

## Cyber Insurance Prep Checklist

Prepare your organization for cyber insurance applications and renewals with this ~~comprehensive~~ checklist.

## 1. Security Fundamentals

These are baseline security controls that nearly all cyber insurers require. Ensure these are in place and documented before applying.

- Multi-factor authentication (MFA) enabled for all remote access
- MFA enabled for email access (especially Microsoft 365/Google Workspace)
- MFA enabled for privileged/administrative accounts
- Endpoint Detection and Response (EDR) deployed on all endpoints
- Email filtering and anti-phishing controls in place
- Regular automated backups with offline/immutable copies
- Backup restoration tested within the last 6 months

## 2. Access Control & Identity

- Privileged Access Management (PAM) solution implemented
- Principle of least privilege enforced for all accounts
- Regular access reviews conducted (at least quarterly)
- Terminated employee access revoked within 24 hours
- Service account inventory maintained and reviewed
- Password policy meets industry standards (length, complexity, rotation)
- Single Sign-On (SSO) implemented where possible

### **3. Network Security**

- Network segmentation implemented between critical systems
- Firewall rules reviewed and documented within last year
- Remote Desktop Protocol (RDP) not exposed to internet
- VPN with MFA required for all remote access
- Intrusion detection/prevention systems deployed
- DNS filtering implemented to block malicious domains
- Wireless networks secured and segmented from production

### **4. Vulnerability Management**

- Regular vulnerability scanning performed (at least monthly)
- Critical vulnerabilities patched within 14 days
- High vulnerabilities patched within 30 days
- Patch management process documented and followed
- End-of-life systems inventoried with remediation plans
- Third-party/vendor software included in patching program

### **5. Incident Response & Business Continuity**

- Documented incident response plan exists
- Incident response plan tested within last 12 months
- 24/7 incident response contact identified
- Relationship with incident response retainer/vendor established

- Business continuity plan documented and tested
- Disaster recovery capabilities tested within last 12 months
- Cyber insurance policy details accessible during an incident

## **6. Security Awareness & Training**

- Annual security awareness training for all employees
- Phishing simulation exercises conducted regularly
- Role-based security training for IT/security staff
- Security policies acknowledged by all employees annually
- New hire security training included in onboarding

## **7. Documentation & Governance**

Insurers often request documentation to verify security controls. Ensure the following are current and accessible.

- Information security policy documented and approved
- Data classification policy in place
- Acceptable use policy signed by all employees
- Third-party risk management program documented
- Privacy policy aligned with applicable regulations
- Board/executive security reporting established
- Security metrics and KPIs tracked and reported

## 8. Application Information

Gather this information before starting your insurance application.

**Annual Revenue**

**Number of Employees**

**Industry/Sector**

**Number of Records/Customers**

**Geographic Locations**

**Previous Cyber Incidents (last 3 years)**

**Current/Desired Coverage Amount**