




Inside Job: The Federal Insider Threat Report

September 14, 2015

Underwritten by:  **Symantec™**

meritalk.com

Addressing data breaches and cyber incidents **perpetrated by insiders** – whether malicious or unintentional – is a mounting challenge for Federal IT executives. As agencies are entrusted with storing and managing a range of sensitive information, the potential channels for data loss are becoming more complex. Underscoring the risk, the damage from these incidents is significant, lasting, and expensive.

- What are the most common insider threats agencies face today?
- What are the strengths and weaknesses of current insider threat programs?
- How can Feds leverage technology to minimize the risks and consequences of this growing vulnerability?

To learn more, MeriTalk surveyed **150 Federal IT managers** familiar with their organization's cyber security efforts. The resulting Inside Job report highlights challenges, progress, and – importantly – recommendations for change.



- **Federal agencies are struggling to combat insider threats:**
 - In the past 12 months, **45%** of Federal IT managers say their agency has been a target of an insider incident
 - And nearly one in three (**29%**) say their agency has *lost data* to an insider incident
- **Many agencies overlook basic security measures:**
 - Just **39%** offer employees annual in-person security training
 - Fewer than half employ two-factor authentication or endpoint encryption agency-wide
 - More than **40%** of agencies cannot tell the moment a document has been shared or how*
- **Formal governance and insider threat programs may help:**
 - **77%** of Federal IT managers believe that Presidential Cross-Agency Priority (CAP) goals will aid agency-wide government efforts to combat insider threats
 - The **55%** of Federal agencies with a formal insider threat program are also more likely to have advanced training, real-time alerts, and agency-wide security measures in place

- **Nearly one in three Federal agencies report losing data in the past 12 months to an insider incident**

In the past 12 months...

45% of Federal IT managers say their agency has been a **target** of an insider incident

29% say that their agency **lost data** to an insider incident



Nearly 40% of these incidents are the result of **unintentional actions** (well-meaning employees who unintentionally expose information or systems to risk)

Take Away: Crimes of Accident and Intent

Heightened Surveillance

- Agencies are making a concerted effort to minimize insider threats, but say it is still common for employees to unintentionally put them at risk

76% say their agency is more focused on combating insider threats today than one year ago

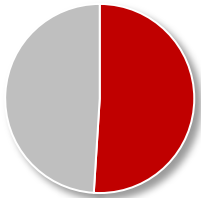


However...

- 65% say it is **common** for employees/contractors to email documents to personal accounts
- 51% say it is **common** for employees/contractors to not follow appropriate protocols
- 40% say **unauthorized employees** access government information they shouldn't at least weekly

Take Away: Missing What Is Under Their Nose?

- While many agencies run mock attacks and offer annual online training, few offer in-person training or security manuals for review



51% say their agency runs mock attacks or other test scenarios (i.e., phishing attacks) to better understand unintentional insider threat risks

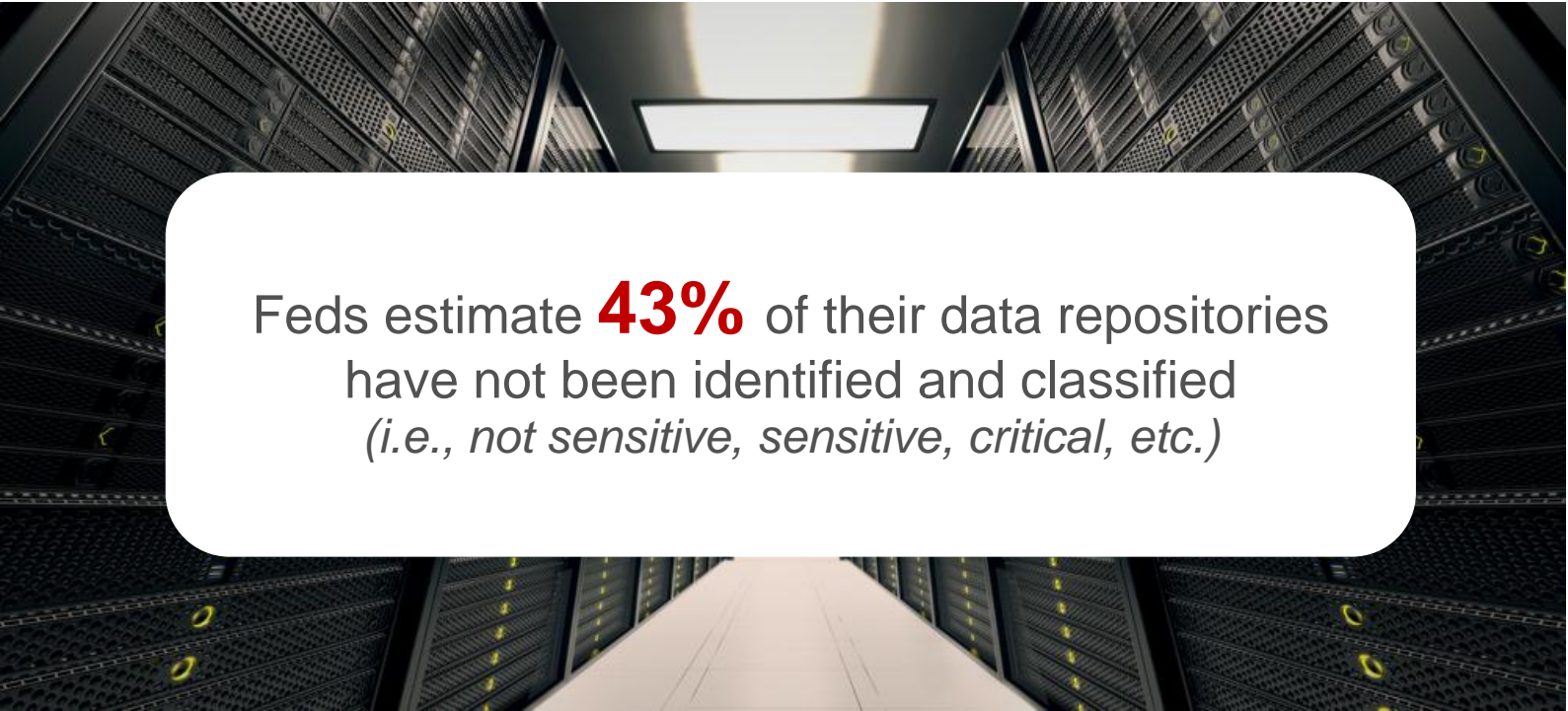
Which of the following types of security training do employees receive at least once a year?

- 73%** Online training
- 39%** In-person training
- 29%** Updated security protocol manual for review



Take Away: Change their Minds, Change their Behaviors

- When it comes to data protection, agencies may be missing an important first step

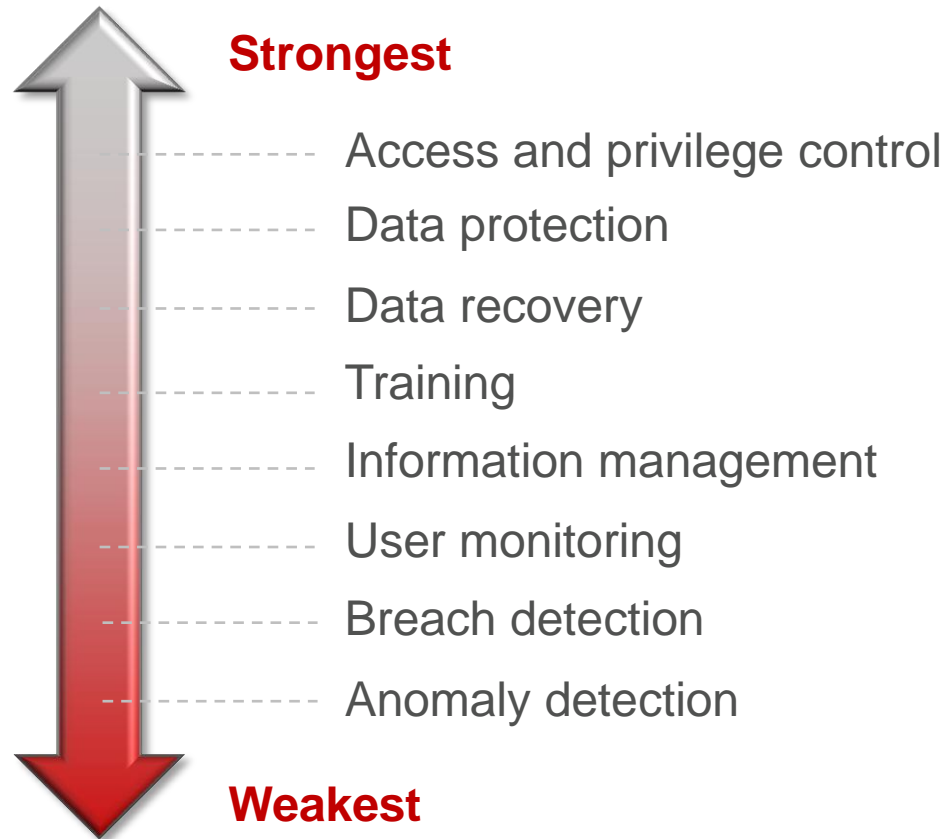


Feds estimate **43%** of their data repositories have not been identified and classified (*i.e., not sensitive, sensitive, critical, etc.*)

Take Away: Unidentified Data = Unprotected Data

- While defenses are strong in the area of access and privilege control, Feds see opportunities to improve breach and anomaly detection

How would you rate your agency's insider threat protection in the following areas?*

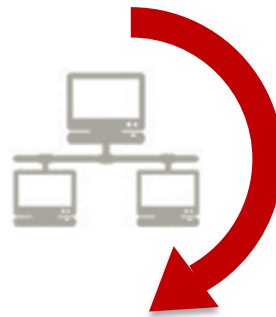


Take Away: Upgrade Trip Wires

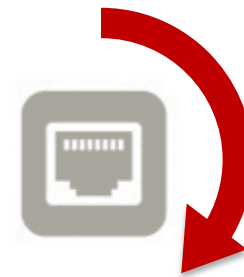
- More than 40% of agencies cannot tell the moment a document has been shared or how



45% of agencies cannot tell *if* a document has been inappropriately shared*



42% cannot tell *how* a document was shared*



34% cannot tell *what data* has been lost*

Take Away: Wanted: More Real-Time Alerts

- Fewer than half say security measures such as email encryption and two-factor authentication are used agency-wide

Where does your agency stand with each of the following technologies?*

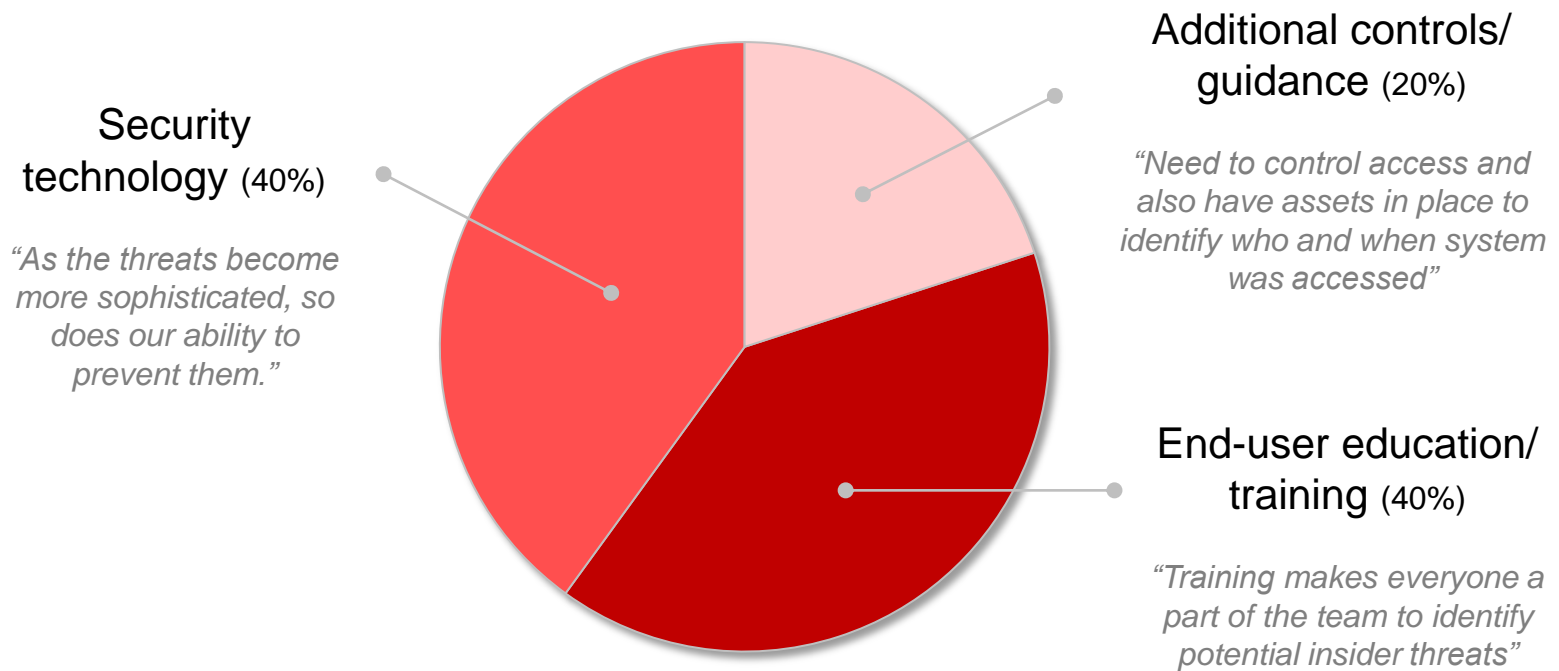
<i>Answer Options</i>	<i>Used agency-wide</i>	<i>Used selectively</i>	<i>Plan to implement within the next 2 years</i>
Data loss prevention	48%	36%	10%
Two-factor authentication	46%	33%	13%
Digital signatures	44%	39%	13%
Email encryption	43%	40%	9%
Endpoint encryption	40%	37%	18%
Access management solution	39%	39%	15%
File/folder encryption	37%	47%	12%
Anomaly detection	36%	45%	10%
Social mapping to track unusual behaviors	25%	30%	22%

42% say their agency has fewer than three of these measures implemented agency-wide

Take Away: Missing Key Entry and Exit Points

- Federal IT managers are undecided on the single best way to prevent insider threats

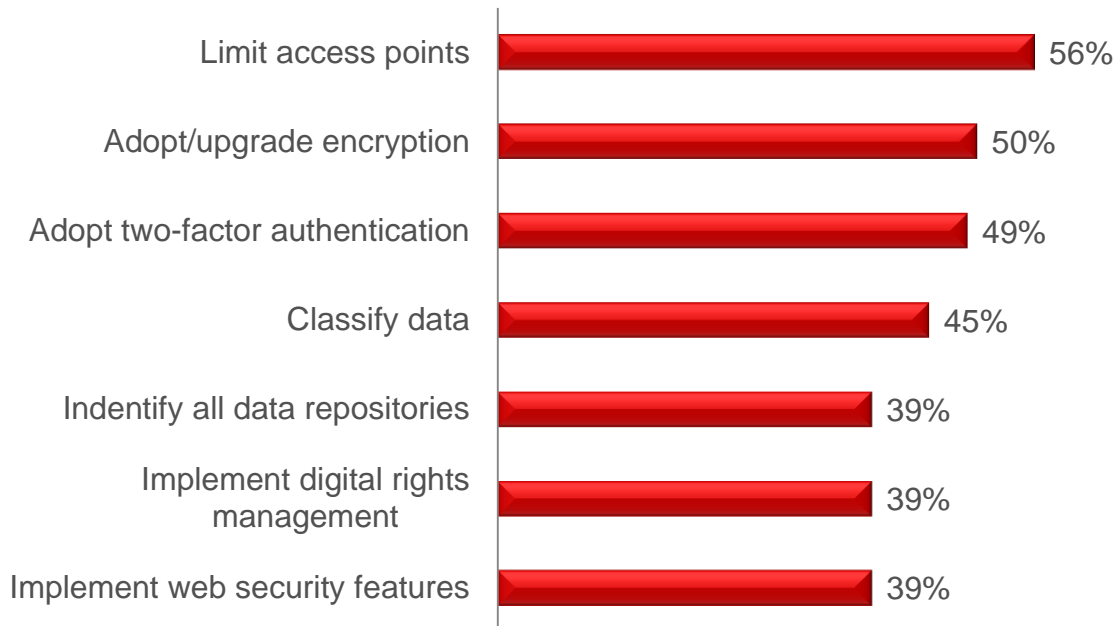
Overall, what do you believe is the *linchpin* to preventing insider threat activity?



Take Away: People, Process, and Technology All Critical

- To minimize data loss, Feds suggest limiting access points and upgrading technologies such as encryption and two-factor authentication

Going forward, how can Federal agencies minimize data loss when faced with an insider threat?*



How does your agency typically determine the success of these investments?

“Periodic security audits by an independent agency”

“Percentage reduction in threats over a time period”

“KPIs on threat discovery”



Take Away: Start with Access Points

- **Feds say government-wide efforts such as ISCM, CDM, and the Presidential CAP goals will also help combat insider threats**



77% of Federal IT managers believe that Presidential Cross-Agency Priority (CAP) goals will aid agency-wide government efforts to combat insider threats

The top CAP goals for agencies include:*

- #1** Enhancing security culture (47%)
- #2** Developing an insider threat prevention program (38%)
- #3** Sharing adverse information (35%)

Feds also believe ISCM (86%), CDM (82%) and DoD Directive 5205 (82%) will help

Take Away: Guidance Matters

Putting the Plan in Motion

- Agencies with formal insider threat programs are more likely to have robust security training, real-time alerts, and agency-wide security

The **55%** of Federal agencies with a formal insider threat program are also more likely to have:

Advanced training

including

- Annual In-person security training (51% to 18%)*
- Annual Security protocol manuals (37% to 20%)*
- Phishing exercises (69% to 33%)*



Real-time alerts

for

- Inappropriate access (73% to 33%)*
- Inappropriate sharing (59% to 36%)*
- Data loss (73% to 36%)*



Agency-wide security

for

- Access management solutions (51% to 27%)*
- Endpoint encryption (51% to 27%)*
- Anomaly detection (47% to 18%)*



Take Away: Formalize for Results

Start with a Formal Insider Threat Program:

Developing and executing on a formal program can help agencies expand training, take advantage of real-time alerts, leverage cyber intelligence, and enhance agency-wide security

Scale Up Training & Technology:

Frequent, hands-on employee training is critical to improving security habits within agencies. But, people will make mistakes – so agencies must rely on robust security systems as a vital second line of defense

Leverage Government Momentum:

Feds say government-wide efforts like ISCM, CDM, and the Presidential CAP goals will enhance the overall security culture and help combat insider threats



Methodology and Demographics

- MeriTalk, on behalf of Symantec, conducted an online survey of 150 Federal IT managers familiar with their agency's cyber security in July and August 2015. The report has a margin of error of $\pm 7.97\%$ at a 95% confidence level

Job Title:	
9%	Senior IT leadership
35%	IT director/supervisor
16%	IT systems engineer or solutions architect
15%	Cyber security or network manager
5%	Data center manager
20%	Other IT manager

Agency Type:	
64%	Civilian agency
36%	DoD or intelligence agency

100% of managers are familiar with their organization's cyber security efforts



Thank You

Lisa Fisher
703-883-9000 ext. 156
lfisher@meritalk.com

meritalk.com