Browne Jacobson

Facing the threat of cyber security breaches

Universities and colleges are not immune from deception by unscrupulous bad actors. The extent to which educational institutions can manage and control risk not only depends on financial management and internal controls, but also the robustness of security and processes which can be exploited from outside the organisation.

07 October 2022

Universities and colleges are not immune from deception by unscrupulous bad actors. The extent to which educational institutions can manage and control risk not only depends on financial management and internal controls, but also the robustness of security and processes which can be exploited from outside the organisation.

Internal fraud can be demoralising. Staff exploiting weaknesses in internal processes to set up false suppliers, abuse the company credit card or claim additional expenses appear minor, but all amount to fraud and could have serious repercussions for the individuals concerned.

A recent decision in the Supreme Court in R v Andrews [2022] UKSC 24 has highlighted that anyone falsely claiming qualifications on their CV can be stripped of the profits of their deception. The Supreme Court permitted a Proceeds of Crime Act 2002 (POCA) confiscation order on the basis of the pre-appointment earnings. Ensuring that validation in recruitment processes is properly and diligently carried out would avoid the worst excesses of CV fraud, but would also deter appointments of people who may see education as a soft target.

But what of the external actors who target education and charities, who rely on volunteers, community support, co-operation and public goodwill to operate effectively and generate additional income? The sophistication and variety of modes of the attack has certainly evolved over the past two years, as has the frequency of experience and level of disruption caused.

“92% of HEIs identified a breach”

The Department for Digital Culture Media and Sport has surveyed the education sector as part of its aim to inform government policy on cyber security in its annual Cyber Security Breaches Survey 2022 . The results show 92% of higher education institutions identified a breach, while the education sector as a whole, experienced some of the highest levels of the most dominant form of attack in phishing emails, outstripping even the business sector.

But one concern is the survey identified that most education establishments experienced some form of attack or breach on a weekly basis. Spoof emails or impersonation attacks, and attempts at gaining unauthorised access through malware, were also a common occurrence.

The high levels of reporting could point to increased security, senior management engagement and staff vigilance underlining their preparedness to invest in approaches to prevent attacks – such as security monitoring or penetration testing, as well as maintaining risk assessment and disaster plans to trigger appropriate responses.

In reality, where these attacks were effective, a significant proportion of the institutions experienced a negative outcome, with loss of data for illicit purposes or financial losses or accounts systems being compromised. As a consequence, they reported significant disruption with increased manpower and staff time to deal with the reporting and stakeholder engagement, post event.

Kudos to the education sector

One key feature of the report is the kudos given to the education sector as a result of its cyber security planning and policies, the level of knowledge of directors and trustees and how they dealt with breaches – including external reporting (with stakeholders, insurers, regulators) and implementation of additional controls (passwords and two factor authentication). In fact, it was regarded as the equivalent of large businesses, who are considered to be the most well-equipped to deal with these issues.

It is perhaps testament to the education sector's reported high levels of compliance with the 10 Steps to Cyber Security and its proactivity in seeking guidance and enhanced security that has led to its overall rating which, in some instances, outperforms businesses. Despite the concerning levels of attacks which target educational institutions, these efforts go a long way to block potential disruption. Regrettably, in the digital and online times in which we live, it does not eradicate the risk, but it mitigates the harm and allows educators to focus on what they do best, which is heartening news.

Contact

Paul Wainwright

Partner

paul.wainwright@brownejacobson.com

+44 (0)121 237 4577

Related expertise

Data protection and higher education

Education law

Fraud and asset recovery