Data Risk Report…

Overview

Before going through the findings, check out these key terms and how we classify them as they come up throughout the report.

- Sensitive files: contain credit card information, health records or personal information subject to regulations like GDPR, HIPAA and PCI.
- Global access, exposed files and folders: indicates files and folders open to everyone (all employees). This data represents the biggest risk.
- Stale data: information no longer needed for daily operations.
- Stale user accounts (AKA “ghost users”): enabled accounts that appear inactive and often belong to users who are no longer with the organization or company.

Scope of the Risk Report

Some of the 30+ industries covered include healthcare, pharmaceuticals, biotech, retail, financial services, tech, manufacturing, energy and utilities, education, defense and government (local, state, and national). See some more precise figures below:

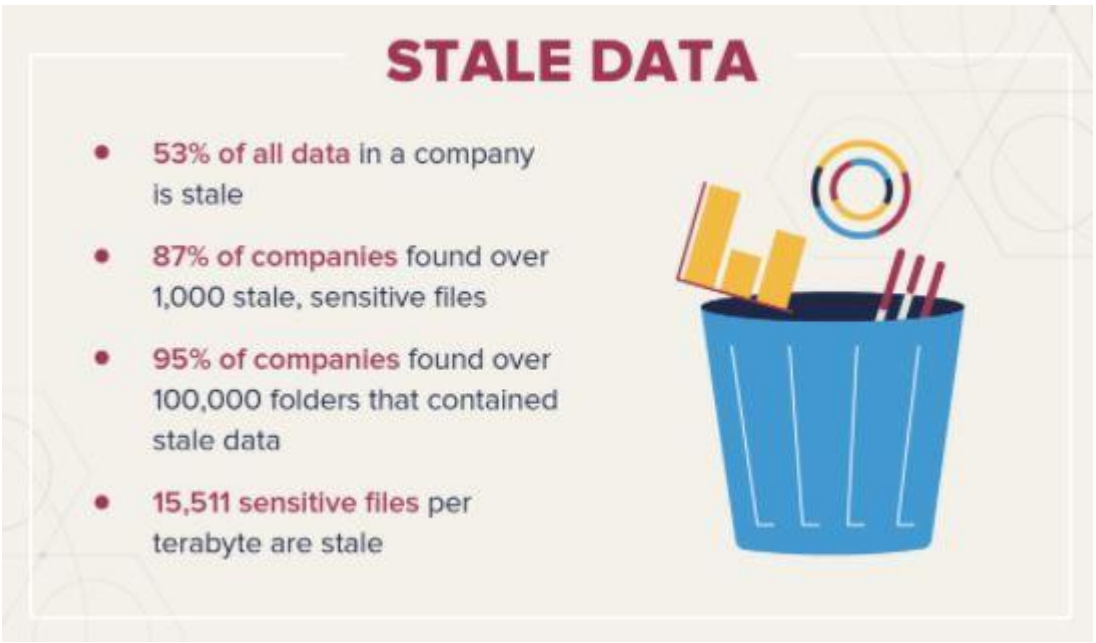
- Total data: 54.58 petabytes
- Folders analyzed: 4,332,290,346
- Folders with global access: 953,616,561
- Files analyzed: 53,885,498,652
- Files with global access: 13,445,993,510
- Total number of user accounts: 12,754,608
- Average number of folders per TB: 128,782
- Average number of files per TB: 1,460,000
- Number of exposed, sensitive files per TB: 3,144

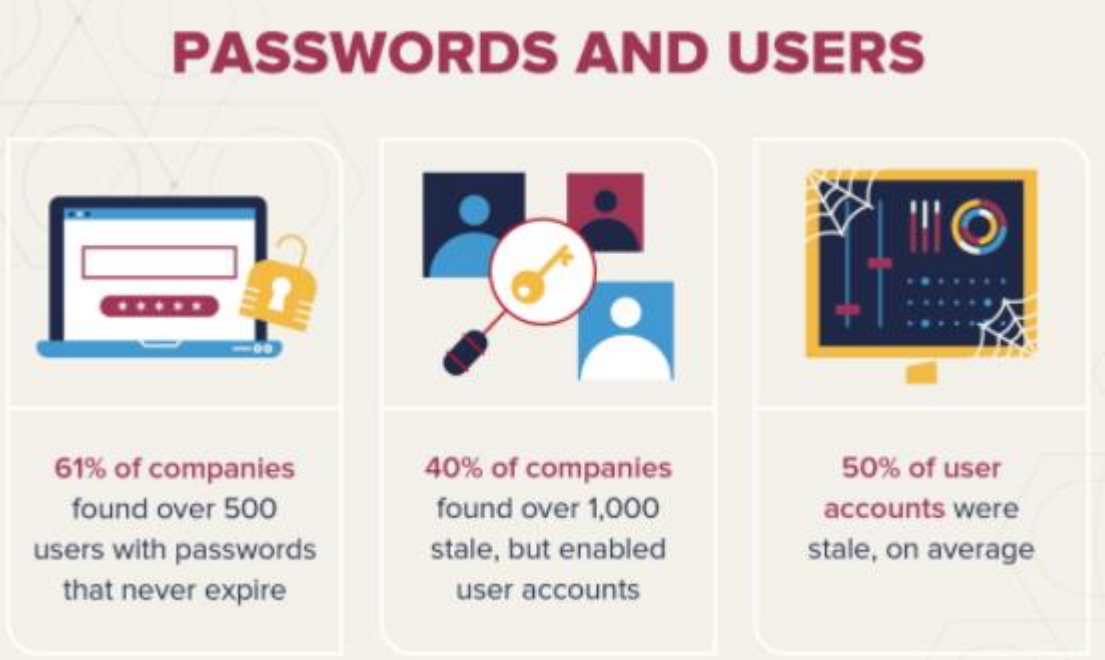
Data Risk Report Findings

Globally accessible data also puts organizations at risk from insiders and outside attackers.

It could just take one accidental click on a phishing email or other scam to set off a chain reaction that encrypts or destroys all accessible files.

- 17% of all sensitive files were accessible to all employees
- 15% of companies found 1,000,000+ files open to every employee
- On average, every employee had access to 17 million files





- 38% of all users sampled have a password that never expires
- 11% of enabled users have expired passwords
- 58% of companies were found to have over 1,000 folders that had inconsistent permissions
- 27% of a company's users had removal recommendations and were likely to have more access to data than they require

---

What Does the Data Risk Report Say About Your Company?

Your company or a company you patronize likely has these four risks looming over their security:

- Over-exposed sensitive data
- Sensitive stale data
- Stale accounts
- Non-expiring passwords

Who's Most At-Risk?

1. Financial services: 21% of sensitive files were exposed
2. Manufacturing: 21% of sensitive files were exposed
3. Healthcare, Pharma & Biotech: 15% of sensitive files were exposed
4. Energy & Utilities: 14% of sensitive files were exposed
5. Retail: 14% of sensitive files were exposed
6. Government & Military: 12% of sensitive files were exposed

---

Learn & Improve

Minimize Risk & Exposure:

- Identify and fix global access groups that grant access to sensitive data
- Ensure only appropriate users retain access to sensitive, regulated data
- Routinely run a full audit of your servers, looking for any data containers (folders, mailboxes, SharePoint sites, etc.) with global access groups applied to their ACLs
- Replace global access groups with tightly managed security groups
- Start with the most sensitive data and test changes to ensure issues do not arise
- Apply additional "preventive controls"— like encryption— through digital rights management (DRM)

Eliminate Stale Data:

- Minimize the sensitive data you collect, who gets to see it and how long you keep it
- Identify stale data — especially sensitive information
- Create a predetermined data retention period
- Archive or delete stale data if no longer needed

Limit Passwords & Users:

- Hunt and eliminate stale accounts and non-expiring passwords
- IT must disable non-expiring passwords and set passwords for all users to expire at set intervals
- If an account requires a static password, it must be extremely long, complex and random
- Use enterprise-wide password managers and two-factor authentication, as well as monitoring and alerting on suspicious failed login attempts
- Make sure stale accounts are disabled and monitored to re-enable activity or delete the account
- Implement procedures to ensure that all user accounts are active, governed and monitored

- Understand what constitutes normal behavior on both user and service accounts so you can be more effective at spotting inactive users and behavioral abnormalities
- Boost your anomaly detection capabilities and response processes