Ransomware Recovery Readiness Checklist (2026 Edition)

This checklist helps you verify whether your business can recover quickly, safely, and without negotiating with attackers.

Ransomware Recovery Readiness Checklist

1. Verified Backup System (Not Just “Set Up”)

- ☐ Backups run automatically on a scheduled basis
- ☐ Backup success is reviewed regularly (not assumed)
- ☐ Failed backups are flagged and corrected immediately

Why this matters:
Backups that aren’t verified are the #1 reason businesses pay ransomware demands.

2. Backup Isolation (Critical Modern Requirement)

- ☐ Backups are stored offsite or in a separate environment
- ☐ Backup systems are not directly accessible from user devices
- ☐ Backup credentials are separate from normal user logins

Why this matters:
Modern ransomware actively targets and deletes accessible backups.

3. Test Restore Capability (Proof of Recovery)

- ☐ Files have been successfully restored in the last 90 days
- ☐ Full system recovery has been tested (not just individual files)
- ☐ Recovery time is known and documented

Why this matters:
A backup is only valuable if it restores quickly under pressure.

4. Multi-Factor Authentication (MFA) Coverage

☐ MFA is enabled on email, admin accounts, and remote access
☐ MFA is enforced for all users—not optional
☐ Backup and admin systems also require MFA

Why this matters:
Most ransomware attacks begin with compromised credentials.

5. Endpoint Protection and Monitoring

☐ All devices have active antivirus/EDR protection
☐ Systems are monitored for unusual activity
☐ Alerts are reviewed and acted on quickly

Why this matters:
Early detection can stop ransomware before it spreads.

6. Patch and Update Management

☐ Operating systems are updated regularly
☐ Critical software is patched promptly
☐ Unsupported systems are identified and replaced

Why this matters:
Unpatched systems are a primary entry point for attackers.

7. Access Control and Least Privilege

☐ Users only have access to what they need
☐ Admin privileges are limited and controlled
☐ Shared drives are not fully open to all users

Why this matters:
Ransomware spreads faster in environments with excessive access.

8. Email and Phishing Protection

☐ Employees are trained to identify phishing attempts
☐ Suspicious emails are reported and reviewed
☐ Email filtering is in place and active

Why this matters:
Phishing remains the most common ransomware entry point.

9. Device Security and Remote Access Control

□ Remote access (RDP, VPN) is secured and monitored
□ Devices require login protection (PIN/biometric)
□ Lost or stolen devices can be remotely secured

Why this matters:
Unsecured remote access is a high-risk attack vector.

10. Incident Response Plan (Ransomware-Specific)

□ A response plan exists and is accessible offline
□ Key contacts are documented and reachable
□ Staff knows who to notify immediately

Why this matters:
Confusion during an attack increases downtime and damage.

11. Data Classification and Prioritization

□ Critical business data is identified and prioritized
□ Recovery order is clearly defined
□ Non-essential data is separated from critical systems

Why this matters:
Not all data needs to be restored first—prioritization speeds recovery.

12. Credential and Identity Protection (Emerging Risk Focus)

□ Password manager is used across the team
□ Weak or reused passwords are eliminated
□ Credential exposure is monitored regularly

Why this matters:
Attackers increasingly target identities before deploying ransomware.

What To Do If Ransomware Is Detected

Disconnect affected devices immediately
Do NOT power off systems unless instructed
Do NOT attempt to “fix” files manually

Notify IT support immediately
Preserve evidence for investigation

Recovery Reality Check

If you answered “No” or “Not Sure” to any of these:

- **Your recovery time will increase**
- **Your risk of paying a ransom increases**
- **Your business disruption will be longer than expected**

Quick Rule of Thumb

Backups don’t protect your business.
Tested, isolated, and recoverable backups do.

SofTouchSystems.com
No-Surprise IT — Predictable. Proactive. Proven.