Browne Jacobson

Lessons from the 2025 cyber security breaches survey for higher education

29 April 2025 Matthew Alderton

On 10 April 2025 the government published its annual Cyber Security Breaches Survey, which aims to explore the policies, processes and approach to cyber security, for businesses, charities and educational institutions.

Consistent with the findings of previous surveys, the 2025 survey of 32 higher education institutions found that they were more likely to be affected by cyber breaches and attacks on a frequent (weekly) basis (30%) compared to primary schools (9%) and secondary schools (16%).

91% of higher education institutions attacked

Overall, 91% of higher education institutions surveyed had experienced a cyber attack during the previous 12 months and 40% of those affected experienced a negative outcome as a result.

The following types of breaches or attacks in the last 12 months were found to be most common for higher education institutions (in descending order):

- Phishing attacks.
- Impersonation.
- Viruses, spyware or malware.
- Denial of service attacks.
- Ransomware.
- Takeover of organisation's user accounts.
- Unauthorised access by students.

As in previous years, many educational institutions expressed low awareness of government guidance like the National Cyber Security Centre's (NCSC) 10 Steps to Cyber Security and Board Toolkit, certification schemes like Cyber Essentials, and communications campaigns like Cyber Aware.

Further, although higher education institutions scored well on matters such IT architecture and configuration, awareness and training, and the logging and monitoring of incidents, the survey showed there was still work to be done around supply chain security and the management of risks, incidents and assets.

Supply chain vulnerabilities

These are matters that can have a significant impact on an institution if neglected. There has been a significant increase in cyber-attacks as a result of vulnerabilities within supply chains in recent years, which can lead to expensive and long-term consequences for institutions.

Available support

We recommend higher education institutions make use of the helpful guidance published by the NCSC and ICO to help to alleviate these risks.

Our data protection team are experts at advising higher education institutions of the steps they can take to boost their cyber security and protect the personal information they hold amid the growing threat of cyber-attacks.

Please don't hesitate to contact us if you have any questions around data security, supply chain security and risk management.

Contact

Matthew Alderton

Partner

matthew.alderton@brownejacobson.com

+44 (0)330 045 2747

Related expertise

Data protection and higher education

Data protection and privacy

Supply chain optimisation