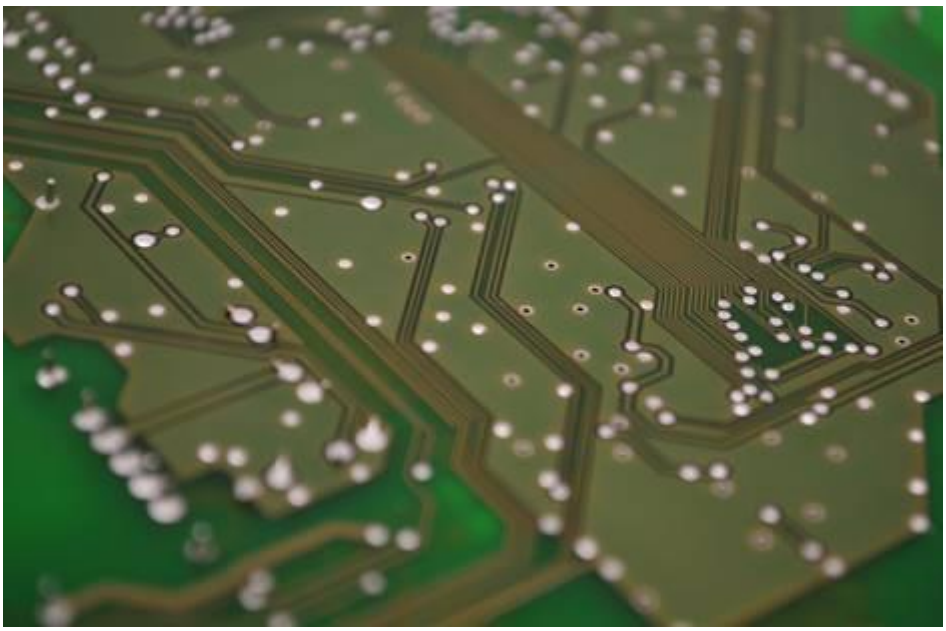
Important information – please pass to your Business Manager

How can you judge if you are doing enough on Cyber Security?



Achieving proportionate responses to Cyber Security threat

The National Cyber Security Centre is warning to be extra **vigilant** as the tragic events unfold in Russia and the Ukraine. It's a reminder that conflict these days transcends boundaries & that the arsenal of weapons available **includes** those related to **Cyber Security.**

It might be that you don't think you might be a **target** – perhaps only larger multi national organisations should worry? Actually no - there are plenty of '**threat actor**' groups who target **third sector** organisations with unfortunately Russia being quite active. Look out for 'Turla', 'Wizard Spider', 'TA505' & 'REvil'.

However you **can't** focus too hard on one thing – Cyber threats can come from **many directions**. Analysis shows that for schools & colleges upwards of 80% can expect Phishing attacks but actually the range of other possibilities is **daunting.** Impersonations (as much as 58%), Viruses (30%), unauthorised access (14%), denial of service (30%), hacking (5%) & ransomware (8%), are clear & present risks. The Government full report is **here**

In some ways though stark this isn't news. So you would think everyone is **prepared** - right? Actually, **no.** In the Charitable sector over a **quarter** of charities reported attacks with a similar proportion saying they happened weekly. In response just 32% said they did cyber security assessments & only 27% had Business Continuity plans with cyber security included. It also appears gaps might be **widening** – only 69% had malware protection & 57% had sufficient network firewalls and this figure is **DROPPING**.
The Governments statistics are **here**

So **why** the gap? It's difficult to say but Covid has had an effect & high levels of homeworking with its associated challenges are here to **stay**. For sure if nothing is done with increased sophistication in types of threat the gap will **increase**.

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 & that of your organisation too.**

It goes without saying we want to help – so here is what we think:

#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. Choose a partner.

#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.

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. We think the South West Regional Organised Crime Unit information is particularly good in talking about what our police are doing & how we can all engage.

#5 Communicate relevantly & currently.

Threats emerge often. Heard of 'Credential Stuffing' or 'Brute-Force'? The key to combatting these in particular are better password management & that's something you can talk to others about right now. You need to keep reading & keep communicating though.

#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.

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 team.

Our mailing address is:

One_West@bathnes.gov.uk

Want to change how you receive these emails? Just let us know