One West
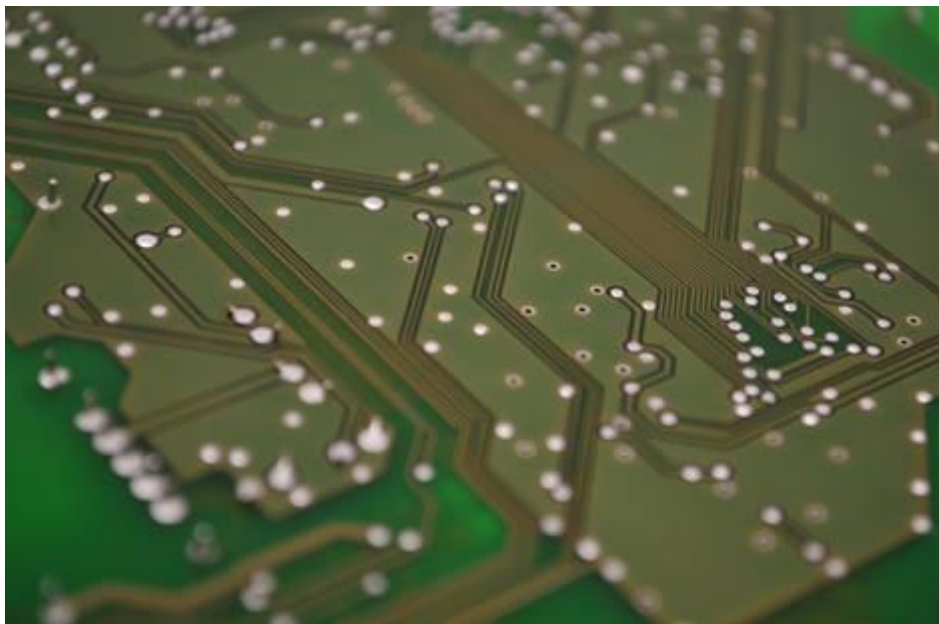
Important information – please pass to your Business Manager

6 weeks of advice on approaches to Cyber Security

Cyber Security #2

How can you start to 'raise the bar' on your approach to Cyber Security?

Consider for a moment just how much of an issue Cyber Security is.

To fight against it, our Government has linked the National Cyber Security Centre with GCHQ. This is one of the top electronic intelligence & security centres in the world. That's not done lightly.

We are getting used to thinking about Cyber threats as likely to compromise our ability to function but it does not stop there. The threats also link to GDPR, which we support many of you with. This link though is often not fully realised.

Basically, GDPR legislation says you have to have appropriate technical & organisational measures to ensure an appropriate level of security. The bottom line is potential for issues with the ICO, not to mention reputational harm.

There might be a tendency to feel somewhat disempowered in the flurry of cyber issues but actually you don't need to feel this way. There is a lot you can do.

A key point is understanding what to look out for & what can be done in order to raise your personal bar. This will help you raise it within your setting too.

It goes without saying we want to help – so lets get onto it:

#1 Take advice.

There is no 'right' answer to delivering Cyber Security. There are frameworks for provision of it but actually organisations have to work on their own approach. Having someone to help can be a great boost. We are there to help.

#2 Play your part in fighting back.

One of the biggest issues is suspicious emails & these are getting more sophisticated. The NCSC wants to know about these & is having some great successes in closing down scammers.

Anything can be reported the NCSC's **Suspicious Email Reporting Service** (SERS) at **report@phishing.gov.uk** . If you don't already, why not start reporting?

#3 Focus.

Rome was not built in a day & neither can your approach be. Close in on some of the key things of value to help you fight. 5 areas of investment can reap big benefits.

Consider looking at:

How are your boundary firewalls & internet gateways?
Is your IT configuration secure?
Do you have satisfactory access controls in place?
How good is your Malware protection?
Have you considered & done something about patch management?

#4 Keep on top of what's happening 'out there.'

There are lots of resources with useful information. Lately there has been some excellent information on ransomware attacks in the educational sector as well as advice to early years practitioners. Both are worth a thorough read.

#5 Communicate relevantly & currently.

New threats emerge often. Heard of 'Credential Stuffing'?

This is where stolen usernames and passwords are 'stuffed' into various web based system logins with the hope of entry.

Slightly different to brute-force where the hacker uses software to crack passwords one character at a time. The key to combatting this is better password management & that's something you can talk to others about right now.

A top tip is that Password managers help. Something like Dashlane (which has a free version) can save a lot of time when trying to think of a password.

#6 Make Cyber Hygiene your mantra.

Repetition is the key to making sure everyone understands the need for this & takes note. For sure, risk in this critical area is not going to go away.

Many of you will be early in your journey & may be scratching your head on next steps. Our best advice is to consider a health check. We can help you with that & would be delighted to have a conversation.

Watch out for our next bulletin **Cyber Security #3** – part of our **6 weeks of advice** on this extremely important topic.

If interested, drop us a line & we will happily get this arranged. Contact:

Steve_Debruin@bathnes.gov.uk or

Jo_Buchan@bathnes.gov.uk

Thanks & we look forward to telling you more.

The One West **Business & Cyber Security** team.