ICO’s call to action amid rising cyber attacks

The ICO has issued a statement following an increase in the number of cyber breaches being reported to it.

24 June 2024

The Information Commissioner's Office ('**ICO**') has recently issued a statement urging all organisations to enhance their cyber security in order to protect the personal information they hold. This call comes in light of the ICO noticing an increase in the number of cyber breaches being reported to the ICO, with over 3,000 reported in 2023, particularly in the finance, retail, and education sectors.

The ICO has also shared a new report, "Learning from the Mistakes of Others", which provides insights into common security mistakes and practical advice for enhancing security measures. It identifies five main causes of cyber security breaches:

- **Phishing**: where fraudulent messages trick users into sharing passwords or downloading harmful software.
- **Brute Force Attacks**: where criminals use trial and error to guess login details or encryption keys.
- **Denial of Service**: where criminals overload a website or network to disrupt its normal functioning.
- **Errors**: where security settings are misconfigured due to poor implementation, lack of maintenance, or unchanged default settings.
- **Supply Chain Attacks**: where criminals compromise an organisation's products, services, or technology to infiltrate their systems.

The ICO emphasises that organisations must report any data breach from a cyber attack within 72 hours of becoming aware of it.

To support you in managing such incidents, our Cyber Response+ service is available 24/7 worldwide, ready to assist you in navigating and mitigating the effects of a data breach. Please feel free to reach out to Lawrence Brown or Robert Allen if you would like to sign up.