Chartered Institute of Information Security

Pulse:

May 2022

Education Matters

Educational institutions top target for malware attacks during pandemic

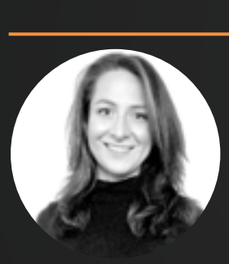
Multi-Cloud Security

Possible solution to protect end-users data from cyber threats?

Life after a breach

Managing all of your communications properly after a breach

EDUCATION MATTERS



DR Caroline Stockman
Senior Lecturer in Education Studies, University of Winchester

The education sector experienced a sharp rise in cyberattacks during pandemic times, amidst the rushed shift to remote learning and heavy dependence on new IT systems. This rise is acknowledged across different national and international reports and appears to be higher than the average yearly increase in cybercrime, considering both its general prevalence as well as sector-specific trends.

Educational institutions are not randomly caught in the line of fire during cyberattacks. Even prior to the COVID-19 pandemic, education formed a particularly lucrative, specific target for cyber criminals. Its high-value assets include a wealth of personal and sensitive data about children and adult learners (including grade outcomes, notes on behaviour and pastoral care, learning disabilities and impairments, contact details, staff data, teaching resources and intellectual property.)

The most common attacks materialise as ransomware incidents, typically sparked by a school network infiltration of malware through a phishing email. The criminal activity exploits existing vulnerabilities of the sector, which Tes, formerly known as the Times Educational Supplement, describes as substandard technical infrastructure due to tight budgets, as well as a lack of human capability such as inaccurate understanding of the threat or how to manage an attack.

According to 2021 SonicWall Cyber Threat Report, educational institutions experienced more malware attempts than any other sector from August to October 2020, the start of the first school year in pandemic times. This trend continues in 2021, with an average of 22.5% of education customers targeted by malware in any given month according to the 2022 SonicWall Cyber Threat Report. This correlates with multiple warnings in 2021 by the UK's National Cyber Security Centre (NCSC), reporting a significant increase in ransomware attacks on educational institutions. However, some data pertaining to late 2020 indicate slightly fewer data breaches occurred than expected. According to the Department for Digital, Culture, Media, and Sport, this might be due to fewer breaches being reported, rather than fewer breaches actually taking place. Certainly the endeavour to continue education in a pandemic was already extremely trying and hectic in itself, aside from avoidance behaviour in causing reputational embarrassment and financial liability, known to occur in other sectors as well.

Human factors are still a prevalent cause for incidents to occur. These range from causing unintended disclosures typically of a smaller scale (such as emailing data to the wrong recipient), to unlocking highly sophisticated phishing and ransomware attacks, which are widespread and damaging across the sector.

In their 2021 Cyber Security Breaches Survey, the UK government reports around a third of secondary schools, and a quarter of primary schools, have experienced loss of control, data or money due to cyber attacks, being predominantly phishing attacks. Though cyber security has grown to be a common priority for school leadership, financial constraints are a real issue for many schools, even in multi-academy trusts which typically have greater financial autonomy and internal resilience. Still, highly secure systems, IT support, staff and student training … all costs more than budgets allow at times.

According to 2021 SonicWall Cyber Threat Report, educational institutions experienced more malware attempts than any other sector from August to October 2020,

For tertiary education, Jisc finds that approx. 60% of Further Education colleges and Higher Education institutions reported cyber security incidents in 2021, with multiple high-profile incidents in the UK. Next to the assets produced by its teaching activity, there is also the Higher Education sector's unique need to develop state-of-the-art knowledge and cross-institutional research collaboration, which will include sensitive data on research subjects, or other assets such as intellectual property.

Aside from the common financial and reputational damage, the disruption in education also affects student satisfaction scores, teaching efficiencies (which impact measures such as grade outcomes and student employment success rates), and research excellence (measured by government-regulated audits and internal output comparisons). All of these directly influence a school, college or university's place in national and international rankings, which impacts national and international student intake, confidence from research funding organisations, attractiveness as an employer,…

Yet despite its clear vulnerabilities, we can also have confidence in the power of education and training to improve all-round cyber resilience. On one hand, this must include 'the basics' such as being told the rules of good password management or attention to personal devices on campus. However, for people to truly learn something, they need to understand why they're doing it, and even more importantly, (learn to) care about it. So cybersecurity training which is built to stimulate formulaic, rule-driven behaviour management or purely technical compliance will limit the educational potential. To create strong, secure institutional cultures, we must aim to spark an intrinsic commitment which good education can achieve.

It makes sense because we know that aside from its technical compliance requirements, cybersecurity is a social practice. It isn't just machine-based, yet research shows educators often consider it to be an IT issue. Reversely, it's important we do have IT support and development which understands the special and specific nature of educational settings. To achieve good cyber resilience, we have to aim for education which bridges a gap.

It's the core of my own teaching and research. Our BA in Educational Technology for example aims to bridge that gap and educate many generations of strong graduates, to work in educational institutions or industry settings. It provides a unique combination of educational theory and hands-on computing, with the intrinsic purpose of building better worlds. Whether that's in the role of teachers, learning technologists, software developers, database managers, IT support, information security experts, …

We need more people who speak both languages: human, and machine. Much like any language learning, it goes beyond repetition of words and sounds, to a deeper understanding of meaning, connotations, and the values and beliefs which make up a culture. In my research on technology acceptance and digital data protection rights, successful integration always comes back to a consideration for the symbiotic nature of human-technology living.

Current events re-emphasise the importance of that deep symbiotic view. At the start of March 2022, the NCSC and Jisc warned the education sector to brace for the likely impact of Russian state-sponsored cyber attacks, following their aggressive physical invasion of Ukraine. These attacks already include a high increase of hostile emails, attempting to spark the common ransomware incidents as well as brute Denial of Service attacks. In light of these increased threats, our defensive resilience relies more than ever on strong and holistic human-technology education.