Resilience Check

15-minute

Version 1.0

CYBERBUSTERS B.V.

How do you use this check?

Answer the 15 questions below honestly for your organization. Assign the following points to each question:

- **Yes** = 2 points
- **Partly** = 1 point
- **No** = 0 points

The 15 Practical Questions

Question	Answer options	Score
1. Is there a current and tested incident response plan?	Yes = 2 pt Partly = 1 pt No = 0 pt	
2. Do employees know who to report a (suspected) cyber incident to immediately?	Yes = 2 pt Partly = 1 pt No = 0 pt	
3. Are contact details for external experts (such as the IT provider, cybersecurity partner and insurer) immediately available?	Yes = 2 pt Partly = 1 pt No = 0 pt	
4. Are regular backups made and stored offline or in an isolated location?	Yes = 2 pt Partly = 1 pt No = 0 pt	
5. Has backup recovery recently been tested for functionality and speed?	Yes = 2 pt Partly = 1 pt No = 0 pt	
6. Is Multi-Factor Authentication (MFA) mandatory for all critical systems and accounts?	Yes = 2 pt Partly = 1 pt No = 0 pt	
7. Are security updates and patches applied automatically or within a short timeframe?	Yes = 2 pt Partly = 1 pt No = 0 pt	
8. Do employees receive periodic training on cyber risks such as phishing and social engineering?	Yes = 2 pt Partly = 1 pt No = 0 pt	

Question	Answer options	Score
9. Is there a clear protocol for isolating infected devices or networks during an incident?	Yes = 2 pt Partly = 1 pt No = 0 pt	
10. Are employee permissions and access limited to what is necessary for their role (Least Privilege)?	Yes = 2 pt Partly = 1 pt No = 0 pt	
11. Do we have visibility of all devices and systems connected to the corporate network?	Yes = 2 pt Partly = 1 pt No = 0 pt	
12. Are there agreements and protocols for communicating with customers and suppliers during a crisis?	Yes = 2 pt Partly = 1 pt No = 0 pt	
13. Is it known which legal notification obligations (such as those to the Dutch Data Protection Authority) apply and within what timeframe?	Yes = 2 pt Partly = 1 pt No = 0 pt	
14. Are critical business processes and data regularly mapped and categorized by risk?	Yes = 2 pt Partly = 1 pt No = 0 pt	
15. Does the organization review and revise its cybersecurity policy after every incident or at least annually?	Yes = 2 pt Partly = 1 pt No = 0 pt	

Your Score

- **26–30 points:** Resilient, your organization has an excellent foundation and knows what to do when things go wrong.
- **16–25 points:** Moderate, good steps have been taken, but critical vulnerabilities remain.
- **0–15 points:** Vulnerable, immediate action is required to safeguard business continuity during an incident.

Disclaimer: This resilience check is part of a broader assessment and does not replace a full audit or in-depth risk analysis.

Would you like to discuss the results and identify the most important risks or improvement areas for your organisation? Feel free to get in touch: https://cyber-busters.com/contact