Cyber Resiliency Assessment

Brought to you by Stillwell Risk Partners

Company Name: _____ Date: _____

Primary Contact: _____ Email: _____

Completed By: _____ Phone: _____

Cybersecurity Awareness & Culture

1. Do employees receive cybersecurity awareness training at least annually?	☐ Yes	☐ No	☐ Not Sure
2. Are executives and management included in cybersecurity training?	☐ Yes	☐ No	☐ Not Sure
3. Are phishing simulation tests conducted to see if employees can recognize fake emails?	☐ Yes	☐ No	☐ Not Sure
4. Do new hires get cybersecurity training during onboarding?	☐ Yes	☐ No	☐ Not Sure
5. Is there a mandatory training program for properly using social media for business purposes?	☐ Yes	☐ No	☐ Not Sure
6. Do you regularly review and update your cybersecurity practices, policies, and tech based on new threats?	☐ Yes	☐ No	☐ Not Sure

Company Policies & Governance

7. Do you have a formal cybersecurity policy with rules for passwords, data use, and acceptable tech?	☐ Yes	☐ No	☐ Not Sure
8. Does Management commit the resources needed to implement the program effectively?	☐ Yes	☐ No	☐ Not Sure
9. Do you have a policy for securely disposing of old data and personal identifiable information (PII)?	☐ Yes	☐ No	☐ Not Sure
10. Are wire transfers verified through in-person or secondary contact validation to prevent fraud?	☐ Yes	☐ No	☐ Not Sure

11. Are employee access privileges reviewed at least annually to ensure only the right people have access?	☐ Yes	☐ No	☐ Not Sure

Technology & Systems Protections

12. Is Multi-Factor Authentication (MFA) enabled for company email, cloud accounts, and financial systems?	☐ Yes	☐ No	☐ Not Sure
13. Do company devices (computers, tablets, phones) have Next-Generation Antivirus (NGAV) or Endpoint Detection & Response (EDR)?	☐ Yes	☐ No	☐ Not Sure
14. Are Remote Desktop Protocol (RDP) and Remote Desktop Gateway (RDG) access restricted or disabled unless secured with MFA & VPN?	☐ Yes	☐ No	☐ Not Sure
15. Is sensitive company data encrypted at rest (on devices) and in transit (during transmission)?	☐ Yes	☐ No	☐ Not Sure
16. Are data backups performed regularly to protect company data?	☐ Yes	☐ No	☐ Not Sure
17. Are data backups performed daily?	☐ Yes	☐ No	☐ Not Sure
18. Do you periodically test your backups to validate they're working?	☐ Yes	☐ No	☐ Not Sure
19. Are backups stored securely, offline, and segregated from the main network?	☐ Yes	☐ No	☐ Not Sure
20. Is all software up-to-date and regularly patched, including applicable Microsoft vulnerability updates?	☐ Yes	☐ No	☐ Not Sure
21. Is your network segmented to limit access and contain breaches (e.g., separating employee and guest Wi-Fi)?	☐ Yes	☐ No	☐ Not Sure

Incident Response & Recovery Preparedness

22. Is there an assigned individual or team specifically responsible for safeguarding privacy and network security?	☐ Yes	☐ No	☐ Not Sure
23. Do you have a clear process for employees to report suspicious cyber activity (e.g., odd emails or system glitches)?	☐ Yes	☐ No	☐ Not Sure

24. Does your company have a designated person or team responsible for cyber incidents?	☐ Yes	☐ No	☐ Not Sure
25. Do you have a documented Incident Response Plan (IRP) with clear recovery steps?	☐ Yes	☐ No	☐ Not Sure
26. Do you have pre-selected crisis partners (PR firm, forensic investigator, legal counsel) for cyber incidents?	☐ Yes	☐ No	☐ Not Sure

Third-Party & Supply Chain Risks

27. Do you assess the cybersecurity posture of vendors & suppliers before granting them system access?	☐ Yes	☐ No	☐ Not Sure
28. Do vendor contracts require cybersecurity best practices (e.g., secure data handling, cyber insurance)?	☐ Yes	☐ No	☐ Not Sure
29. Do you have a process for retrieving company data from vendors, former employees, and contractors after they leave?	☐ Yes	☐ No	☐ Not Sure
30. Do you verify that contracts with third parties for data management, hosting, or access include hold harmless agreements covering their negligence?	☐ Yes	☐ No	☐ Not Sure
31. When you sign contracts to use data from third parties, do you check that their hold harmless agreements and insurance terms protect you fairly?	☐ Yes	☐ No	☐ Not Sure
32. Do you mandate that third-party organizations involved in managing, hosting, and accessing your data maintain comprehensive professional liability (if applicable) and cyber liability insurance coverage?	☐ Yes	☐ No	☐ Not Sure
33. Are all third-party vendors and partners required to adhere to the same cybersecurity standards as your organization?	☐ Yes	☐ No	☐ Not Sure

Regulatory & Compliance Awareness

34. Do you follow industry-specific cybersecurity regulations (e.g., HIPAA, PCI-DSS, GDPR, CMMC)?	☐ Yes	☐ No	☐ Not Sure
35. If you process credit card transactions, do you comply with PCI-DSS security standards?	☐ Yes	☐ No	☐ Not Sure

36. Have you determined the total count of distinct personal information records (PII) stored within your network or by third parties acting on your behalf?	☐ Yes	☐ No	☐ Not Sure

Cyber Insurance Policy & Risk Transfer

37. Do you have a separate cyber insurance policy?	☐ Yes	☐ No	☐ Not Sure
38. Does the cyber insurance policy cover all types of cybersecurity incidents, including data breaches, network intrusions, and cyber-attacks?	☐ Yes	☐ No	☐ Not Sure
39. Are you aware of your policy's coverage limits and deductibles?	☐ Yes	☐ No	☐ Not Sure
40. Does the policy cover the costs of investigating a cybersecurity incident, including forensics and legal fees?	☐ Yes	☐ No	☐ Not Sure
41. Does the policy cover credit monitoring costs and identity theft protection for affected individuals?	☐ Yes	☐ No	☐ Not Sure
42. Does the policy cover the costs of restoring lost data and systems in the event of a cybersecurity incident?	☐ Yes	☐ No	☐ Not Sure
43. Does the policy cover the costs of business interruption and lost revenue in the event of a cybersecurity incident?	☐ Yes	☐ No	☐ Not Sure
44. Does the policy provide coverage for fines and penalties resulting from a cybersecurity incident?	☐ Yes	☐ No	☐ Not Sure
45. Does the policy cover the costs of cyber extortion and ransomware attacks?	☐ Yes	☐ No	☐ Not Sure
46. Does the policy cover liability for damages resulting from a cybersecurity incident, including lawsuits and sealements?	☐ Yes	☐ No	☐ Not Sure
47. Does your policy provide coverage for social engineering?	☐ Yes	☐ No	☐ Not Sure
48. Does your policy provide coverage for betterment to cover the cost of improving and updating computer hardware and software after a security breach?	☐ Yes	☐ No	☐ Not Sure

49. Does the policy provide access to resources and support in the event of a cybersecurity incident, such as breach coaches and crisis management services?	☐ Yes	☐ No	☐ Not Sure
50. Does your policy cover breaches caused by third-party vendors or partners?	☐ Yes	☐ No	☐ Not Sure

Next Steps

Often, this assessment is enough to show where there are gaps in your Cyber Resiliency and identify where to get started.

If you're looking for more resources, Stillwell Risk Partners is an insurance and risk management firm with a focus on helping businesses and organizations build their cyber resiliency.

To gain access to our resources, please submit this form to our secure portal at www.stillwellriskpartners.com/cyber-resiliency. We'll provide you with a full report and free 30 minute consultation.

Stillwell Risk Partners can also be contacted directly at 610.671.3500 or contact@stillwellriskpartners.com.