How cyber aware is your business?

Cyber awareness scorecard

20 questions to help identify cybersecurity gaps and guide a practical conversation with your technology partner.

How to use it
Review each statement with business leaders and your internal or external IT support, as applicable. Select one answer based on the organization's current, consistent practices, not future plans.

Scoring
YES = 2
PARTLY = 1
NO / UNSURE (?) = 0

Add all 20 answers.
Maximum score: 40.

Next step
Circle priority gaps, then discuss the completed scorecard with your technology partner.

1. Know your business risk

1. Decision-makers know which systems, data and services are essential to daily operations.	Y	P	N/?
2. The business has identified the cyber events most likely to interrupt operations or cause financial loss.	Y	P	N/?
3. Security responsibilities are clearly assigned across leadership, employees and technology providers.	Y	P	N/?
4. Cybersecurity risks are reviewed when the business adopts new technology, vendors or working practices.	Y	P	N/?
5. Leaders receive regular, understandable updates on cybersecurity risks and priorities.	Y	P	N/?

2. Protect what matters

6. The organization knows which users, devices and applications can access business information.	Y	P	N/?
7. Access to systems and data is limited according to each person's business responsibilities.	Y	P	N/?
8. Business devices, applications and accounts are kept current and securely configured.	Y	P	N/?
9. Critical data is protected with backup and recovery measures appropriate to the business.	Y	P	N/?
10. Employees know the organization's expectations for handling sensitive information and using technology safely.	Y	P	N/?

3. Spot and report warning signs

11. Employees know how to question and verify unusual requests before taking action.	Y	P	N/?
12. The organization can identify suspicious activity affecting accounts, devices or business systems.	Y	P	N/?
13. Employees are trained on the established channels and communication protocols for reporting security concerns or mistakes.	Y	P	N/?
14. Reported concerns are reviewed promptly and escalated through a defined process.	Y	P	N/?
15. Cybersecurity awareness is reinforced throughout the year, not discussed only after an incident.	Y	P	N/?

4. Respond and recover

16. The organization has a documented plan for responding to a cyber incident.	Y	P	N/?
17. Key contacts, decision-makers and technology partners know their responsibilities during an incident.	Y	P	N/?
18. The business can communicate with employees, customers and suppliers if normal systems are unavailable.	Y	P	N/?
19. Recovery procedures are tested, and the organization knows how long restoring critical operations may take.	Y	P	N/?
20. Lessons from incidents, tests or near misses are used to improve security practices.	Y	P	N/?

Your score: ____ / 40

Priority gaps to discuss: 1) _____ 2) _____ 3) _____

31-40 | Strong foundation	21-30 | Developing	11-20 | Important gaps	0-10 | Action needed
Maintain momentum and review changing risks.	Several practices exist, but consistency can improve.	Prioritize the lowest-scoring areas.	Begin with ownership, response and recovery basics.

Let's review your score.

This scorecard is a discussion tool. It is not a technical audit, compliance assessment or guarantee against cyber incidents.