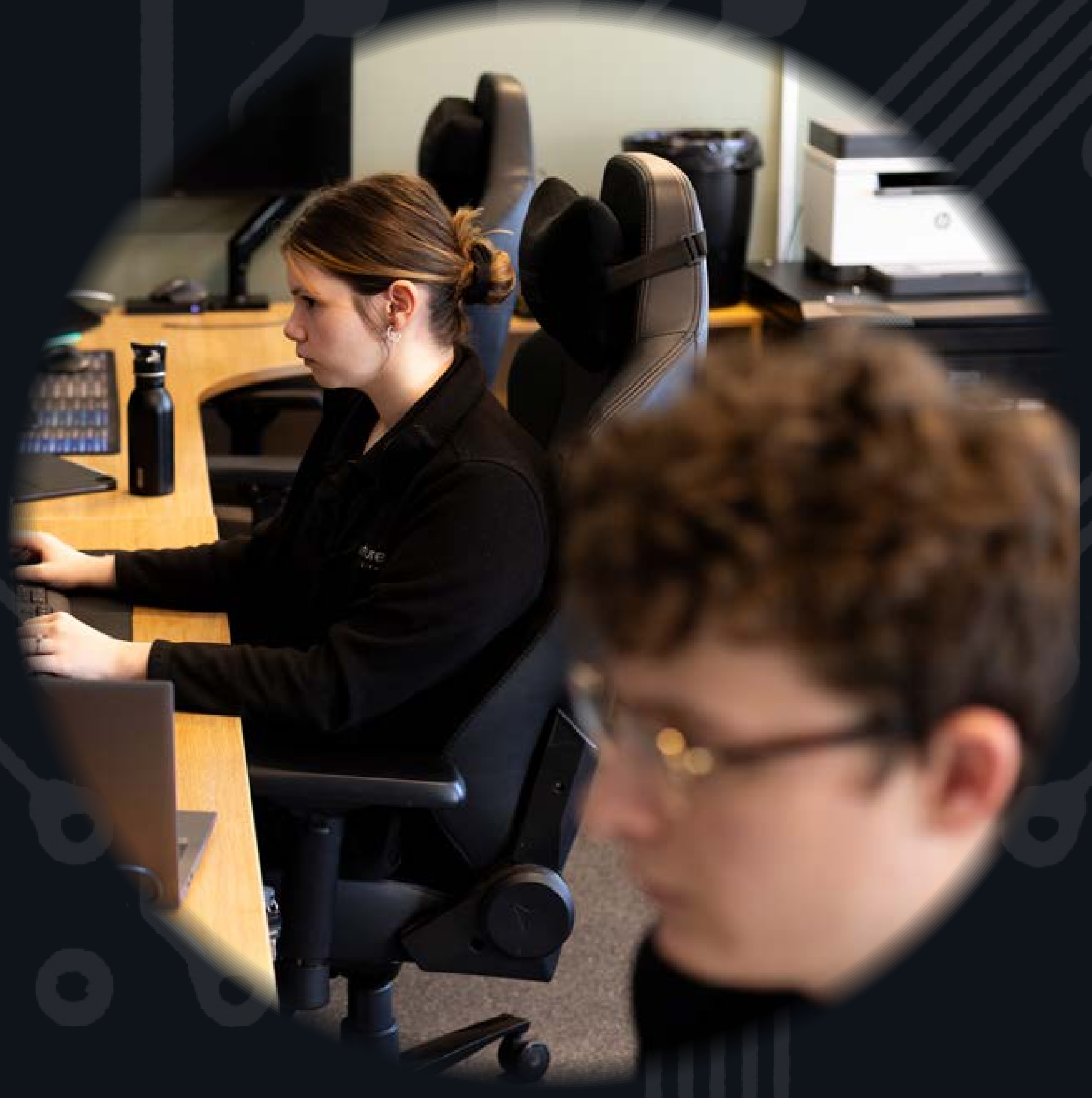
interfuture
BUSINESS IT SECURITY

Interfuture Security News



Now we're getting into the summer months, the cyber security landscape is heating up! Find out all about it in the June edition of the **Interfuture Security Newsletter.**

We give you a step by step guide to navigating a ransomware attack and explore an upcoming bill set to be passed into UK law that could have a significant impact on your IT security.

As always, any feedback or queries please contact us via our social media channels or on our website.

Key Point

Ransomware is a type of malware – malicious software – that can infect devices via phishing emails, malicious links, vulnerabilities in software or compromised websites.

What makes ransomware unique is that once it is inside a system, it locks or encrypts files and displays a message demanding payment to be made to return the files to the user.

Ransom - be - ware!

If you are the victim of a ransomware attack, what steps you should take?

Isolate: disconnect affected systems from the network, remembering to disable Wi-Fi and unplug ethernet cables.

Notify: make your leadership team aware of the breach, to prevent it spreading further.

Report: report to **Action Fraud** or the **National Cyber Security Centre**, as well as your cyber security provider (us!).

Assess: identify impact and check logs to understand the scope of the attack.

Don't pay: even if you do pay, there is no guarantee that your data will be recovered, and it may further criminal activity. Talk to law enforcement and cyber security experts before acting.

Restore: if clean backups exist, wipe infected systems and rebuild from backups, ensuring the backups are scanned for malware before restoring.

Investigate: determine how the attack happened, finding vulnerabilities and entry points.

Strengthen: make updates and additions to fix the gaps in your security found in the investigation. Additionally, training on phishing and social engineering for all staff is essential.

Before the Bill

In 2024, it was announced as part of the King's Speech that the **Cyber Security and Resilience (CS&R) Bill** would be introduced over the next two years. The purpose of the bill is to modernise and improve the UK's cyber security framework. So, what is the bill rumoured to contain?

Organisations such as Managed Service Providers (MSPs – like us!), data centres and critical suppliers will be brought under regulation and held to higher security standards. Often, breaches occur when one link in the chain has poor defences – this will improve resilience not just for these organisations, but those connected to them.

Additionally, the regulators in question will be given better enforcement tools, allowing them to mandate measures and penalise non-compliance with fines and audits. These regulators include **National Cyber Security Centre, Department for Science, Innovation and Technology, Ofcom, Ofgem, Ofwat, Civil Aviation Authority** and **Information Commissioner's Office.**

Furthermore, these organisations will be able to use tools like the **Cyber Assessment Framework (CAF)** and **Cyber Essentials** to keep businesses up to a high standard of cyber security. A broader range of incidents will need to be reported, to give the government a better picture of national cyber threats.

The bill will reflect lessons from recent attacks, modernising legislation to keep up with emerging technology. Attacks such as the 2024 **Synnovis NHS** breach, that caused widespread delays and difficulties, helped the UK government to realise where improvements should be made.

What impact will the bill have? Businesses will have to update their cyber security measures to meet these higher standards. For some industries, few changes will be needed, but for critical services it may be a significant step forward.

Also, incident response plans and supply chain risk assessments will likely become more essential than ever. If you'd like any more information about the **CS&R** bill, please ask us, we'd be happy to discuss it.

Pretty Please?

We don't want to sound desperate, but we would really love it if you could leave us a review on **Trustpilot!** Not only does it help us to find new clients who need cyber security assistance, but it helps us to improve our services for you.

If you could leave a review via the link in the footer of this email, it would be greatly appreciated.

Review Interfuture Security HERE

★ ★ ★ ★ ★