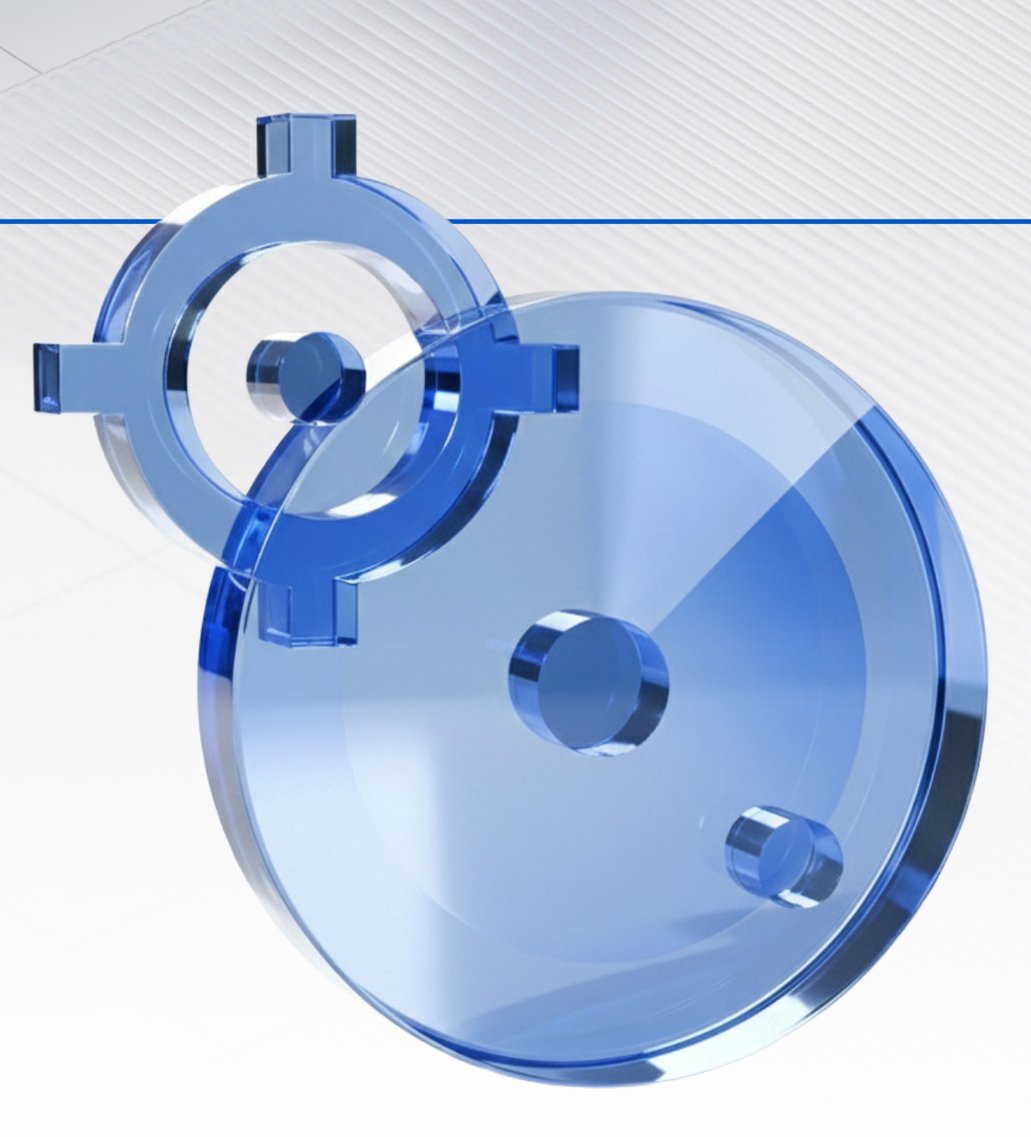
Acronis

Beyond cybersecurity: Building cyber resilience for business continuity

Why modern IT leaders must plan for disruption, not just prevention.

Cybersecurity vs. cyber resilience



Cybersecurity focuses on stopping attacks. Cyber resilience ensures the business continues operating during and after an attack.

Cybersecurity
prevention, perimeter defense, breach avoidance

Cyber resilience
adaptability, recovery, business continuity

Business continuity impact across industries

Why cyber resilience matters across critical industries

Downtime and cyber disruption affect every sector — but the consequences vary by industry.

Health care

60%

health care organizations report that cyber incidents directly disrupt patient care.[1]

Why it matters:
Downtime can delay treatment, divert patients and compromise safety.

Retail

43%

retailers experienced a major outage caused by IT or cyber incidents in the past year.[2]

Why it matters:
Even short disruptions affect revenue, inventory visibility and customer experience.

Financial services

91%

financial institutions experienced at least one cyber incident in the past year.[3]

Why it matters:
Downtime affects transaction processing, customer confidence and regulatory compliance.

Logistics and transportation[4]

94%

organizations say cyber disruptions can cause cascading supply chain failures.[5]

Why it matters:
Downtime halts shipment tracking, warehouse operations and just-in-time delivery.

Public administration / government

60%

network outages cost organizations at least $1 million in operational disruptions.[6]

Why it matters:
Outages affect citizen services, emergency response and public trust.

Downtime is a business continuity failure

Downtime affects revenue, operations and reputation — not just IT systems.

96%

of organizations experienced at least one outage in the past three years.

80%

say outages are becoming more severe.[7]

Why traditional redundancy fails against ransomware

Redundancy protects against hardware failure — not intelligent, propagating attacks.

Replication can spread infection

Fragmented DR and backup tools create blind spots

Tool sprawl increases recovery time and operational drag

Modern resilience requires new recovery metrics

Speed alone is not enough — recovery must be clean and business-aligned.

RTO
Maximum time to restore operations

RPO
Maximum acceptable data loss

MTD
Maximum tolerable downtime before business failure

MTCR
Time to restore a verified, malware-free environment

Clean recovery is now a continuity requirement

Recovering quickly is meaningless if restored systems are compromised.

- Average cost of a data breach: $4.45 million.
- Operational disruption is the largest cost component of breaches.[8]

What business IT leaders should prioritize

Resilience is an economic and operational decision.

Priority actions (high-level)

Align protection with asset criticality.

Test recovery under real cyber scenarios.

Validate backups before restoration.

Reduce complexity through unified platforms.

Cyber resilience enables continuity, confidence and control — even when attacks are inevitable

From cybersecurity to cyber resilience with Acronis

Cybersecurity depends on more than protection. It requires resilience. See how Acronis can help you anticipate threats, withstand attacks, recover faster and adapt for the future

Contact us

[1] U.S. Department of Health and Human Services (HHS)
https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute. "Annual Outage Analysis 2023."
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] World Economic Forum. "Global Cybersecurity Outlook 2024."
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] World Economic Forum – Global Risks Report
https://www.weforum.org/reports/global-risks-report-2024

[5] Ibid

[6] Intelligent CIO. "US government organizations lose millions in an average network outage or breach."
https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute. "Annual Outage Analysis 2023."
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM. "Cost of a Data Breach Report 2025."
https://www.ibm.com/reports/data-breach

Acronis