www.onewest.co.uk

Important information for your Business Manager

Cyber Security – let us help you manage 'Internal Cyber Threats'

'Insider threat' is a real issue in managing Cyber Security. What do you need to do?

We tend to think about Cyber threat as **'out there'** & within our organisations we work hard with colleagues to form bonds & establish trust.

Does that mean anyone should let their guard down with regard to Cyber threats coming from **inside** where we work?

The answer to that is **no** - & this is especially now that for many, our workplaces have a strong virtual element in them.

Also, it needs to be remembered that issues can be **unintentional** as well as **intentional**. If not considered that increases risk.

The South West RCCU have recently raised some interesting points after the conviction of a former IT Technician who had been working with Welland Park Academy in Market Harborough.

In this the person involved worked for a 3rd party provider. After leaving, the individual wiped data, changed passwords & prevented whole school access to the system – **serious stuff.**

So how do you go about managing internal threats?

- **When you recruit or hire do the right checks.**

Make sure staff are vetted to include any Cyber Security past issues. Think in the same way for 3rd party vendors, sub-contractors and other partners.

- **When people leave do the right things to tighten things up.**

Principally this involves revoking user access to shared systems & blocking any passwords formerly used. Look to archive appropriately & delete what isn't needed.

- **Think about the principle of 'Least Privilege.'**

For everyone's protection IT users should only have access to data they need for their work. The fewer highly privileged accounts the better. Also of course as people move around update their privileges accordingly.

- **If possible split the most sensitive processes up.**

Consider if sensitive processes can be split so that more than one person has to complete them. It helps reduce potential for fraud, mistakes & the risk of over reliance on a single person.

- **Check for things that seem different.**

Checking & logging work sessions can illuminate abnormal behaviour. It is sensitive & not the easiest thing to do but certainly if you have any suspicions do it.

- **Ensure training and awareness.**

IT & Cyber issues are moving so fast it is breathtaking. Cyber training & awareness is now a fundamental part of doing our jobs well & safely. Make sure you have access to this in place.

- Make sure your people think it's ok to speak up.

You can't be everywhere & others may well pick up things that concern them. Make sure staff know how to report & be responsive. It may be nothing but good sense says check.

Interested?

If you want to talk with us about this we are there to help. We are partnering organisations to review & make sure Cyber Security related practices are fit for purpose & will remain that way.

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.