses* say their top weakness is data processing and filtering.

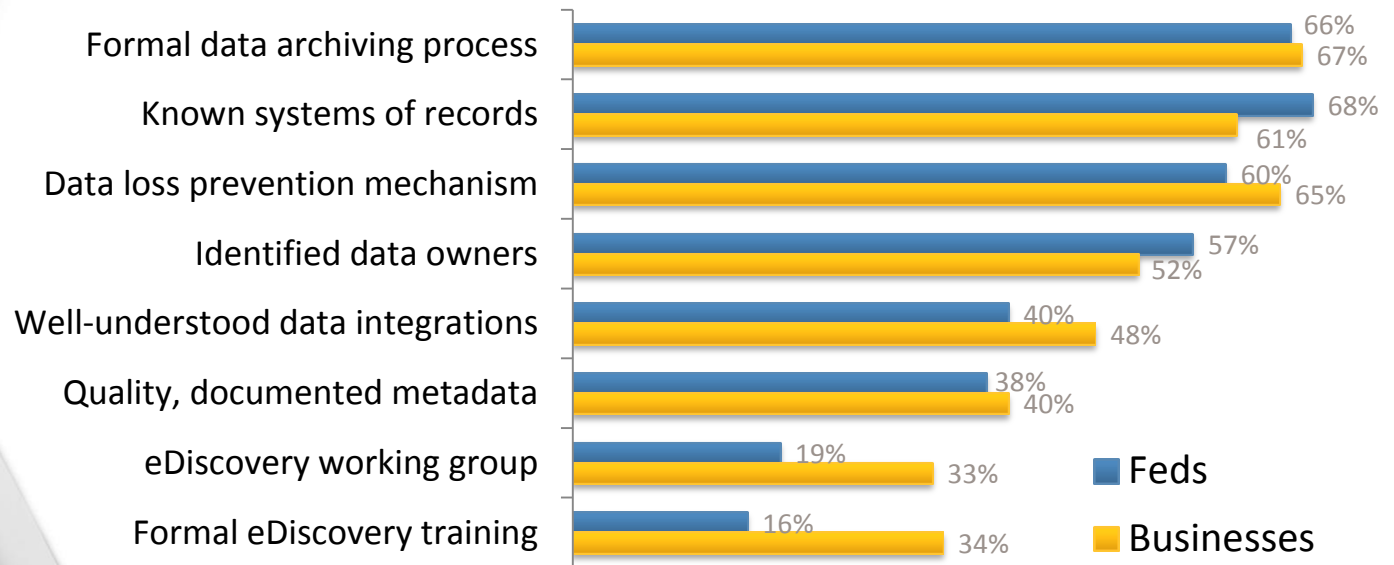
Take Away: Leverage Technology to Address Challenges

What are We Missing?

Most organizations overlook data integration, metadata, and eDiscovery training



Which of the following does your agency's current information governance program include?*



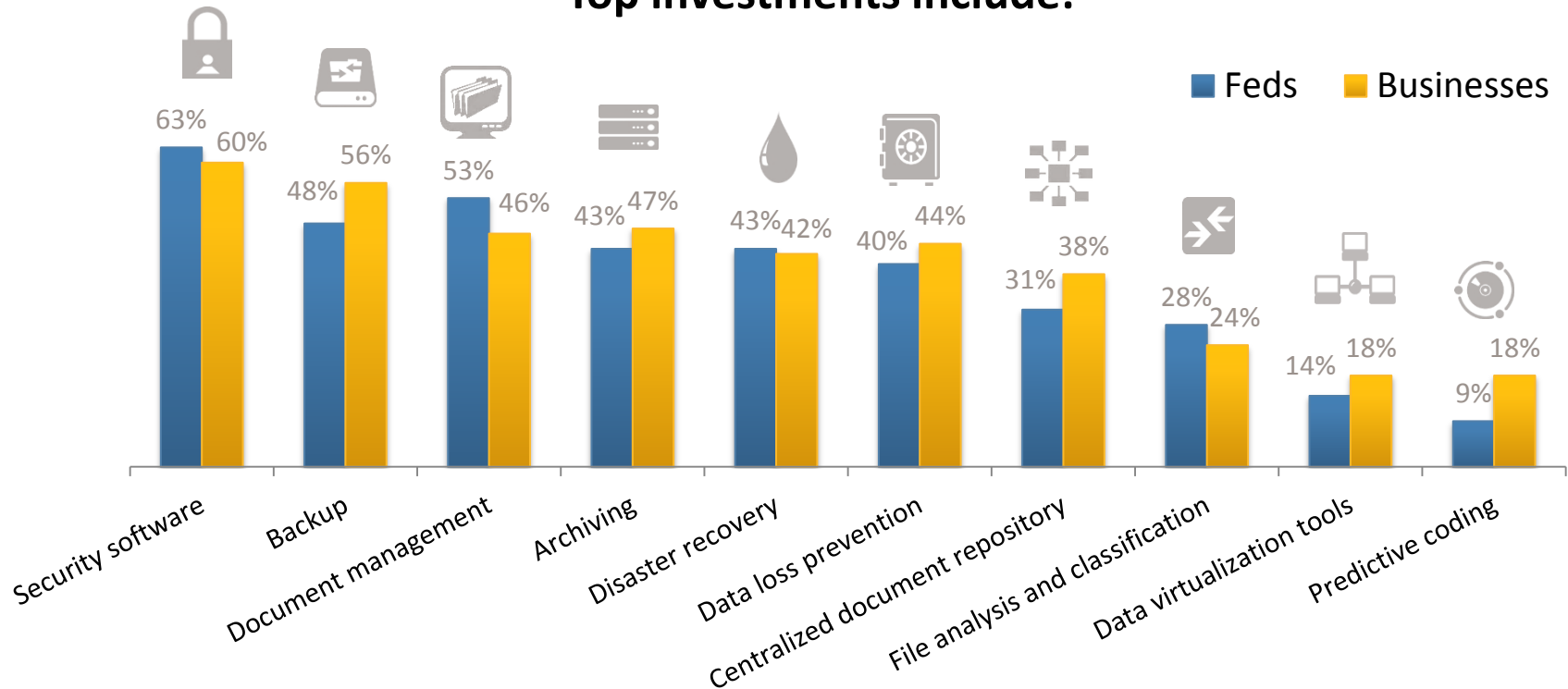
Take Away: eDiscovery Can Get Lost in the Shuffle

*Respondents asked to select all that apply

The Good News

In the last two years, 95% of organizations have made investments to improve information governance

Top investments include:*



Take Away: Investments Span Information Governance Spectrum

*Respondents asked to select all that apply

Rising to the Top

Effective information governance improves organizational efficiency and regulatory compliance

What are the most significant benefits to an effective information governance strategy?*

1. Improves organizational efficiency **62%**
2. Improves regulatory compliance **61%**
3. Improves services to customers/constituents **46%**
4. Prepares the organization for lawsuits and/or investigations **43%**
5. Improves visibility/transparency **39%**
6. Improves decision making **38%**
7. Saves money **36%**



Respondents estimate that an effective system could save them more than **3 days' time** in a routine eDiscovery scenario



Feds see greater value in improved constituent service and transparency. Businesses see greater value in protection/preparation against lawsuits or investigations.

Take Away: Efficiency and Compliance Top Benefits List

Key Challenges

While both sectors struggle to manage the flood of data, Feds face tighter budgets

What are your organization's most significant challenges to effective information governance?*

Feds:

1. Lack of budget to fund initiatives
2. Massive data growth
3. End user reluctance to delete unnecessary data



Businesses:

1. Massive data growth
2. End user reluctance to delete unnecessary data
3. Volume of junk/unnecessary data clogging up the system



Additional challenges:

“Staffing to initiate policies and procedures”

“Multiple offices with legacy systems and procedures in conflict”

“Government regulations”



Take Away: Data Growth and Employee Resistance are Hurdles

Power Struggle

Ownership confusion also complicates information governance efforts

When asked who should lead the information governance team and strategy at their agency or business, responses varied by respondent title:*

IT pros said...	CIOs/IT professionals
Attorneys said...	The legal/compliance department
Records managers said...	Records management



*Interestingly, while not all think IT should lead information governance efforts, the majority believe they should **fund** the initiative, or at least share the funding with other teams*

Take Away: Lack of Stakeholder Collaboration Hinders Success

Significant Risks Drive Need for Improvement

Feds and businesses agree that data security and protection is the single largest risk to information governance



What is the largest risk to information governance if left unaddressed?*



Feds

1. **Data security and protection 43%**
2. Employee time lost due to searching for the right information 26%
3. Data storage 17%



Businesses

1. **Data security and protection 45%**
2. Employee time lost due to searching for the right information 22%
3. Data storage 17%

What would be your top priority if you had more visibility into your unstructured data environment?*

1. **Secure high-value files 38%**
2. Migrate data with little business value to lower cost storage 25%
3. Monitor for abnormal user activity 18%

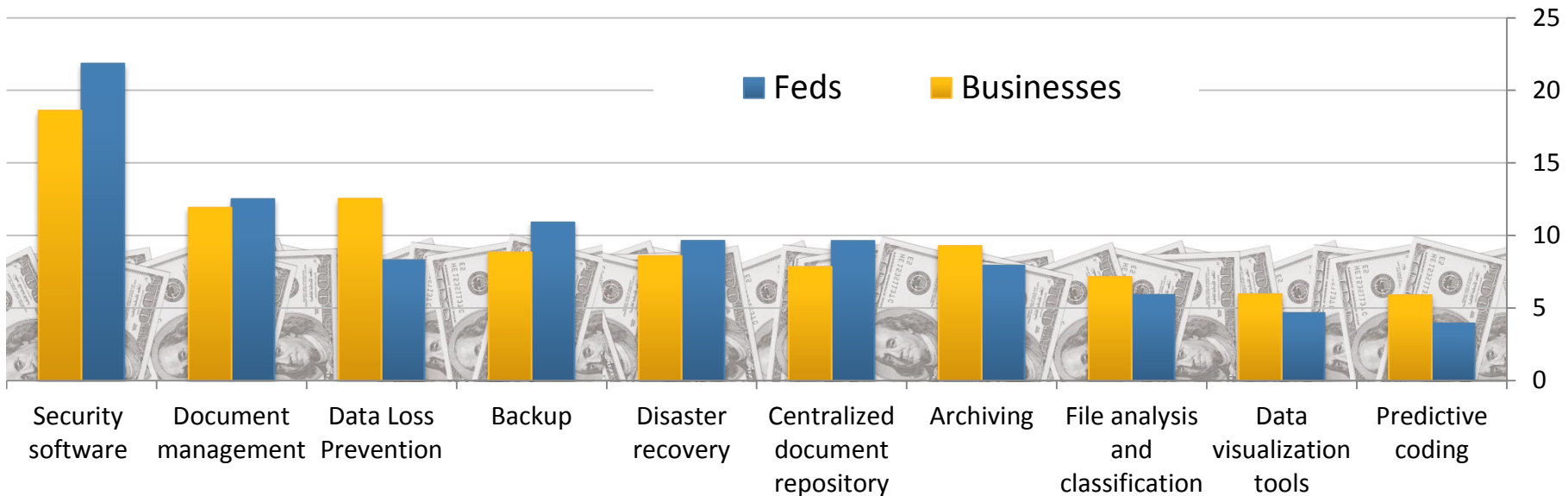
1. **Secure high-value files 35%**
2. Delete data stockpiles 26%
3. Migrate data with little business value to lower cost storage 20%

Take Away: Security Risks are the Top Concern

Investment Outlook

To improve information governance, organizations are most likely to invest in security software

What do you believe your organization is most likely to invest in over the next 12-24 months to improve information governance?*



Take Away: Take a Modular Approach & Plan for Interoperability

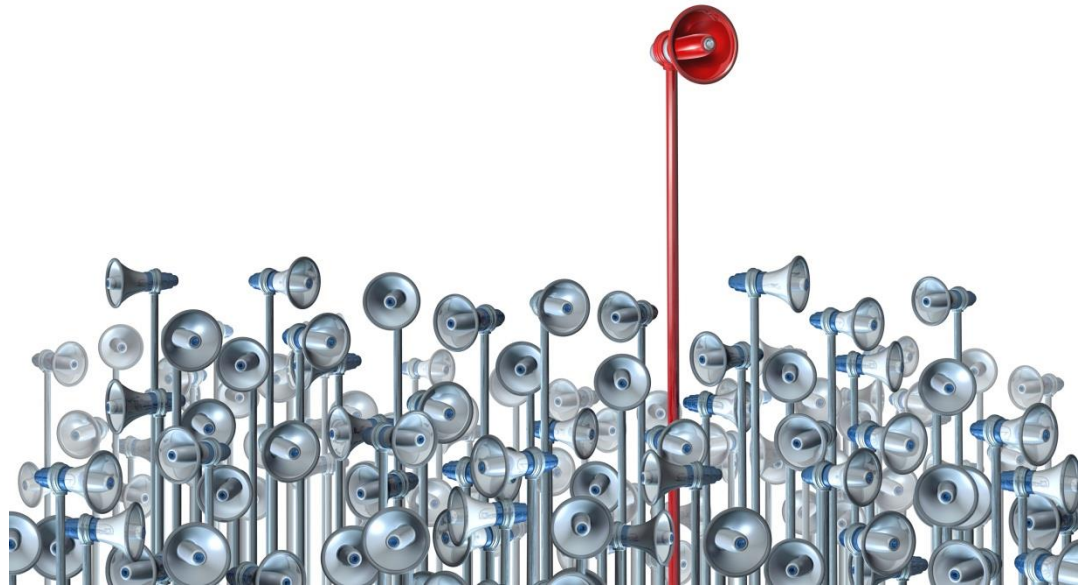
* Respondents asked to indicate their best "bets" by allocating 100 pennies among the possible investments. Feds allocated an average of five pennies to "none"; Businesses allocated three

Guide to Effective Governance

Organizations recommend improved training and end-user education to ensure future information governance success

Feds and businesses say:

1. Improve training
2. Educate end users on the importance of records management
3. Improve technology
4. Build out policies and procedures
5. Hire additional IT resources



Take Away: Success Depends on People, Processes, and Technology

Recommendations

- **Gain Visibility**

- Does your organization have a formal information governance strategy? Do you grasp the potential costs and risks?

- **Take Action**

- Once your organization knows what it has and where it is, it needs to analyze the data and determine what it can and should do with it

- **Assume Control**

- Take a stepwise approach to information governance and reclaim more and more of the business value of your organization's data



Methodology and Demographics

O’Keeffe & Company, on behalf of Symantec, conducted an online survey of 305 information governance stakeholders in July 2014. The report has a margin of error of $\pm 5.57\%$ at a 95% confidence level

Respondent job title:	
3%	CIO/deputy CIO
2%	CISO/deputy CISO
41%	Attorney/legal counsel
31%	IT director/manager
20%	Records manager
3%	Freedom of Information Act (FOIA) agent

Organization type:	
50%	Federal government
50%	Large business (500 employees or more)

Agency type:	
80%	Civilian
20%	DoD or Intelligence

Business type:	
56%	Publicly traded
44%	Privately owned

100% of respondents have responsibility for their organization’s information governance and/or data management efforts



Thank you!

Symantec Federal

Federal_US@Symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.