TRENDS AND FUTURE DIRECTIONS IN DATA SECURITY
Financial services enterprises continue to be a target for both traditional employee theft and criminal hackers trying to steal assets. Insider threats, inside jobs and bank robbers have been around as long as we've had banks. Today, employees with legitimate access, service providers or contractors that maintain infrastructure and privileged users are all possible insider threats to financial services organizations, along with the compromise of their credentials.

Criminal hackers continue to be a top worry for financial services organizations, and nearly every financial sector breach has included a compromise of a privileged user account or a privileged account in a partner with access to the enterprise's network.


WHERE DO INSIDER THREATS COME FROM?

Most vulnerable segment

97% of respondents from U.S. FINANCIAL SERVICES organizations reported that they were vulnerable to insider threats.

Global

Financial Services

89%

U.S. Financial Services

93%

Healthcare

97%

Retail

93%

USA

82%

Germany

82%

FINANCIAL SERVICES ORGANIZATIONS ARE FAILING TO SECURE THEIR DATA

41% of respondents reported that they encountered a data breach or failed a compliance audit in the last 12 months.

27% are protecting data because of past breaches.

WHERE DO INSIDER THREATS COME FROM?

The most dangerous insiders

Privileged users include System Administrators, Network Administrators, Storage Administrators, Domain Administrators and other IT roles.

40% of contractors/service provider employees (Snowden was a contractor).

63% of privileged users.

43% of partners with internal access.

Data protection drivers for U.S. financial services enterprises

TOP 3 REASONS FOR SECURING SENSITIVE DATA

50% Reputation and Brand Protection

43% Compliance

42% Avoiding Data Breach Penalties

TOP 3 SECURITY SPENDING PRIORITIES

57% Protecting against a Data Breach Incident

43% Compliance

39% Fulfilling Compliance Requirements in Other Areas

The most dangerous insiders

Respondents from U.S. Financial Services Organizations top three selections for insiders that pose the largest risk to their organization were:

Financial Services greatest volumes of data-at-risk are in databases, on file servers or in cloud environments. Mobile devices are their area of biggest concern for greatest risk of loss.

Protection from data breach penalties as well as reputation and fraud protection are at the top of financial services organizations lists.


VOLUMES AND WORRIES

Highest volumes of sensitive data

Organizations are most worried about data on:

49% Databases

39% File Servers

36% Cloud

47% Databases

45% File Servers

42% Cloud

Financial services enterprises worry most about data on:

Databases

File Servers

Cloud

50%

50%

50%