Cyber Insurance Readiness Checklist for Small Businesses

Cyber insurance applications now ask more direct questions about MFA, backups, endpoint protection, email security, vendor access, incident response and user training.

Use this checklist before a renewal, application or security review so common gaps are not discovered at the last minute.

BEST FOR	USE IT TO	NEXT STEP
Owners, operations leaders, office managers and internal IT teams preparing for renewal or a security review.	Review practical controls that are commonly requested by cyber insurance carriers.	Turn the findings into a prioritized security and documentation plan.

Identity and Access Controls

Start with access because account compromise is one of the most common business risks.

Multi-Factor Authentication

- MFA is enabled for Microsoft 365 and remote access.
- Administrators use MFA on every privileged account.
- Shared accounts are removed or tightly controlled.
- Legacy authentication is disabled where possible.

User Access Review

- Former employees and vendors are removed promptly.
- Admin permissions are limited to people who need them.
- Shared mailboxes, distribution lists and file permissions are reviewed.
- New user and offboarding steps are documented.

Backup and Recovery Readiness

Carriers often want to know whether the business can recover from ransomware, accidental deletion or system failure.

Backup Coverage

- Critical servers, cloud data and business applications are included.
- Microsoft 365 data protection is reviewed instead of assumed.
- Backup alerts are monitored by someone responsible.
- Retention expectations are documented.

Recovery Testing

- Restore tests are performed on a schedule.
- Recovery time expectations are understood by leadership.
- Backup credentials are protected.
- Offline, immutable or separated backup options are considered where appropriate.

Endpoint, Email and User Protection

Endpoint Protection

Business computers and laptops have managed endpoint protection, alerting and a response owner.

Email Security

Email filtering, phishing protection and suspicious link controls are reviewed for Microsoft 365.

Security Awareness

Employees receive practical training on phishing, password safety, fake invoices and suspicious requests.

Patch Management

Operating systems, browsers, business applications and security tools are updated consistently.

Remote Access

Remote tools use MFA, logging and limited permissions. Old access paths are removed.

Vendor Access

Third-party access is reviewed, documented and removed when no longer needed.

Documentation and Response Planning

The best answer to an insurance question is evidence.

Minimum Documentation to Gather

- Inventory of key systems, users, vendors and security tools.
- Backup and recovery process notes.
- Incident response contact list and escalation path.
- Cybersecurity policy or acceptable use guidance.
- Evidence of MFA, endpoint protection, email security and training.

NEXT STEP

Need help preparing for cyber insurance questions? Nevada IT Support can review Microsoft 365, backups, endpoint protection, email security and cybersecurity documentation before gaps become renewal problems.

Schedule a Technology Review at itsupportnv.com/technology-gap-review/