Cybersecurity Readiness Self-Assessment Questionnaire

This questionnaire covers various aspects of cybersecurity, from policy and training to technical defenses and recovery preparedness. It provides a broad overview of a company's cybersecurity readiness, helping to identify areas that need attention.

Please rate the following statements on a scale from 1 (Not Implemented) to 5 (Fully Implemented):

Cybersecurity Policy: Our business has a formal, documented cybersecurity policy that is regularly reviewed and updated.	
Employee Training: All employees receive regular training on cybersecurity best practices and are aware of their roles in maintaining security.	
Access Control: We have strong access control policies in place, ensuring that only authorized personnel have access to sensitive information.	
Data Encryption: Sensitive data, both in transit and at rest, is encrypted.	
Regular Backups: We regularly back up data and have tested our ability to restore it in the event of a data loss.	
Firewall and Antivirus Solutions: Robust firewall and antivirus solutions are actively used and regularly updated.	
Incident Response Plan: There is an established and practiced incident response plan for different types of cybersecurity incidents.	
Patch Management: We have a system in place for timely application of security patches to our software and hardware.	
Risk Assessment: Regular cybersecurity risk assessments are conducted, and necessary actions are taken based on the findings.	
Third-Party Vetting: Any third-party vendors or partners with access to our network are thoroughly vetted for their cybersecurity practices.	
Physical Security Measures: Adequate physical security measures are in place to prevent unauthorized access to our IT infrastructure.	
Two-Factor Authentication: Two-factor authentication is used for accessing critical systems and information.	
Cybersecurity Insurance: We have cybersecurity insurance to mitigate financial risks associated with cyber incidents.	
Regular Security Audits: External security audits are conducted regularly to assess and improve our cybersecurity posture.	
Awareness of Current Threats: There is a system in place to stay informed about current cybersecurity threats and trends.	
Total Score	

Scoring Interpretation:

0-20: High Risk – Immediate action needed
21-40: Moderate Risk – Improvement necessary
41-60: Low Risk – Good practices in place, but there's room for improvement
61-75: Very Low Risk – Excellent cybersecurity readiness

If you scored low and feel you would like to reduce your risks, please feel free contact the Launch57 team. We are eager to help!

Note: This questionnaire is a self-assessment tool and does not replace professional cybersecurity audits or consultations.