6 Easy Ways to Expose Government Data

SailPoint

How do you protect access to sensitive data that multiplies in size and is saved across disparate locations across your organization? Within any government agency, sensitive information will regularly find its way into spreadsheets, slides and other unstructured formats that are then saved in a variety of file stores such as SharePoint, NAS devices, and cloud storage. This continuously happens as people and even software bots run nightly reports, while others explicitly copy and paste data into documents and presentations. In addition, hard copy documents are regularly scanned, digitized and stored electronically. These activities create a sea of files, also referred to as "unstructured data." If left unmanaged, the U.S. Department of Defense (DoD), the intelligence community and other federal agencies run the huge risk of exposing sensitive information.

So how can federal agencies prevent losing this data through inappropriate access? **Here are six ways in which data is typically exposed.**

1 Ignoring Open Access

Open repositories such as folders and containers that have little or no access controls are a natural spot for data to accumulate. In many cases, this includes highly sensitive information. This data is easy to use and share. Furthermore, this data is a natural target when automated processes are used to share data. The longer these data files exist, the more uses people find for them. All this leads to the **first big miscalculation: overlooking where sensitive data resides.**

2 Never Checking an Account's Access Paths

User access to file folders is commonly managed in a variety of ways, with well-intentioned policies and access groups quickly giving way through nesting and misuse into a clutter of tangled access paths that resembles spaghetti. So, removing the user from one spot often doesn't have any effect on their actual access. This leads to **the second common oversight: presuming there's only one way to gain access.**

3 Manually Reviewing All Access Events

Leaving no stone unturned becomes impossible when you're talking about covering mountains of event data including file modifications, access changes and folder renames. Without using identity information and common sense to filter out regular traffic, examining every event activity becomes impossible. This means high-risk activity may slip by and go unchecked or worse, discovered long after the activity occurred. **Misstep number three is simply trying to boil the ocean by not using identity context to filter out the low-risk event data.**

4 Treating All Folders Equally

A folder containing sensitive data and a folder containing some downloaded articles do not contain the same risk, yet many organizations treat all folders equally. This means that you aren't focusing your governance time and dollars where it will have the most effect. Instead of classifying the type of data located on file folders, identifying open access material, and prioritizing efforts around content with the highest levels of activity, **the fourth mistake is not prioritizing access to file folders based on sensitivity of content.**

5 Making IT Review All the Access

Who better to review access to files than IT, right? After all, IT is responsible for the infrastructure and ensuring access is secure and appropriate. Add to that, no one else has the time. That may not be how some government agencies feel or think, but it's how many act. The reality is that IT does not possess the contextual knowledge of users, the data stored and the location of sensitive information. It is the business users that have this context and are pivotal to ensuring only the right people gain access. Yet, the burden of protecting sensitive data often falls on IT and security teams. **Error number five is not sharing responsibility across all departments.**

6 Using As Many Different Tools to Enforce Your Governance Policies

It is common to develop a layered approach to security that's very effective when using tools that do different jobs. However, when federal agencies govern different cloud vendors with different tools and then add more tools for on-premises storage, NAS and SharePoint, it results in a risky siloed approach to controlling access. Not only does this inconsistent approach lead to security gaps that attackers can exploit, it also makes it difficult to gain a complete view of your risk exposure as well as to respond to changes and new operational directives as multiple tools require multiple attempts to cover the same problem. **Over-diversification of tools is bad idea number six.**

According to Gartner, an estimated 80% of the world's data is unstructured.[1] And 1 in 4 users will save sensitive data to cloud apps or share it with someone else.[2] It's time to tame the sea of unstructured data. It's time to extend identity governance to data stored in files. Here are the six things the U.S. Department of Defense (DoD), the intelligence community and other federal agencies should do to protect sensitive data.

[1] Gartner, *Organizations Will Need to Tackle Three Challenges to Curb Unstructured Data Glut and Neglect*

[2] SailPoint, *Market Pulse Survey 2017*

1. Find and remove open access.
2. Minimize multiple paths of access.
3. Automate real-time activity responses.
4. Discover where sensitive data resides and apply appropriate access controls.
5. Leverage business users (or line of business users) to participate in information security efforts.
6. Implement one tool for the job.

Why is SailPoint Your Ideal Partner?

With more than 60 government agencies already using SailPoint to manage more than 3 million identities, SailPoint is the most trusted name in identity governance. Our long record of success is the foundation upon which SailPoint builds innovations such the infusion of artificial intelligence and machine learning into our proven identity platform. By taking this evolutionary approach, SailPoint enables government agencies to reduce cybersecurity risk **without having to take a leap of faith on unproven platforms.**

SailPoint's Government Pedigree

Support

- NIST 800-53 security Controls
- Implementation of the FICAM services for identity management
- ICAM Modernization Strategy
- FIAR and FISCAM security controls
- Protection of HVA by implementing security controls

Deployed

- At 23 CFO Act agencies to support the DHS CDM Master User Record
- DISA for identity lifecycle

Authorized

- To operate on America's most sensitive DoD and intelligence community networks

Certified

- NIAP Common Criteria

Pursuing

- FedRAMP Authorization

To learn how other federal agencies are leveraging SailPoint **contact us or schedule a demonstration.**

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.