Four simple steps to enhance your cyber protection

The threat of a cyber attack remains one of the biggest potential risks for UK business owners.

Taking these small steps will help ensure that your business is protected.

Step	What to consider	How you or your IT services provider can implement
Regularly back-up critical data to a "cold" or "offline" location and test to ensure those backups are recoverable.	• All organisations should take regular back-ups of their critical/important data and make sure that these back- ups are recent and can be restored. By doing this you can ensure your organisation can still function following the impact of a cyber attack, accidental deletion, physical damage, or theft of data. Furthermore, if you have back-ups of your data that you can quickly recover, you are much less likely to be successfully blackmailed by ransomware attackers. • The more regularly you change your files and data which are critical to your business, the more regularly you need to back-up. If you make lots of changes to critical data each day, then you should consider daily back-ups. If you have little critical data and make few changes then it is possible monthly back-ups may be regular enough.	• Many platforms have built in back-up functionality. Explore what options you already have. • Alternatively, you can explore either a third-party back-up solution (e.g. cloud backup platforms) or perform your own back-ups to external drives that you keep securely, disconnected from your live environment. To find out more please visit the National Cyber Security Centre.
Use multi-factor authentication (MFA) for cloud based services (such as cloud based email account access) and for all remote access to your network.	• Passwords no longer provide enough security especially for services available via the cloud (e.g. Microsoft 365, Google Workspace, etc). • Users might choose passwords that can be easily guessed and/or be susceptible to accidentally sharing their password via social engineering. • MFA is important as it makes stealing your organisation's information much harder for the average criminal.	• MFA doesn't eliminate usernames or passwords, but adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone or mobile app. MFA is built in to most cloud/internet based services so please enable it. • Alternatively, there are third-party suppliers that offer MFA utility through the use of SMS codes, unique codes and even hardware tokens. To find out more please visit the National Cyber Security Centre.
Only allow remote access into your environment with a virtual private network (VPN).	• Attackers are regularly "port scanning" the entire internet for visible remote-access services such as Microsoft's Remote Desktop Protocol (RDP). Any open RDP services will be constantly probed for weaknesses so hiding your remote-access services behind a VPN will afford a good level of protection against these attacks.	• Like MFA, there are many third-party providers that offer VPN services and your own networking infrastructure (e.g. routers) may also have this functionality built in, so may just need enabling. To find out more please visit the National Cyber Security Centre.
Provide cyber security awareness training annually which includes anti- phishing. Include all individuals who have access to your organisation's network or confidential/personal data.	• Your staff are at the frontline of your organisation. They are constantly exposed to electronic communications with third-parties that may leave them open to attack. Even though technical security measures like email gateways and endpoint detection and response (EDR) software may afford some level of protection, it is still essential for them to be aware of the risks. • Training will help them identify cyber risks and hopefully prevent them from impacting your organisation in the first place	• The National Cyber Security Centre (NCSC) offers free cyber security training for staff, which has an anti-phishing module within it. There are also third- party providers that offer a range of cyber security training services, such as our partner provider, KnowBe4. Beazley cyber policyholders receive discounted rates. To find out more please visit the National Cyber Security Centre.

beazley