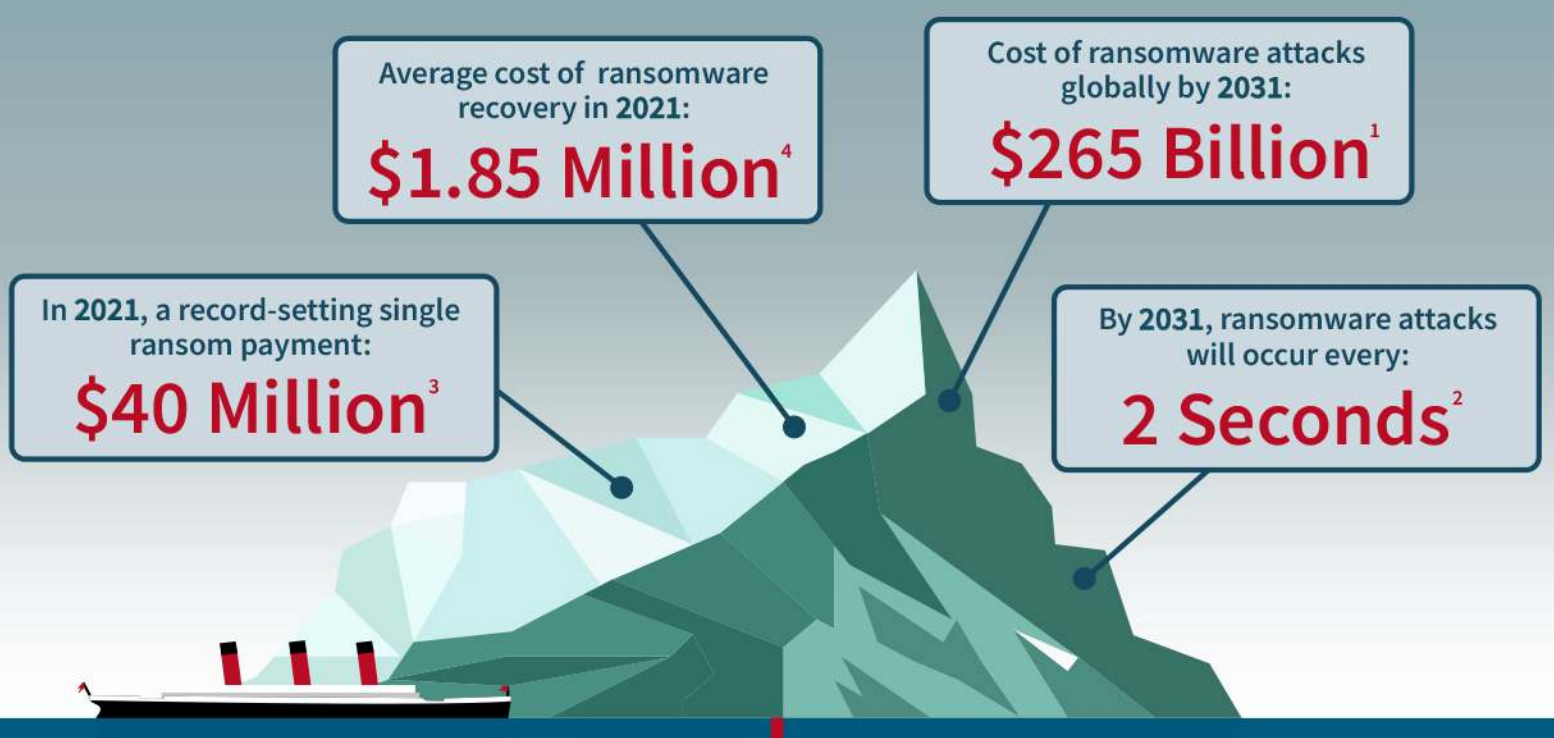
Ransomware Readiness

Zerto
a Hewlett Packard Enterprise company

It's not a matter of if — but when.

Ransomware attacks are increasing in frequency and cost to organizations they hit. Enterprises not prepared for such attacks are making the news—not just for paying millions of dollars in ransoms, but for the disruptions to their business and services. There is no industry, public or private, that is safe from ransomware attacks, and these attacks will only continue to escalate.



Ransoms are just the tip of the iceberg in terms of costs. Organizations will likely experience revenue loss, productivity loss, and brand reputation loss—not to mention recovery costs that oftenінvolve expensive third-party consultants to help restore systems and data.

The less prepared an organization is, the greater the impact of a ransomware attack. Cyber insurance can help recover some of the costs, but nothing can recover the loss of brand reputation from an extended disruption.

21 days was the average disruption period of an attack[5]

66% of victims suffered significant revenue loss[6]

42% of cyber insurance claims did not cover all costs[7]

25% of victims suffered a period of business closure[8]

Ransomware Readiness Checklist

Determine whether your organization is ransomware-ready with this quick checklist.

✓ Ransomware Prevention

- ☐ **Active antivirus solution**—Have an up-to-date antivirus scanning solution to detect incoming infected files
- ☐ **Active firewall protection**—Have active firewalls in place restricting port access on your network
- ☐ **Multi-factor authentication (MFA)**—Use MFA where possible to restrict unauthorized access attempts
- ☐ **Latest OS security updates**—Eliminate known vulnerabilities in the OS by applying available patches
- ☐ **Latest application security updates**—Keep applications updated to eliminate known vulnerabilities
- ☐ **Regular security training for users**—Make sure users are trained on how to avoid phishing and other malware attacks and how to keep their personal devices secure
- ☐ **Regular security training for IT staff**—Make sure IT staff are trained and up-to-date on security best practices and technologies

✓ Disaster Recovery Solution

- ☐ **RPO of seconds**—Have the ability to recover data to seconds before the attack happened
- ☐ **RTO of minutes**—Have the ability to bring systems back online within minutes of the attack
- ☐ **Individual file recovery**—Have the ability to recover individual files that were encrypted
- ☐ **Application consistent failover and recovery**—Have the ability to recover entire applications that may span multiple servers with consistent data
- ☐ **Full site failover and recovery**—Have the orchestration and automation to recover an entire site of data and servers
- ☐ **Immutable data copies**—Have the option to make some data copies immutable to encryption
- ☐ **Non-disruptive DR testing**—Have the ability to test frequently without affecting production servers

✓ Ransomware Response and Recovery Plan

- ☐ **Ransomware incident response team**—Identify and document the IT staff responsible for responding to an attack
- ☐ **Network isolation plan**—Have a plan to isolate infected servers, data, and users from the network
- ☐ **Malware detection**—Have a plan for finding and identifying the malware causing the attack
- ☐ **Recovery testing**—Have the ability to test the recovery in isolation before recovering to production
- ☐ **Fully documented disaster recovery runbook(s)**—Make sure all procedures and plans are documented for DR testing, training, and for a DR response

Get Zerto Free Edition **Watch the Demo**

[1,2] David Braue, "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031." Cybercrime Magazine. Jun. 3, 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
[3] Brittany Chang, "One of the Biggest US Insurance Companies Reportedly Paid Hackers $40 Million Ransom After a Cyberattack." Business Insider. May 22, 2021. https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5
[4] Sophos, "State of Ransomware 2021." https://sophos-state-of-ransomware-2021-wp.pdf
[5] "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands." Coveware Quarterly Ransomware Report. Feb. 1, 2021. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
[6,7,8] "Ransomware: The True Cost to Business. A Global Study on Ransomware Business Impact." eBook. Cybereason. 2021. Page 4. https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf