West & Berry
ACCOUNTANTS AND REGISTERED AUDITORS

ACCA Think Ahead

www.westandberry.co.uk
hello@westandberry

Twenty questions to ask your IT provider

Many companies use external service providers to look after their IT systems to enable them to focus on their core business. Whilst the day-to-day management can be outsourced, security should be everyone's responsibility as the consequences if it goes wrong can be catastrophic. These questions have been developed using material supplied by HMRC and aim to promote conversation between businesses and their IT providers supporting a strong cybersecurity culture within the business. Security is a sliding scale that needs to be balanced within a risk management framework; not all of the methods discussed will be appropriate, or even sufficient, for different companies.

How do we protect our network?

1. How do we stop people accessing our network from outside?
2. If we did have unauthorised access, how would we identify it?
3. How do we secure our connection to our network when working from home?

Secure devices and software

4. Do we know what computers and devices we have connected to our network?
5. Do we know what software we have installed on our computers?
6. Is that software up-to-date?
7. What protects our clients' data if our devices get lost or stolen?

Control access to your data and services

8. Do our staff have administrator accounts with full control of their computers?
9. Do our staff use two-factor authentication to log into their online accounts?

10. If we can remotely log into our computers from home, how do we stop other people from logging in, too? How do we know that doesn't happen?
11. What extra controls do we have to protect our most sensitive data?

Protect yourself from malware

12. How do we stop malware getting in via email?
13. How do we stop malware getting in through web browsing, or USB devices?
14. How do we know when these controls have failed?

Being prepared

15. How does my IT provider keep their knowledge current about cyberthreats?
16. Are my staff aware of common cyberattacks and how to avoid them?
17. Do we have plans in place to promptly respond to cyber incidents?
18. Should an incident occur, do we keep enough system logs to enable an IT security specialist to determine the cause so our IT provider can fix it?
19. Is my business prepared with backup and plans in case our computers are locked with ransomware?
20. If my business has an internet domain, eg mybusiness.co.uk, has my IT provider enabled domain-based message authentication, reporting and conformance (DMARC) to limit criminals impersonating my business and abusing my brand?

The National Cyber Security Centre (NCSC) provides clear, practical advice and guidance for a range of audiences, including a dedicated section for small businesses: ncsc.gov.uk/smallbusiness.

Cyber Essentials is a scheme developed by government and industry to help business get the basics right to defend against cyberattacks. A self-assessment questionnaire can be completed to certify your business; this will reassure your customers about your security and may attract new business. If you're not Cyber Essentials certified already, consider working with your IT supplier to achieve it. For more information, visit cyberessentials.ncsc.gov.uk.

ACCA LEGAL NOTICE
This is a basic guide prepared by ACCA UK's Technical Advisory Service for members and their clients. It should not be used as a definitive guide, since individual circumstances may vary. Specific advice should be obtained, where necessary.

December 2018