Ransomware Protection Checklist

A vendor-neutral assessment tool for executives, risk leaders and technology leadership to test whether the organization's ransomware strategy is designed to prevent, contain and recover from a serious attack.

How to use it	For each statement, mark Yes, Partial, No or N/A. A "Yes" should mean the organization can produce **current evidence** - not simply that a policy exists.
What matters most	Treat any "No" relating to privileged access, isolation, backup recoverability, recovery testing, incident authority or executive crisis procedures as a priority risk requiring an owner and target date.
What this is not	This is not a product selection guide or a substitute for a detailed technical assessment. It is designed to help leadership identify where evidence, ownership or resilience may be weak.

Executive scorecard

Domain	Yes	Partial	No	N/A	Priority / owner
Governance, accountability and business impact					
Identity and privileged access					
Attack surface and lateral movement reduction					
Detection, logging and containment					
Backup, restoration and recovery					
Incident response, crisis management and communications					
Third parties, suppliers and concentration risk					

Suggested interpretation: The score is less important than the pattern. A strategy with strong prevention but weak recovery, or good technology controls but unclear executive decision-making, can still fail badly during a ransomware event.

1. Governance, accountability and business impact

Checklist item	Yes	Part.	No	N/A
1.1 A named executive is accountable for ransomware resilience across prevention, response and recovery.	☐	☐	☐	☐
1.2 Ransomware risk is included in enterprise risk reporting and is reviewed by the board or an appropriate board committee.	☐	☐	☐	☐
1.3 The organization has identified the business services whose disruption would create material operational, financial, safety or regulatory impact.	☐	☐	☐	☐
1.4 Maximum tolerable downtime and recovery objectives are defined for critical business services and the technology that supports them.	☐	☐	☐	☐
1.5 Decision authority during a ransomware event is documented, including who may isolate systems, suspend services, invoke crisis management and communicate externally.	☐	☐	☐	☐
1.6 Cyber insurance coverage, exclusions, notification obligations and insurer/breach-counsel contact procedures are understood before an incident occurs.	☐	☐	☐	☐

2. Identity and privileged access

Checklist item	Yes	Part.	No	N/A
2.1 Multi-factor authentication is required (by policy) for privileged access, remote access, cloud administration and other high-risk access paths.	☐	☐	☐	☐
2.2 Privileged accounts are separate from normal user accounts and are restricted to the minimum rights needed.	☐	☐	☐	☐
2.3 Dormant, unnecessary and orphaned accounts are identified and removed on a defined schedule.	☐	☐	☐	☐
2.4 Service accounts and machine identities are inventoried, governed and protected from unmanaged credential reuse.	☐	☐	☐	☐
2.5 Administrative access to critical systems is limited to controlled management paths.	☐	☐	☐	☐
2.6 Identity logs are retained and monitored so suspicious sign-ins, privilege escalation and unusual administrative activity can be investigated.	☐	☐	☐	☐

3. Attack surface and lateral movement reduction

Checklist item	Yes	Part.	No	N/A
3.1 Internet-facing systems and services are inventoried, owned and reviewed for unnecessary exposure.	☐	☐	☐	☐
3.2 Security patches for operating systems, applications, network devices and security appliances are reviewed and prioritized by exploitability and business risk, and patches are applied in a defined timeframe.	☐	☐	☐	☐
3.3 Unsupported or end-of-life systems have been removed, upgraded, isolated or placed under formally accepted compensating controls.	☐	☐	☐	☐
3.4 Remote administration and remote monitoring tools are inventoried, approved and monitored for unauthorized use.	☐	☐	☐	☐
3.5 Network segmentation limits lateral movement between users, servers, management systems, backups, critical applications and operational technology where applicable.	☐	☐	☐	☐
3.6 Email, web and endpoint controls reduce common ransomware entry paths such as malicious attachments, links, scripts, executable content and credential theft.	☐	☐	☐	☐
3.7 The organization maintains current network and data-flow documentation sufficient to support rapid containment during an incident.	☐	☐	☐	☐

4. Detection, logging and containment

Checklist item	Yes	Part.	No	N/A
4.1 Security monitoring can detect suspicious endpoint behavior, credential abuse, privilege escalation, mass file changes and unusual network activity.	☐	☐	☐	☐
4.2 Logs from critical identity, endpoint, server, network, cloud and security systems are centralized and retained for investigation.	☐	☐	☐	☐
4.3 High-confidence ransomware indicators can trigger rapid containment actions without waiting for lengthy manual approval.	☐	☐	☐	☐
4.4 The organization can isolate a compromised endpoint, server, subnet, account or cloud workload quickly and knows who is authorised to do so.	☐	☐	☐	☐
4.5 Detection coverage is periodically tested against realistic ransomware techniques rather than assumed to be effective.	☐	☐	☐	☐
4.6 Monitoring includes signs of data staging or exfiltration, recognizing that ransomware incidents may involve extortion as well as encryption.	☐	☐	☐	☐

5. Backup, restoration and recovery

Checklist item	Yes	Part.	No	N/A
5.1 Recovery requirements are documented. Critical data and system configurations are backed up according to documented recovery requirements.	☐	☐	☐	☐
5.2 At least one offsite recoverable copy of critical backup data is isolated from normal production credentials and cannot be altered by a compromised production administrator. For Cloud-resident data, offsite isolated data must be in a separate geographic region with separate credentials.	☐	☐	☐	☐
5.3 Backup administration is separated from routine production administration and protected with strong authentication.	☐	☐	☐	☐
5.4 Backup completeness and integrity are monitored; failed or incomplete backups are investigated rather than simply recorded.	☐	☐	☐	☐
5.5 Restoration of critical applications and data is tested on a defined schedule using realistic recovery scenarios.	☐	☐	☐	☐
5.6 Recovery tests demonstrate that required recovery time and recovery point objectives to a defined scale can actually be achieved.	☐	☐	☐	☐
5.7 The organization has defined the minimum clean infrastructure, identity services, network services and administrative capability required to begin recovery.	☐	☐	☐	☐
5.8 The organization has defined the timeframe and resources required to bring operations back to full production scale.	☐	☐	☐	☐
5.9 Recovery procedures address rebuilding to production-level scale from trusted sources rather than restoring compromised systems indiscriminately.	☐	☐	☐	☐

6. Incident response, crisis management and communications

Checklist item	Yes	Part.	No	N/A
6.1 A ransomware-specific incident response playbook exists and is integrated with the broader cyber incident response plan.	☐	☐	☐	☐
6.2 The playbook addresses detection, isolation, evidence preservation, eradication, credential resets, restoration and validation before reconnecting systems.	☐	☐	☐	☐
6.3 Legal, regulatory, law-enforcement, insurance and contractual notification requirements are known and assigned to named roles.	☐	☐	☐	☐
6.4 Internal communications can continue if normal email, collaboration or identity platforms are unavailable.	☐	☐	☐	☐
6.5 External communications plans cover customers, employees, regulators, partners, media and other stakeholders as appropriate.	☐	☐	☐	☐
6.6 The organization has pre-agreed principles for handling ransom demands, including executive, legal, law-enforcement and sanctions considerations.	☐	☐	☐	☐
6.7 Ransomware tabletop exercises involve business leadership as well as IT and security teams.	☐	☐	☐	☐

7. Third parties, suppliers and concentration risk

Checklist item	Yes	Part.	No	N/A
7.1 Critical suppliers and service providers are identified according to the business services they support.	☐	☐	☐	☐
7.2 Contracts for critical providers include appropriate security, incident notification, cooperation and recovery obligations.	☐	☐	☐	☐
7.3 Third-party remote access is controlled, time-bounded where feasible and monitored.	☐	☐	☐	☐
7.4 The organization understands which critical business processes depend on a single technology provider, cloud platform, managed service or other concentration point.	☐	☐	☐	☐
7.5 Continuity plans address the failure or compromise of a critical third party, not only compromise of internal systems.	☐	☐	☐	☐

Executive challenge questions

A strong ransomware strategy should survive these questions without relying on assumptions or individual heroics.

1. If a privileged administrator account were compromised tonight, what prevents the attacker from reaching critical systems and backups?
2. How quickly can we isolate an affected user, server, network segment or cloud environment, and who has authority to do it?
3. When did we last restore a critical business service from backup, and did we meet the recovery objective?
4. Which business service would hurt us most if unavailable for five days, and have we exercised that exact scenario?
5. Could we still coordinate executives, legal, communications and incident responders if corporate email and identity services were unavailable?
6. What evidence tells us that our detection and containment controls work against current ransomware behaviors or Zero Day attacks?
7. Which third party could stop a critical business process if they were hit by ransomware, and what is our fallback?
8. If data were stolen before encryption, do our response and communications plans address extortion and disclosure risk as well as system recovery?

Priority actions identified

Priority gap	Executive owner	Target date	Status

About this checklist

This checklist is vendor-neutral and is intended as a practical management aid for organizations reviewing their ransomware resilience. It is designed to help leadership assess whether appropriate governance, preventive controls, detection capability, containment procedures, recovery arrangements and executive decision-making processes are in place and supported by evidence.

Organizations should adapt the checklist to their own business environment, technology estate, risk appetite and operating model. Particular attention should be given to the ability to maintain appropriate security logging, detect and isolate compromised systems quickly, protect privileged access, maintain recoverable and

appropriately isolated backups, test restoration procedures, conduct realistic incident exercises and sustain critical business operations during a significant cyber incident.

Ransomware response planning should also take account of applicable legal, regulatory, contractual and sector-specific obligations, including requirements relating to cybersecurity incident reporting, preservation of relevant records and logs, notification of affected parties, protection of personal data and cooperation with competent authorities where required.

The effectiveness of a ransomware strategy should be demonstrated through periodic testing and review rather than assumed from the existence of policies or technology controls. Recovery objectives, incident response procedures, escalation paths and communications arrangements should be validated against realistic scenarios and updated as threats, business dependencies and regulatory requirements change.

This checklist does not represent a complete cybersecurity assessment and should be used alongside appropriate technical, legal, regulatory and business continuity expertise.

Reference framework: NIST IR 8374 Rev. 1, Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile (June 2026); CISA, #StopRansomware Guide.

HARAREI
Secure. Connect. Transform.
hararei.com

Disclaimer

This checklist is provided by Hararei solely as a general informational and educational resource to assist organizations in reviewing their approach to ransomware resilience. It is not intended to constitute, and should not be relied upon as, legal, regulatory, compliance, insurance, cybersecurity, technical or other professional advice or as a comprehensive assessment of an organization's security posture.

Cybersecurity threats, technologies, business environments and regulatory requirements vary between organizations and change over time. The inclusion or omission of any control, practice or consideration in this checklist should not be interpreted as a representation that it is appropriate, sufficient or complete for any particular organization or circumstance.

Hararei makes no representation, warranty or guarantee, express or implied, as to the accuracy, completeness, suitability or continued applicability of the information contained in this checklist. In particular, Hararei does not warrant or guarantee that implementation of any measure described or contemplated by this checklist will prevent, detect, contain or mitigate ransomware, cyberattack, data loss, business interruption or any other cybersecurity incident.

Users remain solely responsible for assessing their own risks, systems, business requirements and legal and regulatory obligations and should obtain appropriate professional advice where required.

To the maximum extent permitted by applicable law, Hararei excludes liability for loss or damage arising from the use of or reliance upon this checklist. Nothing in this disclaimer is intended to exclude or restrict any liability that cannot lawfully be excluded or restricted under applicable law.

Use of or access to this checklist does not create a client, advisory, fiduciary, consulting or other professional relationship between Hararei and the user.

Contact Hararei at sales@hararei.com or visit our website at https://hararei.com