aiimi

SAMPLE REPORT | FOR: DEMONSTRATION

DATA RISK ASSESSMENT.

THIS RISK ASSESSMENT IS DESIGNED TO PROVIDE YOU WITH A 'STATE-IN-TIME' REPORT ON YOUR DATA RISK SURFACE AREA RIGHT NOW. WE ALSO PROVIDE SOME BESPOKE REMEDIATION RECOMMENDATIONS TO HELP YOU MAINTAIN A STRONG DATA GOVERNANCE POSTURE, HOWEVER YOU INTEND TO PROCEED IN THE FUTURE.

SCOPE OF DATA AT REST.

_DATA SOURCES.

_DATA SOURCES MONITORED.

- USER SHARE
- COMPANY
- PRODUCTION
- SHAREPOINT

_CONTENTS.

- 760,525 FILES
- 672.66 GB OF DATA

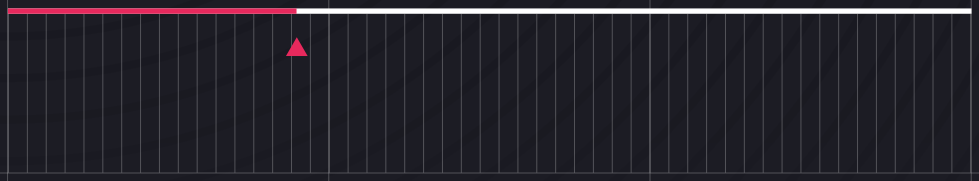
_A SAMPLE OF YOUR COMPANY'S DATA WAS ASSESSED IN THE FOLLOWING AREAS:

- FILES CONTAINING SENSITIVE DATA (HIPAA/GDPR/PCI/SOX)
- OVEREXPOSED, REGULATED, & SENSITIVE DATA
- STALE, REGULATED, & SENSITIVE DATA
- ACCESS GOVERNANCE PROFICIENCY
- DATA PRIVACY & COMPLIANCE PROFICIENCY
- ASSOCIATED RISK LEVELS

KEY FINDINGS.

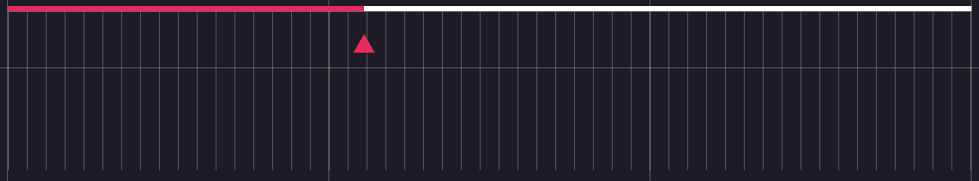
_SENSITIVE DATA DISCOVERY. *Percentage of total data that is sensitive.*

30%



_DATA EXPOSURE. *Percentage of total data that is overexposed.*

37%



_STALE DATA. *Percentage of files not accessed within the last 90 days.*

95%

DATA THAT IS OPEN TO EVERYONE.

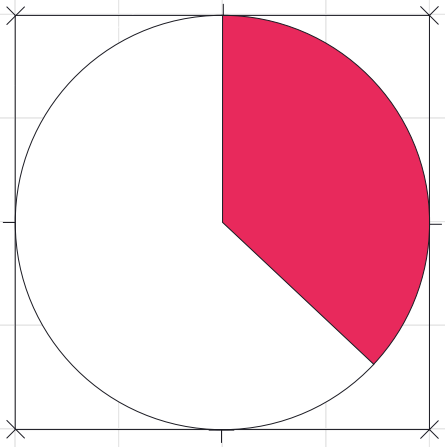
_CONSIDER.

Overexposed data is a common security vulnerability, and excessive access is one of the primary causes of data breach – this is particularly relevant to critical sensitive data. Managing access manually can be very time consuming and is open to error, so we advise operating an automated data governance mechanism where possible. This can reduce overall risk and be demonstrated to regulators where required, to prove commitment to information protection legislation and act as a post-incident investigatory aid.

_RECOMMENDATIONS.

- REMOVE GLOBAL ACCESS GROUP PERMISSIONS TO IDENTIFY FOLDERS OPEN TO GLOBAL GROUPS.
- PLACE ACTIVE USERS IN A NEW GROUP.
- REPLACE THE GLOBAL ACCESS GROUP WITH THE NEW GROUP ON THE ACCESS CONTROL LIST.

_RISK LEVEL.



37 PERCENT.

RECORDS ACCESSIBLE TO EVERY EMPLOYEE.
(284,489 / 760,525)

SENSITIVE DATA.

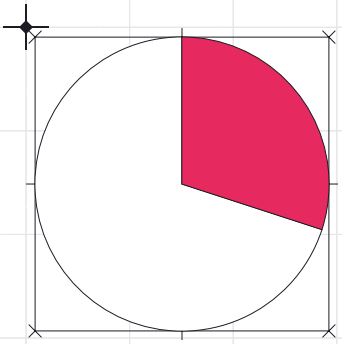
_CONSIDER.

We've discovered that as many as 30% of the files and folders in your environment may contain critical information about employees, customers, projects, clients, or other business-sensitive content. Much of this data may be subject to regulations such as SOX, HIPAA, PCI, GDPR, GLBA, and more.

_RECOMMENDATIONS.

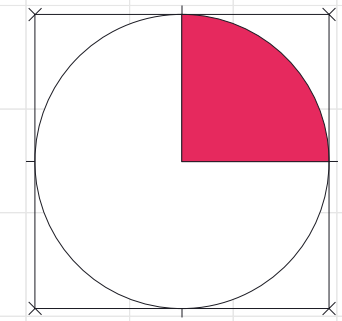
- ONGOING CLASSIFICATION OF CORPORATE DATA, HIGHLIGHTING REGULATED AND SENSITIVE DATA.
- IMPLEMENT A MECHANISM TO UNDERSTAND WHERE SENSITIVE DATA EXISTS IN THE ENVIRONMENT.

_RISK LEVEL.



230,503+ FILES.

CONTAIN SENSITIVE DATA
(230,503 / 760,525)



70,228+ FILES.

SENSITIVE FILES ARE OPEN TO ALL EMPLOYEES

STALE DATA.

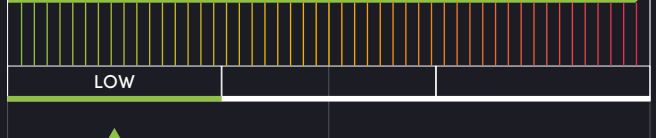
_RECOMMENDATIONS.

Stale data (data that has been kept beyond a pre-determined retention period or has not been used in a while) can be expensive to store and manage. This poses an increased and unnecessary security risk.

_CONSIDER.

- IDENTIFY STALE DATA AND DETERMINE THE DATA YOU CAN MOVE, ARCHIVE, OR DELETE.
- IMPLEMENT A POLICY TO MANAGE STALE DATA.

_RISK LEVEL.



FILES NOT ACCESSED.

IN THE PERIOD OF
1 YEAR

_84% OF ALL FILES WERE NOT ACCESSED.
_31% OF FILES NOT ACCESSED ARE SENSITIVE.

(642,942 / 760,525)
(200,804 / 642,942)

IN THE PERIOD OF
90 DAYS

_94% OF ALL FILES WERE NOT ACCESSED.
_29% OF FILES NOT ACCESSED ARE SENSITIVE.

(721,990 / 760,525)
(212,010 / 721,990)

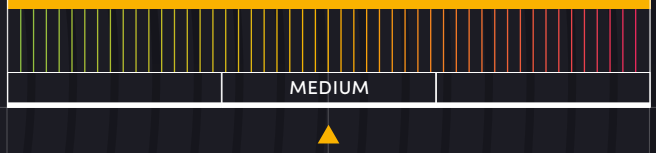
POTENTIALLY

130,000+ FILES

HAVE BEEN DUPLICATED

OVERALL RISK.

_OVERALL WE DEEM YOUR RISK POSTURE AS:



- BASED ON THE DATA POINTS WE HAVE CRAWLED, ENRICHED, AND ANALYSED, WE DEEM YOUR RISK LEVEL AS MEDIUM RISK.

_HIGH RISK.

- **230,503 (147GB)** RECORDS CONTAIN SENSITIVE INFORMATION
- **70,228** SENSITIVE FILES ARE AVAILABLE TO ALL IN THE ORGANISATION
- **95,918** STALE DATA RECORDS ARE OVER 5 YEARS OLD AND CONTAIN SENSITIVE INFORMATION
- **111,393** RECORDS ARE DUPLICATES THAT CONTAIN SENSITIVE INFORMATION

_RECOMMENDATION

Ensure that permissions on files and folders are authorised, and you are not creating users with excessive permissions. Classify data based on its sensitivity and segment your network accordingly. Keep sensitive data separate from less critical information; this makes it harder for unauthorised users to access sensitive data. Consider automated data classification on newly created, modified files and folders. Conduct regular audits and assessments to determine if sensitive data is an ongoing risk.

_MEDIUM.

- **31,181** SENSITIVE DATA RECORDS ARE MORE THAN TEN YEARS OLD
- **214,261** NON-SENSITIVE FILES ARE OPEN TO EVERYONE IN THE ORGANISATION

_RECOMMENDATION

Reducing the amount of stale data (data that is outdated, no longer needed or irrelevant) is essential for maintaining efficient data management and reducing security risks. Implement an archiving strategy for less frequently accessed data. Move stale data to long-term storage or archive to free up space on primary systems. Consider utilising a deletion schedule and define a time period for the deletion of stale data in accordance with legal and regulatory requirements. Ongoing data classification and discovery can help here.

_LOW RISK.

- **130,896** DUPLICATE FILES
- **TOP FIVE USERS WITH ACCESS TO THE HIGHEST NUMBER OF RECORDS:**
  /ADMIN1
  /USER1
  /USER2
  /USER3
  /USER4

_RECOMMENDATION

Schedule regular data clean-up activities and periodic data audits to identify duplicate files and data. Automated ongoing Data Discovery and data governance can help to reduce duplicate files. Review the access control lists of individuals who have visibility over corporate data to ensure that current levels are appropriate, and that access is still required.

WWW.AIIMI.COM