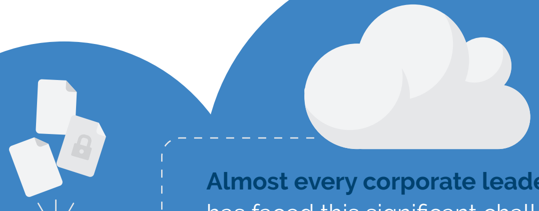
Do You Know

WHAT YOUR CORPORATE DATA DID IN THE CLOUD LAST NIGHT?

Managed Methods

3 out of 4 companies
have experienced loss or theft of important data.*



Almost every corporate leader has faced this significant challenge to their business and reputation!

HOW DID DATA INSECURITY BECOME THE NORM?

1. Data needs to flow

The pace of modern business requires information to flow quickly and efficiently to those who need it to do their jobs; **we need the data now!**

Cloud collaboration apps allow Jim (Finance) can access key customer purchase data from Susan (Operations).

88% of end users say their jobs require them to access and use proprietary information.*

2. More accessibility, more problems

When data is easily accessible, it's **easily abused**. Often problems occur by accident, not maliciously.

A simple user error, like uploading a sensitive file to the wrong folder in Dropbox, can result in the accidental disclosure of client data, trade secrets, and even health records.

Data abuse is more than twice as likely to be due to innocent employee behavior than cybercrime.*

*Closing Security Gaps to Protect Corporate Data, Ponemon Institute

THE SOLUTION

Aside from removing all data access or firing all employees, what can you do to **protect your company?**

Cloud Access Monitor, ManagedMethods' CASB solution, provides all critical features plus APIs to Office 365, Google Apps, and other popular platforms.

Visibility

CASBs provide visibility into the use of collaborative cloud apps.

See who is using which apps on what devices, even if they're outside the corporate security perimeter.

Control

Know what type of data is being shared and adjust access.

Is it credit card or social security numbers? Proprietary development code?

Detect and rectify suspicious data behavior before your company becomes another statistic.

Want to see how a CASB can protect against innocent insider security mistakes?

Visit managedmethods.com

powered by contellio