

Ransomware: the true cost to business 2024



Global results of our annual study on the business impact of ransomware.

Ransomware attacks are becoming more frequent, more sophisticated, and more effective.

Attackers are evolving

More complex, low-and-slow attacks are designed to compromise as much of the targeted network as possible to exact the highest ransom in 'RansomOps' attacks.

56%

didn't detect a breach for 3-12 months.

How did they get in?

41%

got in via a supply chain partner.

24%

got in directly.

22%

got in with the help of an insider.

Paying the ransom isn't the best solution

Despite most victims agreeing to pay the ransom, less than half got their systems and data back uncorrupted. And most were breached again within a year.

84%

paid the ransom.

But only 47%

got their data and services back uncorrupted.

78%
were then breached again.

63%
of these were asked to pay more the second time.

Ransom fees are high

Ransom fees remain high, and they are just the tip of the iceberg regarding the true cost of an attack.

Average ransom payments over the last 24 months:

USA: \$1.4 million

UK: \$423k

France: \$1 million

Germany: \$762k

But the true cost is higher.

46%

estimate total business losses of \$1-10 million.

16%

estimate total business losses of over \$10 million.

It's difficult to get the right people and plans in place

Most organizations increased their investment in cybersecurity after a breach, but the risk remains.

Less than half say their businesses are adequately prepared for the next attack.

In fact, the chances are high that you will get hacked again.

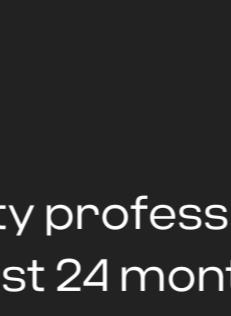
Yet only

41%

feel they have the right people and plan to manage the next attack.



increased spend.



Reject the ransom



Paying millions of dollars to ransomware attackers is not always the solution.

It doesn't guarantee:

- You will get all your systems and data back uncorrupted
- Your data won't be sold on the black market
- You won't be attacked again

In fact, the chances are high that you will get hacked again.

Make your business invincible with AI-powered protection

Cybereason is undefeated by today's attackers and ready for tomorrow's.

Our powerful combination of solutions and services deliver:

- Round-the-clock security
- Optimized security operations
- The fastest detection, triage and time to remediation on the market



cybereason®

Read the full global survey

Learn from over 1,000 enterprise cybersecurity professionals who have been breached by ransomware at least once in the last 24 months.

The results will surprise you.

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in La Jolla, California with customers in more than 40 countries.