

# 2022 Thales Data Threat Report

Critical Infrastructure Edition

cpl.thalesgroup.com

#ThalesCIReport

### Security threats to critical infrastructure



security attacks

security attacks

55% ranked malware as the leading source of increased





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



experienced a security breach in the past 12 months

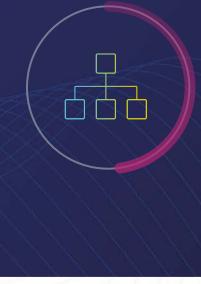
Ransomware has changed

## breach economics 19%



were willing to pay ransom if needed

have experienced a ransomware attack



a ransomware attack

45%

24%

have a formal plan to follow in case of

#### 6% 3% 10%

Negative fallout of

a ransomware attack



Security risks of continued remote working

are concerned

about the security

risks of employees

working remotely

of critical infrastructure

organizations utilize

Authentication (MFA)

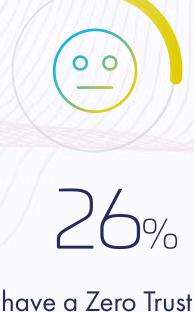
Multi-Factor-

Zero Trust strategy

have no formal

Zero Trust

strategy at all



strategy in

planning and

a formal Zero

have actively

embraced Zero

Trust policies and

research stages Trust strategy Where in the world is my data?



of critical infrastructure respondents had complete knowledge of where their data was stored

in the cloud

of respondents reported that over 60% of their cloud data is sensitive



# 62%

Encryption is still #1





Protect sensitive data at rest, in

data anywhere

Discover and classify

motion and in use Control user access to

sensitive data and

management of keys

throughout their lifecycle

451 Research S&P Global

Market Intelligence

Visit cpl.thalesgroup.com/critical-infrastructure to download the full report, including 451 Research recommendations

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales