Combating insider threats

Enable security across any device, from any location

Highly publicized security breaches have brought insider threats into the eye of the government. Recent federal initiatives and executive orders aimed to mitigate these threats still leave defense, intelligence and civilian agencies vulnerable and in need of stronger measures to manage documents and data rights within their organizations.

Data breaches are on the rise:

60,753 events — Fiscal 2013

Nearly 70,000 events — Fiscal 2014

Federal agencies reported **15% more** information security incidents

In one year, data breaches:

Exposed 17.3M documents

Costing IT leaders an estimated **$860K** in data loss and downtime

The biggest threat comes from within.

The majority of federal breaches were traced to government employees and contractors.

- 21% — Violated policies
- 16% — Lost or had devices stolen
- 12% — Improperly handled sensitive printouts
- 8% — Ran or installed malicious software
- 6% — Were enticed to share private info

"With insider threats, there is no single solution…Three key focus areas to address insider threat from a solutions approach are behavioral, physical and technical."

— Daniel Bradford, U.S. Army Network Enterprise Technology Command (NETCOM), Fort Huachuca, Arizona, January 29, 2015

Behavioral

DoD is doing a better job at training than civilian agencies.

- 71% of the DoD sector cited end-user training as a priority.
- 55% of civilian agencies prioritize training differently.

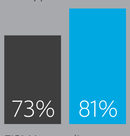
Physical

Protecting devices and portals is an important step.

Two-factor ID checks were related to and could have stopped 65% of incidents.

Technical

Agencies protect assets through encryption and other means.



Federal Information Security Management Act (FISMA) compliance increases

FISMA compliance averages have increased in security areas by adopting configuration management, remote access authentication and email encryption.

But more work still needs to be done.

Only 72% of DOD employees with significant security responsibilities have taken security training. — 72%

Three-quarters of agencies, up from about two-thirds in the previous year, have employees use ID cards to access their computers instead of entering log-ins and passwords.

To further increase FISMA compliance and reduce the risk of insider threats and data breaches, individual documents must be protected.

Preventing threats is an ongoing mission, but dealing with breaches is essential too.

Agencies expend a lot of effort anticipating insider threats—but if a breaches occurs, they must be able to identify it and execute a proper course of action, as required by FISMA.

On average, it takes **87 days** to recognize that insider fraud has occurred, and **105 days** (more than 3 months) to get to the root of the problem.

A holistic approach to managing documents and data is necessary.

Implementing analytics into document management allows for tracking and activity monitoring to mitigate a breach before it happens and minimizes downtime should it occur. The approaches agencies should take include:

- Analytics to track unusual content consumption behaviors
- Analytics to track who is using specific documents
- Fine-grained access control within content management systems
- Multiple isolated access networks
- Digital rights management
- Content redaction
- Encryption
- Digital signatures

Adobe Government solutions give you the tools you need to create engaging communications for any medium, easily manage assets and deliver to any device, and measure the success of your communications plan.

Find out what Adobe can do for your department or agency today.

To access the infographic, visit blogs.adobe.com/adobeingovernment/mitigating-insider-threat-with-digital-rights-management.

Sources:

Nextgov—6 Biggest Blunders in Government's Annual Cyber Report Card, March 2015

Symantec—Understanding Insider Threats Through Data Loss Prevention, June 2014

SC Magazine—IT leaders count the cost of breaches, data loss and downtime, November 2013

C4ISR & Networks Editorial Webcast–"Insider threats and protection of military networks"

Federal Times—Cybersecurity priorities shift to insider threats, November 2014

Office of Management and Budget—Annual Report To Congress: Federal Information Security Management Act, February 27, 2015

Newsmax—Feds Hit by Record-High 70,000 Cyberattacks in 2014, March 2015

Cisco—The High Cost of Insider Threats, November 2008

Business Insider— The U.S. Government is Struggling to Protect Social Security Numbers and Military Secrets, November 2014

High Tech Highway—The Cost of Insider Threats, May 2013