

5 steps to building cyber resilience in health care



The health care sector is a lucrative target of widespread cyberattacks, and the costs to recuperate are increasing to the tune of tens of billions of dollars every year. Why are recovery expenses going up? Today's health care ecosystems are largely interconnected, which only amplifies the impact and damage of attacks. Attackers require less time and resources to do more damage.

From the boardroom to operating table: Downtime affects everyone in health care

92%

of health care organizations reported at least one attack in 2024.¹

300%

more ransomware attacks have hit the health care sector since 2015.²

41%

of CISOs name ransomware as one of the top three threats.³

56%

of health care organizations report poor patient outcomes because of attacks.⁴

53%

of health care organizations saw increased medical complications due to an attack.⁵

28%

of health care organizations faced with cyberattacks report increased mortality rates.⁶

Five steps to building health care cyber resilience: Defense and recovery



Prioritize robust cybersecurity

Invest in advanced threat detection, prevention and response. Regularly update software and patch vulnerabilities promptly.



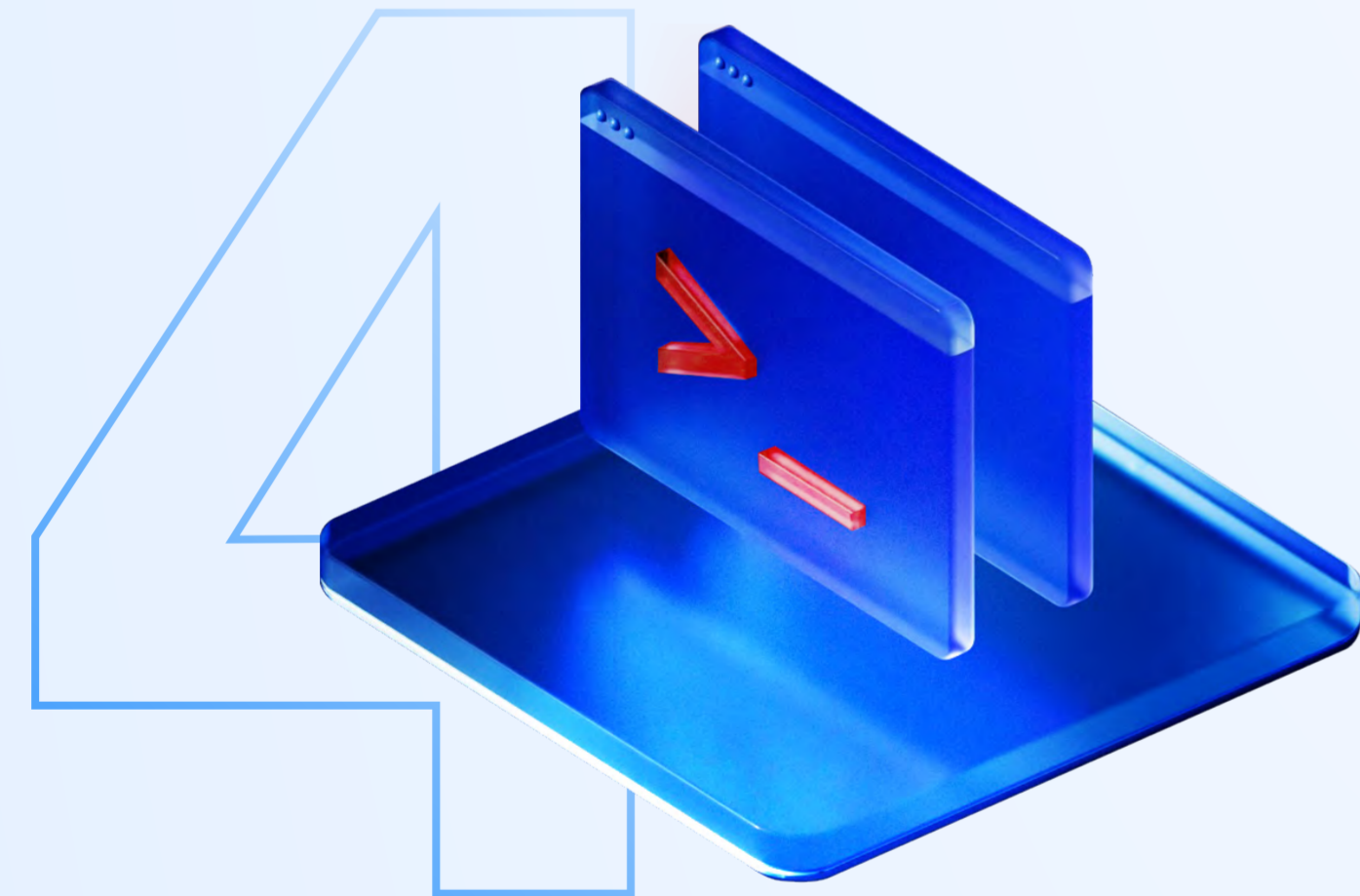
Implement strong segmentation

Limit the lateral movement of attackers within your network. Isolate critical systems to prevent widespread disruption.



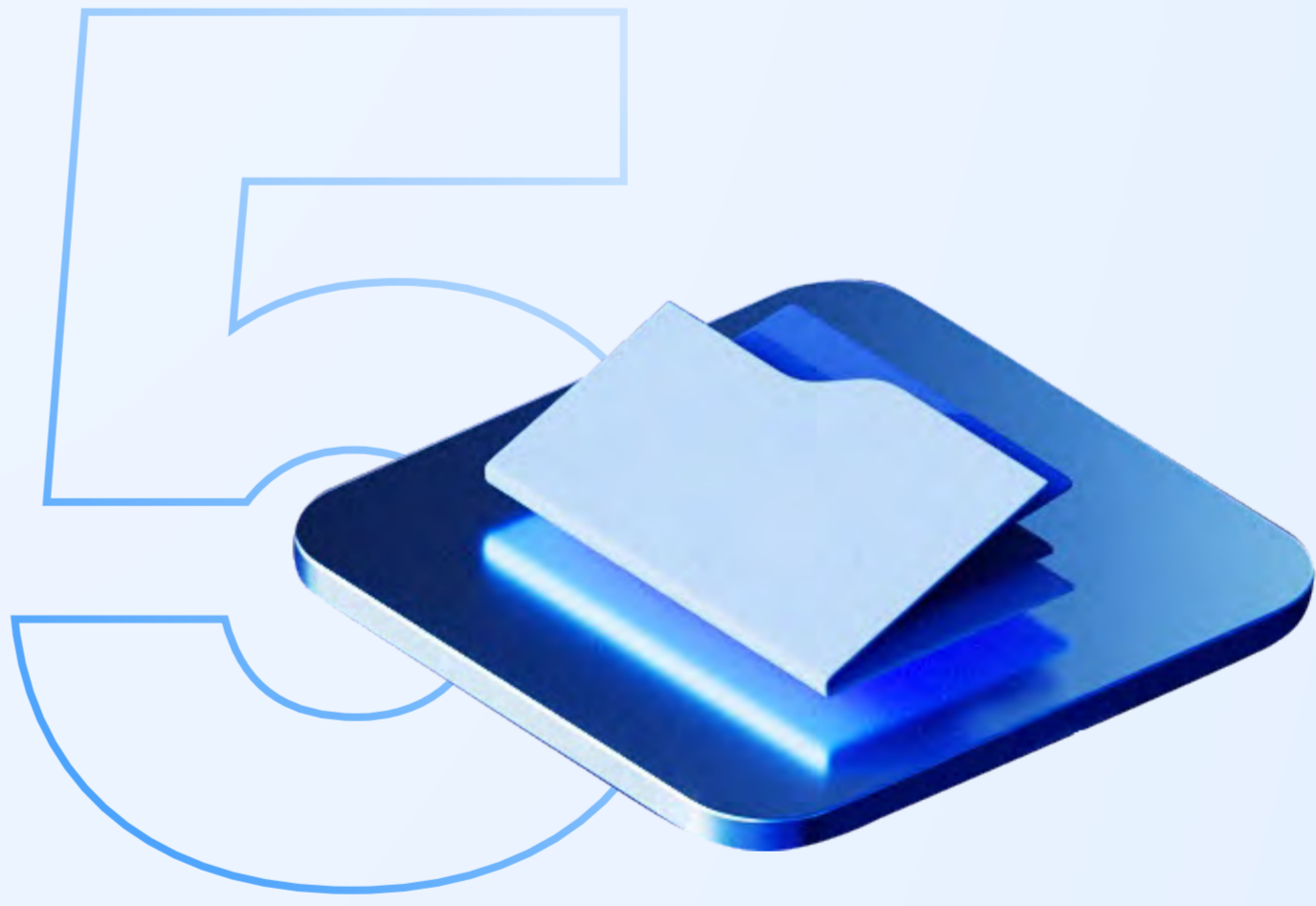
Develop business continuity and disaster recovery plans

Have well-tested plans in place to ensure business operations can continue or be quickly restored after an attack.



Strengthen third-party risk management

Thoroughly vet and continuously monitor the security practices of all vendors and partners, especially those with significant system access.



Enhance incident response capabilities

Establish clear protocols for identifying, containing and recovering from cyber incidents. Conduct regular simulations and training.

Learn more about Acronis Cyber Protect for health care

➤ [Explore more](#)



¹The HIPAA Journal. "92% of U.S. Healthcare Organizations Experienced a Cyberattack in the Past Year." Posted October 9, 2024. <https://www.hipaajournal.com/92pc-us-healthcare-organizations-cyberattack-past-year/>

²IBM. "When ransomware kills: Attacks on healthcare facilities." Posted January 30, 2025. <https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities>

³Statista. "Most significant cybersecurity threats in organizations worldwide according to Chief Information Security Officers (CISOs) as of February 2024." Published March 10, 2025. <https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/>

⁴Healthcare Dive. "Nearly 70% of healthcare organizations hit by cyberattacks report patient care disruptions: survey." Published October 8, 2024. <https://www.healthcaredive.com/news/healthcare-cyberattacks-patient-care-disruption-ponemon-proofpoint-survey/729251/>

⁵Ibid.

⁶Ibid.