

2026 Ransomware Readiness Checklist

A companion self-assessment to CyberClan's "What 20,000+ Breaches Taught Us" — benchmark your organization against this year's ransomware and human-element data before an attacker tests it for you.

48%

of breaches involved ransomware (2026 DBIR)

62%

of breaches involved the human element

88%

of small-org breaches involved ransomware

43

median days to fully remediate a known vulnerability

How to use this checklist: work through each section with your IT lead, security owner, or MSSP. Check every box that's **currently true** for your organization — not planned, not "in progress," true today. Total your checks and see the scoring guide on the back page.

1. Assume Data Theft, Not Just Encryption

87.6% of ransomware claims now involve both encryption and data exfiltration (Travelers, 2024)

- ☐ Our incident response plan explicitly assumes attacker data exfiltration, not just encryption, on day one of any ransomware incident.
- ☐ Our breach-communications plan addresses a double-extortion scenario, including the possibility of stolen data being published.
- ☐ We maintain a data classification / data-mapping record so we know what's actually exposed if attackers claim to have taken data.
- ☐ Our cyber insurance policy has been reviewed in the last 12 months for extortion and data-breach notification triggers — not just ransom payment coverage.

2. Human-Element Controls

The human element was involved in 62% of breaches in the 2026 DBIR — up from 60% the year prior

- ☐ Simulated phishing testing runs at least quarterly, with results tracked over time — not once a year for compliance.
- ☐ MFA is enforced on every account with access to sensitive systems or data, not just email and VPN.
- ☐ Phishing-resistant MFA (FIDO2 security keys, passkeys, Windows Hello for Business) is prioritized for admin and privileged accounts.
- ☐ User access follows least-privilege and has been reviewed within the last 6 months.
- ☐ A written policy governs employee use of AI tools, and staff have been told what it says.
- ☐ Our helpdesk has a documented identity-verification protocol for any MFA or password reset request.

3. Vendor & Patch Management

48% of breaches involved a third party; only 26% of known-exploited vulnerabilities were fully remediated in 2025

- ☐ We maintain a current inventory of every third-party vendor with access to our systems or data.
- ☐ Vendor risk assessments have been completed or refreshed within the last 12 months.
- ☐ We have a patch management SLA for critical/known-exploited vulnerabilities, targeted well under the 43-day industry median.
- ☐ CISA's Known Exploited Vulnerabilities (KEV) catalog is actively monitored against our environment.
- ☐ Remote access paths (VPN, RDP, vendor remote-access tools) are restricted, monitored, and reviewed for third-party connections.

4. Incident Response Readiness

A tested plan is what turns a bad day into a contained one — not the document itself

- ☐ A written incident response plan exists and has been reviewed or updated in the last 12 months.
- ☐ The plan has been tested through a tabletop exercise, with leadership present, in the last 6 months.
- ☐ A 24/7 incident response contact — internal team or external retainer — is identified, with response-time commitments in writing.
- ☐ Backups are tested for successful restoration — not just completion — at least every 90 days.
- ☐ Breach notification requirements are documented for every jurisdiction in which we operate or hold customer data.
- ☐ Legal counsel and our cyber insurer are pre-briefed and have current contact information on file.

Score Your Readiness

- 18 - 22** Strong readiness posture. Maintain your cadence and reassess quarterly — threat data shifts fast.
- 10 - 17** Moderate gaps. Prioritize the Incident Response Readiness and Human-Element sections first — they close the widest exposure fastest.
- Under 10** Significant exposure. This is the profile CyberClan's IR team sees most often on breach calls. Schedule a Cyber Resilience Assessment now, not after an incident.

Turn This Checklist Into a Tested Plan

CyberClan's incident response team helps organizations close these gaps before an attacker finds them — through tabletop exercises, IR retainers, and readiness assessments built from what we see in live engagements.

Schedule a complimentary Cyber Resilience Consultation

24/7 EMERGENCY INCIDENT RESPONSE HOTLINE:

US/CA: 1 800 762 3290

UK: 0800 368 8731

AU: 61 1800 413 128

Sources: Verizon 2026 Data Breach Investigations Report; Travelers Insurance (2024); IBM Cost of a Data Breach 2025; CrowdStrike/StrongDM (2025). See the companion blog post, "What 20,000+ Breaches Taught Us," for full citations and context. This checklist is an educational self-assessment tool, not legal, compliance, or insurance advice — consult qualified counsel and your insurer for guidance specific to your organization.



Incident Hotline
US/CA 1 800 762 3290
UK 0800 368 8731
AU 61 1800 413 128
response@cyberclan.com

General Inquiries
US/CA 1 855 685 5785
UK 0800 048 7360
info@cyberclan.com