Cybersecurity Checklist

Cyber insurance providers typically require firms to confirm that specific security controls are in place. While terminology may vary by carrier, the requirements below appear on the majority of applications.
This checklist outlines those requirements and how Nimbl's IT services support them today.

For more information, head over to our website for **full explanations** regarding what each of these items mean.

01 Endpoint Detection & Response (EDR / MDR)

What insurers expect:

- Advanced endpoint security with continuous monitoring to detect and stop malware, ransomware, and intrusions on all devices.
- With Nimbl, managed EDR/MDR is included on all supported client devices as a default, using Malwarebytes for Windows PCs and Jamf Protect for Macs.

02 Multi-Factor Authentication (MFA)

What insurers expect:

- MFA enabled for email, remote access, and administrative accounts. Nimbl enforces MFA on its own administrative and technician access.
- Client user MFA must be implemented by the firm within its systems, with guidance available from Nimbl Tech.

03 Vulnerability Management & Patch Management

What insurers expect:

- Regular application of operating system and software updates to reduce exposure to known vulnerabilities.
- For all Nimbl clients, operating system and software patches are automatically applied weekly to managed devices. Network-level vulnerability scanning is available as an add-on service.

04 Secure Data Backups (Off-site or Air-gapped)

What insurers expect:

- Recent backups that are isolated from the primary network and recoverable after a ransomware event.
- As an add-on, Nimbl can design and manage secure off-site or cloud-based backup solutions tailored to the firm's systems.

05 Security Awareness Training

What insurers expect:

- Ongoing employee training, including phishing simulations and security education.
- Security awareness training is included for all Nimbl clients, with quarterly micro-trainings and monthly phishing simulation exercises.

06 Written Security Policy & Incident Response Plan

What insurers expect:

- Documented security policies and a defined plan for responding to cyber incidents.
- Available as a separate engagement, Nimbl maintains these internally and can assist clients with creating a Written Information Security Plan (WISP) and incident response plan.

nimbl TECH