CopperHead Defense – Business Cybersecurity Risk Assessment

This short assessment helps identify potential security risks within your organization's technology environment. After reviewing your responses, CopperHead Defense will provide recommendations to improve your security posture.

Business Information

Company Name

Contact Name / Title

Email Address

Phone Number

Industry

Number of Employees / System Users

☐ 1–10
☐ 11–25
☐ 26–50
☐ 51–100
☐ 100+

Network & Infrastructure Security

1. Do you currently have a business-grade firewall protecting your network?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
Businesses should deploy a modern firewall with intrusion prevention, threat filtering, and network segmentation.

---

2. Are your network devices regularly updated with security patches and firmware updates?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
Regular updates prevent attackers from exploiting known vulnerabilities.

---

3. Is your Wi-Fi network secured with strong encryption and separate networks for guests or public access?

☐ Yes
☐ No

☐ Not sure

Security recommendation:
Guest networks should be isolated from internal business systems.

Endpoint & Device Security

4. Do company computers have endpoint protection or antivirus software installed?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
All business devices should run centrally managed endpoint protection.

---

5. Are employee computers automatically updated with security patches?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
Automatic patching helps prevent malware and ransomware infections.

Access Control & Identity Security

6. Do employees use multi-factor authentication (MFA) to access email, VPN, or business systems?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
MFA significantly reduces the risk of unauthorized access.

---

7. Are user permissions limited so employees only access the systems they need?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
Applying “least privilege access” prevents internal and external misuse of accounts.

Backup & Disaster Recovery

8. Do you have regular backups of critical business systems and data?

☐ Yes
☐ No
☐ Not sure

---

9. Have your backups been tested to confirm they can be restored successfully?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
Backups should be encrypted, stored off-site or in the cloud, and regularly tested.

Security Awareness

10. Do employees receive training on recognizing phishing emails and cybersecurity threats?

☐ Yes
☐ No
☐ Not sure

Security recommendation:
Employee awareness training reduces the risk of phishing attacks and credential theft.

Security Incidents

11. Has your organization experienced any of the following within the past 24 months?

☐ Ransomware attack
☐ Data loss
☐ System outage or downtime
☐ Unauthorized access attempt
☐ None of the above

Security Goals

12. What are your biggest concerns regarding your organization's cybersecurity or technology environment?

Additional Notes

13. Are there any upcoming technology projects or upgrades you are considering?

After submitting this assessment, a CopperHead Defense security specialist will review your responses and provide recommendations to strengthen your organization’s technology security.