Cybersecurity assessment: How to keep your business safe

60% of SMEs close within six months of a cyberattack. A cybersecurity assessment shows you what's working and, crucially, what isn't. Designed around the '5 Cs of cybersecurity', our simple seven-step checklist shows you want to look out for and how to protect your business.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

1 Set the scope

- Decide which part of your business you're assessing–the whole organisation, remote teams, supply chain, or a specific system.
- List the people, processes, tech, and third parties involved.
- Clarify what's in scope and what's not so nothing gets missed.

2 Identify and prioritise your assets

- List all business-critical devices–laptops, phones, servers, routers, etc.
- Include cloud platforms, email systems, and software your team relies on daily.
- Flag anything that stores, processes, or accesses sensitive data.
- Rank each based on how essential they are or how damaging it'd be to lose them.

3 Map out the risks

- Identify likely threats—phishing, malware, weak passwords, human error, supply chain breaches.
- For each asset, ask: What's the risk? How likely is it? What would the impact be?
- Highlight your biggest vulnerabilities–the ones likely to have the most impact.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

4

Review your current protections

- Check if your antivirus, firewalls, access controls, and encryption tools are active and up to date.
- Review data backup processes and how quickly you could recover from a loss.
- Assess employee training. Do your teams know how to recognise and respond to threats?

5

Review supplier and partner risk

- List suppliers, contractors, or service providers with access to your systems or data.
- Assess each to check if they're meeting your security expectations.
- Check any contracts and SLAs and make sure they have clear security requirements.

6

Create your action plan

- Create a clear, prioritised list of fixes, starting with quick wins and high-impact risks.
- Assign people and set a timeline for clear accountability.
- Monitor progress with regular check-ins.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

7

Test your business response plan

- Run a simulation or mock cyberattack to find out how your team responds.
- Check if your incident plan works in real-time to make sure everyone knows what to do, when to do it, and what happens next.
- Make sure backups, contact lists, and response roles are current and accessible.
- Adjust the plan as needed.

Ready to go from reactive to proactive?

Cybercriminals are getting more sophisticated and threats are changing all the time, so staying one step ahead is key.

By working through this checklist regularly, you can spot weaknesses early, stay compliant, and build better protection into your daily operations.

Need help getting started? Talk to our expert V-Hub advisers for free personalised support.

Want more help setting up a cyber security risk assessment?

Our V-Hub Digital Advisers are here to help.

vodafone business