Protecting Intellectual Property from Insider Threats

*Powered by*

*Data Behavior Analytics (DaBA)*
TABLE OF CONTENTS

3. EXECUTIVE SUMMARY

4. RISKY DATA DESTINATIONS

5. RISKY USERS IDENTIFIED
EXECUTIVE SUMMARY
FOR Acme

Key Findings:

- 328 unique data silos storing sensitive data identified, representing a growing issue of data sprawl. As sensitive data moves outside of an organization's control, business are at a higher risk of leaks and theft.

- 23 high-risk destinations containing 100's of sensitive files observed, including those that the business identified as business critical.

- 2 malicious insider detected exfiltrating multiple sensitive files on 3 separate occasions

- 3 negligent employees detected using privileges to bypass data handling controls

- 1 careless employees detected emailing sensitive data to incorrect destinations

The Data Risk Assessment summarizes the business and security risks associated with business critical data as defined by Acme. The data used for this analysis was gathered by Cyberhaven during the report time period. The report provides actionable intelligence around the sensitive data flows exposing risk that can be employed to reduce the organization's overall risk exposure.
23 high-risk destinations identified:
Removable Media, Personal Email, Social Media, External Cloud Storage, Instant Messaging, Unsanctioned Applications, Non-HTTPS Websites and more.
The high-risk destinations are displayed below. This data can be used to more effectively prioritize your sensitive data control efforts.
2 malicious insiders identified

Malicious insiders displayed below. This data can be used to build a case to terminate identified employees and highlights controls needed to prevent in the future.

Mary has made a clear attempt to hide the file to bypass security prior to exfiltration.

Alex discovers sensitive data in a public repository then exfiltrates using personal email.
3 negligent insiders detected

Negligent insiders displayed below. This data can be used to enforce data handling controls, provide risk training to employees identified and highlights controls needed to prevent in the future.

- Roberta is uploading files to Flikr bypassing approved internal collaboration tools.
- Marcus is using unsanctioned external storage.
- Jack is storing passwords in a text file and using unsanctioned external storage.
1 careless insider detected

Careless insider displayed below. This data can be used to enforce data handling controls, provide risk training to employees identified and highlights controls needed to prevent in the future.

Sam sent confidential information to the wrong destination

DaBA Visibility Thwarts Insider Threats

◆ FUTURE PROOF COVERAGE
No need to predict future breaches; no need to create policies; you are always covered!

◆ GRAPHIC VISIBILITY INTO ALL DATA SILOS
Automatic, effortless visibility into any location your data is in — endpoints, servers, email, proprietary apps and databases, SaaS, custom cloud apps

◆ RAPID RESULTS WITH NO MANUAL WORK
No need to stitch together incidents from several tools to get visibility into your data or investigate a breach. No continuous maintenance of policies, no incident fatigue because of policies that are too broad

Contact us at info@cyberhaven.com