Inside Job: The Sequel

Underwritten by Symantec.

The 2017 Federal Insider Threat Report

Defending against insider threats is a top Federal cyber priority. But, "inside" is becoming a much bigger space to manage. To understand this shift and build on the **2015 Inside Job report**, MeriTalk surveyed 150 Federal cyber security professionals.

Federal agencies raise their focus:

85% say their agency is more focused on combating insider threats today than one year ago

And, most are formalizing efforts:

86% say their agency has a formal insider threat prevention program

But still:

42% Agencies are the target of cyber incidents perpetrated by insiders at roughly the same rate as two years ago

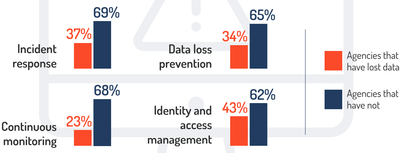
WHY?

Incomplete formal prevention efforts:

- **34%** don't have systems for reporting and maintaining records on data loss
- **39%** don't have systems for reporting and maintaining records on insider incidents
- **40%** don't have formal threat response protocols
- **45%** don't have employee training programs

Gaps in critical technology:

Agencies that have lost data to insider incidents are less likely to use key technologies agency-wide:



Cloud complications:

59% say the increasing number of cloud-based systems has made insider threats **more difficult** to detect

Biggest challenges?

- Increased complexity/number of systems to manage — 53%
- Difficulty monitoring all endpoints — 48%
- Lack of preventative measures — 41%
- Difficulty implementing and enforcing identity and access management policies — 41%

Going forward, how can Federal agencies minimize data loss when faced with insider threats?

1. Limit access points
2. Adopt multi-factor authentication
3. Adopt/expand real-time activity monitoring
4. Classify data and implement data loss prevention capabilities

Applying policies universally may also help address cloud concerns and maximize data protection

To view the full report, visit:

meritalk.com/study/inside-job-the-sequel

Underwritten by Symantec.