2022 Thales Data Threat Report

Retail Edition
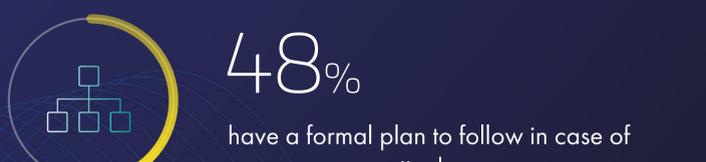
#ThalesRetailReport

cpl.thalesgroup.com

Security threats to Retail organizations
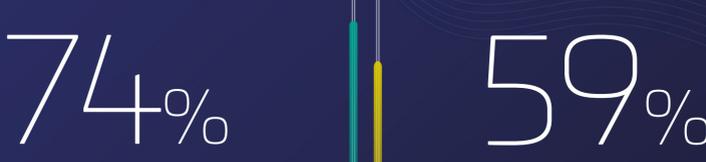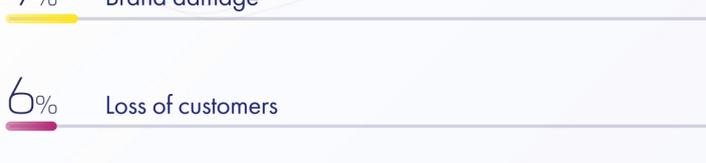
65%

ranked malware as the leading source of increased security attacks

52%

ranked ransomware as the leading source of increased security attacks

45%

reported increases in the volume, severity and/or scope of cyberattacks in the past 12 months

32%

experienced a security breach in the past 12 months

Ransomware has changed breach economics

20%

have experienced a ransomware attack

27%

were willing to pay ransom if needed

48%

have a formal plan to follow in case of a ransomware attack

Negative fallout of a ransomware attack

28% Financial Losses

20% Exfiltration of sensitive information

9% Brand damage

6% Loss of customers

3% Long-term business impacts
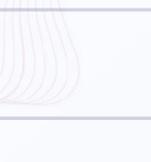
Security risks of continued remote working

74%

are concerned about the security risks of employees working remotely

59%

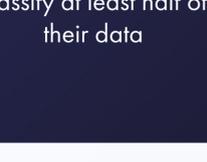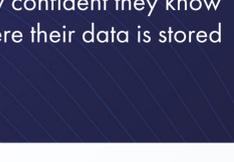of retail organizations utilize Multi-Factor-Authentication (MFA)

It is a multi-cloud world

68%

of retail respondents identified their environments as multi-cloud, and the same percentage (68%) said they have over 25 SaaS applications in use

Data Sprawl: Where in the world is my data?

46%

of retail respondents have complete knowledge or are very confident they know where their data is stored

23%

of retail respondents indicated they could classify at least half of their data

Encryption and key management challenges

x5

59%

reported having 5 or more key management solutions

only 18%

of retailers reported that 60% or more of sensitive data in the cloud is encrypted

Data Security for a Zero Trust World

- Discover and classify data anywhere
- Protect sensitive data at rest, in motion and in use
- Control user access to sensitive data and management of keys throughout their lifecycle