

Businesses face unique challenges every day. One of them is downtime.

62% of businesses suffer from unplanned downtime every month.1

Is your organization prepared to tackle downtime challenges?





Human error

Human error is a major cause of downtime, according to 60% of IT and security professionals.²

A study conducted by Stanford University researchers and a leading cybersecurity firm revealed that around 88% of data breaches stem from employee mistakes.3



Hardware/ software failure

In 2022, outdated hardware caused server downtime for 24% of organizations.4

One in five organizations experienced a "serious" or "severe" data center outage, resulting in significant financial losses and compliance breaches, in the past three years.⁵



Cyberattacks

More than 72% of organizations worldwide have suffered a cyberattack in 2023.6

The average data breach cost reached \$4.45 million in 2023, indicating a 15% increase over the last three years.⁷



Natural disasters

In the first nine months of 2023, the United States witnessed 24 natural disasters causing damages exceeding \$1 billion.8

25% of businesses fail to reopen following a disaster.8

DATA LOSS AND DOWNTIME HAVE BECOME AN EXISTENTIAL THREAT TO BUSINESS. HERE'S WHY.



downtime costs businesses \$500,000.10

A mere one-hour



outages endured for more than 12 hours, with 16% extending beyond 48 hours.¹¹



processes to recover

their data, making data retrieval complicated and time-consuming.14



tested and updated disaster recovery plan.15

have a well-documented,

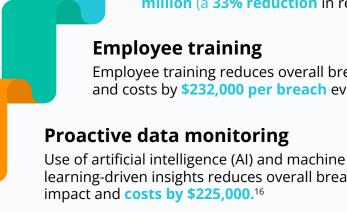




data loss incident within **12 hours** or less.¹³

recover from a severe

Disaster recovery testing Organizations with mature levels of incident response (IR) planning and testing reduce the

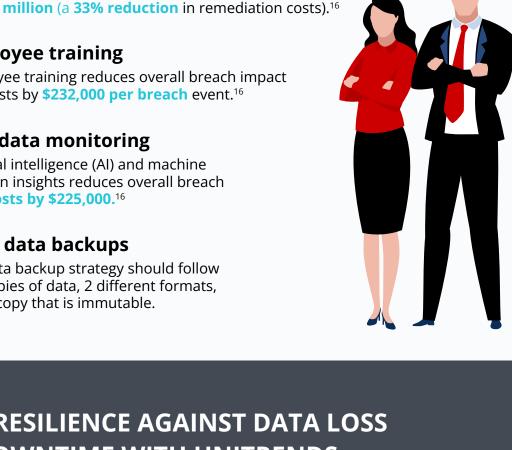


Employee training Employee training reduces overall breach impact and costs by \$232,000 per breach event.16

overall cost of remediating a breach by \$1.49

learning-driven insights reduces overall breach impact and costs by \$225,000.16

Comprehensive data backups At minimum, your data backup strategy should follow the 3-2-1-1 rule; 3 copies of data, 2 different formats,



1 copy off-site and 1 copy that is immutable.

MAXIMIZE RESILIENCE AGAINST DATA LOSS AND DOWNTIME WITH UNITRENDS The threat of data loss and downtime is ever-present across all industries. Resilience is the key to minimizing the negative impacts of downtime and ensuring rapid recovery

cloud, SaaS applications or employee endpoints. Our solutions leverage cutting-edge technologies, like AI and predictive analytics, to help your business stay operational under any circumstance while significantly reducing time, effort and costs. 12 logicmonitor.com

during a crisis. Unitrends backup and recovery solutions are built to defend data against ransomware, data loss and downtime — no matter where the data lives — on-premises,

5 uptimeinstitute.com 7 ibm.com

4 lenovo.com

Sources:

2 zipdo.co

3 blog.knowbe4.com

а **Kaseya** сомрану

13 continuitycentral.com

15 continuitycentral.com

"The assurance that we have with Unitrends is that no matter what the situation, we feel that we will always be able to get to our data."

Don't let data loss and downtime steal your thunder.

Jay Waller

Information Technology Manager Town of Mount Pleasant

Fortify your business against the unexpected with Unitrends.

BOOK A CALL WITH US NOW!

