National Cyber Security Centre

Moving online

Questions to ask your IT providers

COVID-19 has seen many organisations shutter their physical premises and move their business online. Establishing the IT services to support this transition can seem like quite a challenge. This guidance will help you determine how ready your business is, and point the way to any new cyber security measures you should put in place.

Dealing with new ways of working

Moving your business online will present some new risks, placing more reliance on digital technologies such as web hosting, credit card processing, and productivity tools like email, video and chat.

You shouldn't need a degree in computer science to run your small business securely. But, cyber security is complicated. If you don't have all the IT skills yourself, it can be hard to know what to do - and when you've done enough.

Having good relationship with your IT service provider(s) will help massively with this. So we've identified and explained the key cyber security topics we think you should care about, so you can be sure you're covering all the right bases.

1. Assess the cyber security of your business

Consider if the measures you take to deal with the lockdown will become more permanent ways of working. For example, will you look to expand your online business? If so, you'll need systems which are sustainable and can scale as your business adapts and grows.

2. Establish a baseline

Answering the questions below will give you a good idea of your security status, and identify what areas need attention. The NCSC's Cyber Essentials scheme provides a way to demonstrate to others that you have good security in place.

What IT products and services do you use? Is it your job to look after these, or a service provider's?

Some insurance policies now include a basic level of cover for cyber risks. This can be useful if you suffer an incident. Review your policies to understand the level and type of cover (if any) that is provided.

Are you using cloud services? The NCSC's cloud guidance can help you choose secure products, and use them safely.

Do you have access to IT support? As you become more reliant on digital services, think about how you'd cope if these were unavailable.

Are there any regulations you need to follow? If your business is now processing Personally Identifiable Information (PII) online, you will need to read up on GDPR. If you are processing card payment information, the Payment Card Industry Data Security Standard will apply.

3. Talking to your IT service providers

If you are talking directly with your supplier, the following questions will help you ensure that security is at the forefront of any new service you decide to take on.

Patching & Updates: Ask your suppliers how often they patch the services you use, and check any contracts or SLAs to ensure that patching is included.

Backups: What sort of backup arrangements are in place and how often are these tested? You should know how often your data is backed up, where it is stored, and who has access to it.

Access: Is your data (and the data of others which you have responsibility for) being properly protected? Are you able to put 2FA in place to limit access to your data and services?

Logs: Are logs being kept for security purposes? Logging can play a vital role in diagnosing any problems. Logs will also prove invaluable when responding to and recovering from security incidents.

Incident Response: What will happen if things go wrong? Service providers should operate on the presumption that they will be attacked. It should be clear how and when they will engage with you during a security incident.

Find out more

For more information about how to improve cyber security within your organisation, please read the NCSC web pages especially for small businesses at www.ncsc.gov.uk/smallbusiness.