Accordingly discovering and classifying sensitive data is essential to protecting it. A key strategy in achieving this involves auditing data to identify and catalog huge volumes of data to be protected.

What types of classification are needed?

- PII
- PHI
- FPI
- FHP

Who is responsible for classification?

- Creators
- Owners
- Users
- Auditors
- Stewards

What’s at stake?

- Regulation
- Reputation
- Firewalls

The cost increases following data theft which are primarily due to the additional expenses required to protect the organization’s brand reputation. (Data and link to study from Internet Security Report, About.com)

What is the impact of poor or no classification?

- Classifying your sensitive data prevents and reduces 45% of breach events.

How to tackle classification?

- Automate classification, reducing human error.
- Increase security efficiency across a Data Loss Prevention (DLP)Portfolio.
- Reduce post breach risk.
- Future proof your security program.

Start protecting your data today.