www.onewest.co.uk

Important information – please pass to your Business Manager

6 weeks of advice on approaches to Cyber Security

Cyber Security #4

Cyber Security – just who are the 'baddies' and how bad are they?

Do you know what sort of people are behind **Cyber Crime**? Many **aren't** clear.

You might have heard of **'Cyber Threat Actors.'** That is the **umbrella term** for those involved in Cyber Crime but actually the types of people involved are quite **different**

'Hacktivists' and some **Nation States**, actively pursue a **political** or **macroeconomic** aim. For sure, they pose a big problem as a whole (actually sitting alongside terrorism as a tier 1 threat) but they **aren't** after **schools**, **local authorities** and **SME's**.

Of more relevance for you, are those who **would** wish to disrupt your organisation.

These fit into **three main types**:

'Unskilled Individuals'. These are the people who pepper us with **phishing emails**, **phone calls** & the like. Frequently they are quite clumsy, or something about it' just doesn't feel right.' We have to keep our guard up though.

'Script Kiddies'. Often young, often known to you & very often, bearing a grudge or with something to prove. They might even be on site with you.

These are people who, simply want to use their knowledge & skill to cause **disruption**. You have to be careful not only looking **outwards** but also vigilant **inside** with these.

And most **serious** of all:

'Organised Crime Groups' (OCG's). These people want your money & will do anything they can to get it. Worse still, is what they use the money for – very often, human & drug trafficking.

As bad goes, they are **very** bad indeed.

OCG's are **growing** & finding relatively soft targets – very **often** educational establishments. What is worse, is that for them, it is **working well**.

There is every **incentive** to continue & unwittingly, organisations who are bribed, are helping to pay for things they would **unequivocally condemn**.

OCG's preferred method right now is to use **'Ransomware,'** which is what it sounds like – they **disable systems**, demanding considerable sums of money to unlock them Sometimes they threaten to **expose data** too.

The risks are therefore **threefold** – potential **Data Breach**, compromised **IT** & difficulties with **Business Continuity**.

If it happens – definitely not a good day at the office but it is **more serious** than that.

Nobody wants to give up money but considering its future likely use for things, which are as bad as they are, the **dilemma** is even **worse**.

The threat is such is that an international **Ransomware Taskforce** has been formed, supported by the **National Crime Agency** & the **National Cyber Security Centre**, in this country.

The taskforce is there to **break the circle** & is calling on everyone to take part in action deterring Ransomware, thus **disrupting** the 'Ransomware Business Model.'

This means organisations getting a lot more active in **reviewing**, **preparing** & **planning** for **resilience** if the worse happens.

We want to play our part & if **you** do too, we would like to talk.

There is a lot you can do to **review** & **understand** your current vulnerability, in order to **plan** for improvement.

Why don't we do our bit together to help **prevent** the spread of Cyber Crime?

If you want a **conversation** we would love to talk.

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.

Watch out for our next bulletin **Cyber Security #5** – part of our **6 weeks of advice** on this extremely important topic.

Our mailing address is:

One_West@bathnes.gov.uk