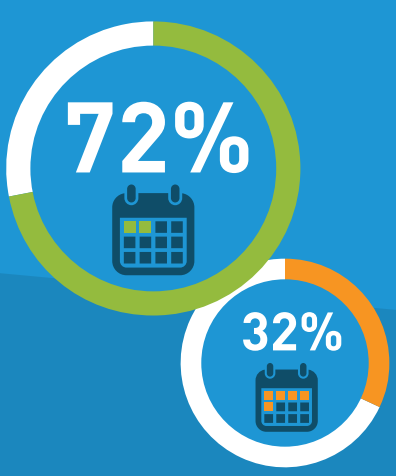
SecuriSync®

When an employee unwittingly triggers a RANSOMWARE ATTACK

Paying the ransom is the least of your worries – and may not even get your files back. No, really. Our crypto-ransomware survey revealed the biggest cost to businesses from an attack is actually downtime.



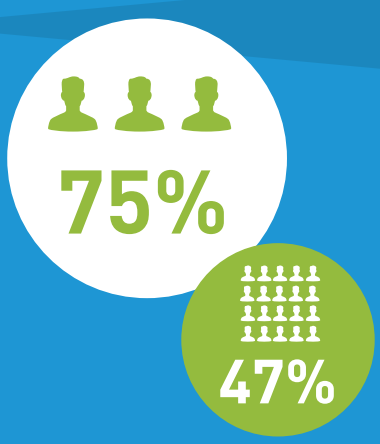
PRECIOUS FEW HAVE A BUSINESS CONTINUITY PLAN IN PLACE

72% of business users lost access to data for at least two days, and 32% lost access for five days or more.

DOWNTIME OCCURS EVEN IF YOU PAY RANSOM

52% of experts reported that the wipe-and-restore process took two or more days for infected devices.

Even worse: 19% of companies that paid the ransom still didn't get their files back.



RANSOMWARE TENDS TO HIT MULTIPLE USERS AT ONCE

75% of outbreaks affected three or more people, and 47% of outbreaks spread to at least 20 people.

DOWNTIME TRIGGERS ADDITIONAL COSTS

In addition to infected machines and lost data, there are lost sales, angry customers and bad PR.

Always be prepared, minimize downtime and never lose another file with SecuriSync. View tip sheet ›

INTERMEDIA
The Business Cloud™

Source: Intermedia Crypto-Ransomware Survey, 2016