Cybersecurity Protection Checklist

If you are missing any of the steps below, you can do research into what cybersecurity companies can provide you with these solutions and/or check with your current company on providing you the services you're lacking.

1. Security Governance

Yes No

- ☐ ☐ Do we have a written Incident Response Plan?
- ☐ ☐ Do we have a Disaster Recovery Plan?
- ☐ ☐ Are regular security awareness training courses conducted for all staff, including training in social engineering, data privacy, compliance, and cybersecurity?
- ☐ ☐ Are simulated phishing tests routinely performed and tracked?
- ☐ ☐ Are cybersecurity policies in place and reviewed and updated annually?
- ☐ ☐ Do we know our critical third parties and do we understand their security posture?

2. Identity & Access Security

Yes No

- ☐ ☐ Is each authorized user of our systems and data using a unique account that attributes activities to them?
- ☐ ☐ Are strong password controls in place that meet current security best practices?
- ☐ ☐ Is multi-factor authentication (MFA) enforced for all accounts?
- ☐ ☐ Are administrative accounts monitored and limited to what is required?
- ☐ ☐ Are permissions and group memberships reviewed routinely and frequently to ensure the right users have the right access?
- ☐ ☐ Are user accounts audited for dormant or unnecessary access?
- ☐ ☐ Have we removed local and domain administrative rights from all regular user accounts?
- ☐ ☐ Are conditional access policies in place to prevent or detect suspicious login attempts?

3. Network Security

Yes No

- ☐ ☐ Are firewalls business-grade, actively monitored, and securely configured?
- ☐ ☐ Do we segment or segregate critical systems from general systems?
- ☐ ☐ Is virtual private network (VPN) access protected with MFA and only allowed for authorized users?
- ☐ ☐ Are we monitoring for unusual data transfers (large uploads, off-hours access, external sharing)?
- ☐ ☐ Is 24x7 security and log monitoring in place to detect incident indicators early?
- ☐ ☐ Are firewall and switch configurations regularly audited?
- ☐ ☐ Are vulnerability scans and penetration tests performed regularly?
- ☐ ☐ Do we block inappropriate and unneeded content on the internet?
- ☐ ☐ Is our network infrastructure hardened and patched regularly?

Cybersecurity Protection Checklist

4. Endpoint & Device Security

Yes	No	
☐	☐	Do we have a solid list/inventory of all devices allowed to access our systems and data?
☐	☐	Do we have next-generation endpoint protection on all devices, monitored 24x7?
☐	☐	Are endpoint devices encrypted?
☐	☐	Do we allow storing of critical business information on an endpoint device?
☐	☐	Do we have the ability to remotely wipe a device?
☐	☐	Are operating systems and third-party applications patched regularly (monthly at minimum)?
☐	☐	Are USB drives and removable media restricted or monitored?

5. Data Security

Yes	No	
☐	☐	Do we have an information asset classification policy and know what our critical and sensitive information is?
☐	☐	Do we know who has, or should have, access to our critical and sensitive information?
☐	☐	Is access to critical and sensitive information restricted based on the principle of least privileged access?
☐	☐	Do we use data loss prevention (DLP) policies?
☐	☐	Is critical and sensitive information encrypted or properly secured?
☐	☐	Are data backups routinely performed (e.g., daily), stored offsite/in the cloud, and protected from modification?
☐	☐	Is a data retention and disposal process in place?

6. Application/Software

Yes	No	
☐	☐	Do we have a solid list/inventory of all software and systems?
☐	☐	Is a secure software development lifecycle process in place that includes security requirements and best practices?
☐	☐	Are applications and software regularly patched/updated?
☐	☐	Are we monitoring for unusual or suspicious activity?

7. Physical Security

Yes	No	
☐	☐	Do we have controlled access to our facilities, buildings, and restricted areas (e.g., data centers)?
☐	☐	Is surveillance and monitoring in place to detect unauthorized access?
☐	☐	Are strong environmental controls like fire suppression systems, HVAC, and temperature sensors in place in data centers/closets?
☐	☐	Are our server and networking rooms locked?
☐	☐	Do we know who has access to our server and networking rooms, who is authorized to have access, and do we periodically review who has access?

Cybersecurity Protection Checklist

8. Disaster Recovery

Yes	No	
☐	☐	Have we identified and prioritized critical systems, processes, and dependencies?
☐	☐	Do we have a communication plan and protocols in place to ensure leadership, employees, and third parties are informed during a crisis?
☐	☐	Are annual data and system restoration tests completed and documented?
☐	☐	Do we perform regular tabletop and simulated failovers to reveal weaknesses/gaps?
☐	☐	Is the integrity of backed up data routinely assessed to ensure its usability in the event of business need?
☐	☐	Do we have redundant infrastructure (internet, generators, uninterruptible power supplies, etc.) where needed to minimize downtime?
☐	☐	Is appropriate documentation in place for systems, such as diagrams, dependencies, and architecture?

9. Business Email Compromise (BEC)

Yes	No	
☐	☐	Are email authentication protocols properly configured and enforced?
☐	☐	Is our email system protected by advanced threat protection that scans links and attachments?
☐	☐	Are we alerting for, blocking, and responding to risky sign-ins?
☐	☐	Are we alerted when email rules are created or when messages are automatically forwarded externally?
☐	☐	Are changes to banking information verified using a documented, out-of-band process (not just email)?

10. Continuous Improvement

Yes	No	
☐	☐	Do we receive regular cybersecurity reports or scorecards from IT or our MSP?
☐	☐	Are we conducting annual risk assessments to identify gaps and track progress?
☐	☐	Are findings and remediation plans documented and reviewed with leadership?