newsletter

March, 2026 | Volume 05

At Resilience, we are more than a cybersecurity provider - we are a trusted partner. We help organisations protect against evolving cyber threats while building long-term digital resilience.

Important changes to Cyber Essentials

Cyber Essentials is set to become harder to attain when the updated question set launches on April 27th.

New automatic failure points include not enabling multi-factor authentication on cloud services and not applying patches within 14 days. The rules around scope are also being tightened, and Cyber Essentials Plus assessments will adopt a more stringent approach.

An introduction to Cyber Security Webinar.

Wednesday 25th March 2 PM - 2:45 PM

Join us to talk all things Cyber and let our expert guide you through the ever changing world of cyber.

Click here to sign up

Business Security, Simplified Event.

Carlisle Racecourse, CA2 4TS

Thursday 23rd April 10 AM - 2 PM

With speakers from Sophos, Gamma, Zest4, Westcoast and Resilience by Eco.

Click here to sign up

Did you know we offer Dark Web Monitoring?

Dark web monitoring scans the dark web for stolen company credentials or sensitive data. We monitor underground forums and marketplaces for company-specific information (e.g., email addresses, passwords, payment details) and provide alerts if your data appears on the dark web.

This enables you to take proactive measures to secure affected accounts and prevent further compromise.

Feedback from Road Transport Solutions

We experienced a compromised Microsoft 365 tenant account and required urgent assistance.

Resilience by Eco were able to intervene promptly and resolve the issue in a timely and controlled manner. The service provided was excellent.

Following this engagement, we have since taken out a Sophos subscription.

Resilience was recommended to us and we, in turn, highly recommend their services to others.

What would you do if your business received a Cyber Threat Awareness Notice tomorrow?

Be aware that cyber threats are increasing, and organisations in your supply chain should reassess their security.

Consider whether:

- Multi-factor authentication is enabled for all accounts
- Your team can recognise phishing or social engineering
- Remote access and legacy systems are properly secured
- You can identify unusual network activity in your environment

QUICK TIP OF THE MONTH

Remove access to the people who no longer need access.

Old accounts and leftover access are often forgotten.
Regularly review who can still get into systems and tools.