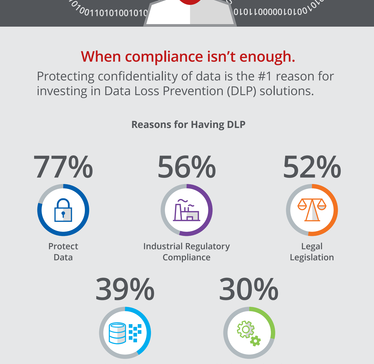
McAfee
Together is power.

Who let the data out?

How serious is data loss? Serious enough that 68% of breaches required public disclosure.[1]



When compliance isn't enough.

Protecting confidentiality of data is the #1 reason for investing in Data Loss Prevention (DLP) solutions.

Reasons for Having DLP

77% Protect Data

56% Industrial Regulatory Compliance

52% Legal Legislation

39% As a Direct Result of a Data Loss Incident

30% Understand and Manage the Data We Have

Education and sharing results are critical.

86% of employees are trained to associate value to data...

but only...

33% of security teams are sharing DLP results with business groups.

How can they improve without feedback?

You can't protect it if you don't detect it.

Monitoring one employee activity averages 17 daily incidents.[2]

Monitoring five employee activities averages 58 daily incidents.[2]

Big Events Create Bigger Risks

Launching a product? Going through a re-org? Get your team ready! Be sure to keep your guard up during these common events, which cause an increase in data loss.

Respondents report that the following business actions increase data loss incidents:

40% New Project Deployment

38% Internal Reorganization

35% New Product Launches

33% Corporate Strategic Planning Activities

29% Peak Seasons of Demand

25% Merger/Acquisition or Divestiture

25% Financial Disclosures

24% Employee Social Media

Healthcare and manufacturing are hot targets for cybercriminals.

Industries that have less mature systems are potential sitting ducks as data theft shifts to personal health data, intellectual property, etc.

Respondents claiming to have a fully deployed solution that meets all requirements–by vertical.

53% of Organizations Feel You Need 6 (or More) Full-Time Employees Dedicated to DLP[3]

Want to learn more?

Read the entire report and discover more about how to better prevent data loss by visiting: www.mcafee.com/safeguarddata

Follow us on Twitter: @McAfee #WhoLetTheDataOut

McAfee
Together is power.

1. 2015 McAfee, Grand Theft Data.
2. Activities include suspicious use of email, inappropriate use of company financial data, etc.
3. Based on 5,000 or more employees