

Cybersecurity readiness checklist

A breach is expensive, and recovery takes longer than most businesses expect. These questions show where you stand before you spend on new security tools.

01 What has your security plan focused on so far?

Antivirus, firewalls, multi-factor sign-in, email filtering, backups or not much yet.

02 If an attack happened right now, how would you know, and who would respond?

An alert, an employee, an IT provider or nobody specific.

03 How much downtime could you tolerate before it seriously hurt the business?

An hour, a day, a week.

04 Do employees get security awareness training?

Yes, sometimes or no.

05 Do you have a written incident response plan?

Yes, in progress or no.

06 Who handles security today?

An in-house IT person, a dedicated security engineer, an outside provider or nobody in particular.

07 Has anything prompted this conversation?

A recent incident, an audit, an insurance questionnaire or a customer requirement.

Rough answers are fine, and "not sure" is a useful answer. Please don't send account numbers, passwords or full bills; if we need to look at a contract, we'll arrange a safe way to share it.