enter

Cyberis

The Case for Real-World Attack Simulation in Schools

Introduction

The cyber-attack threat to our educational institutions is clear and present.

According to the Department for Digital, Culture, Media, and Sport's 2021 Cyber Security Breaches Survey[1], 58% of secondary schools suffered some form of cyber-attack or breach in 2020, as well as 75% of further education colleges and 36% of primary schools.

"Over nine in ten say that cyber security is a high priority for their governors or senior management (98% of primary schools, 94% of secondary schools and 95% of colleges). This is more in line with large businesses (93%) than with the average UK business (77%)."

Schools have an appetite for prioritising cyber security which matches that of large businesses, but schools face greater challenges and fewer resources when it comes to cyber security defences. When we asked a local education specialist how well cyber security challenges were understood within the Education sector, we were told:

"Not all schools have sufficient knowledge or expertise in-house, or externally-sourced IT support is not good enough (lacking proactivity). The rise of MATs has made this more challenging as there is no set structure and this leaves many schools vulnerable - particularly in terms of ageing equipment and resources."

Our schools are passionate about improving learning outcomes, and this drive to improve education also means that they regularly embrace new technology and new solutions which improve student and teacher interaction. There's a downside to rapid innovation when you have stretched resources, though. One local school told us:

"The introduction of new features is continuous, and it is very challenging on school budgets to keep technical staff trained in order to manage the systems."

The National Cyber Security Centre (NCSC) has alerted schools[2] of increased ransomware attacks against the UK education sector by cyber criminals.

"In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing."

Ransomware is a type of malicious software which is designed to prevent the use of computer systems until money is paid to the software controllers – a ransom. The impact of ransomware on a school can be severe, preventing access to educational resources and essential safeguarding information.

The newest trends for this type of attack also involve the theft of sensitive data which the attackers threaten to release if a ransom demand is not met. Data stolen in recent attacks has included teaching resources, school trip information and the personal data of staff and students, including medical information. Attacks have forced schools to close entirely until systems can be restored from backups or re-installed.

Data breaches in schools lead to clear safeguarding risks for students, disrupted learning outcomes and financial exposure. Schools not taking appropriate steps to secure personal data may face sanctions or fines from the Information Commissioner's Office.

[1]https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021-education-annex

[2]https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

"Defence in depth"

NCSC and other bodies recommend a defence in depth approach. The emergence of the Cyber Essentials for Schools scheme provides a validation pathway for schools against a baseline of cyber security controls, but these approaches do not assess real-world resistance to attack. Baseline standards are extremely helpful, but once basic controls are in place it can be difficult to work out where additional investment or attention is needed.

Successful cyber-attacks typically involve chaining together a series of smaller focussed attacks to compromise IT (Information Technology) systems – these form an attack path. A criminal wanting to successfully attack an organisation, such as a school, has several challenges to overcome.

If they want to take control of a school computer, they need to somehow introduce malicious software to that computer. They might do this by sending malicious software by email, getting users to click on a link, or hosting their malicious software on a website that users might visit. They might also gain access by guessing user account passwords, or by using previously-stolen data to log in to user accounts. Once the criminal has access to an account or a laptop, they then may move through the network, exploiting vulnerabilities and gathering access rights before they complete their objective of installing malicious software which locks users out of their computers.

At each touch point in this chain of events towards system compromise, cyber security controls have the opportunity to interrupt the attack. For example, a school might have software which inspects incoming emails and quarantines malicious software sent in that way. Web filtering software might be in place which can examine downloads from websites for malicious software and block these. A configuration setting on a user's laptop might stop them from running any unauthorised software - such as the malicious software sent in by the criminal.

No single cyber security control is fool-proof - attackers are always looking for ways to bypass defences - but by putting in place many layers of defence, it becomes much more difficult for a criminal to successfully execute an attack. Think of layers of chicken wire, laid on top each other until the gaps are smaller.

Many of the cyber security controls which can be easily audited aim to prevent the initial compromise of a laptop or a user account. Understanding how well your defensive layers function together, however, means exploring the whole attack path through the many layers of defence, rather than focussing on the first introductory step.

Assessing defensive capability

Penetration testing is the process of assessing systems for vulnerabilities or weaknesses using the same techniques that a criminal attacker would use. When conducted by skilled professionals, penetration testing approaches are extremely effective at exploring attack paths and identifying weak points in defences which can be addressed to improve resilience.

We believe our educational institutions need a higher level of expert security guidance, informed by real-world attack simulation, if they are to achieve resilience.

Our Hypothesis

We believe schools and colleges would benefit from detailed technical assessment of their cyber security resilience posture via active real-world simulation, using penetration testing approaches.

To test this hypothesis, we partnered with a local Multi-Academy Trust (MAT) to see whether our services could provide useful input to their cyber security resilience programme. We wanted to see whether we could give real-world insights into how effective the school's controls were when tested against the tactics, techniques and procedures of real threat actors commonly targeting educational institutions.

Threat actor	Common technical objectives	Skills / Motivation / Resources
Criminal group	Ransomware Extortion Double Extortion etc.	**Skills** – moderate to high **Motivations** – financial gain **Resources** – moderately resourced financially, multiple operatives, access to commodity tooling
Internal, such as a student	Unauthorised access to systems and data.	**Skills** – Low to moderate **Motivations** – Entertainment, kudos, learning opportunity, academic advantage **Resource** – limited

The MAT we worked with for our pilot project included secondary and specialist schools and therefore faced a set of challenges reflecting the wider education sector.

We chose a specialist school within the MAT as the environment for our initial pilot. This was a specialist college focusing on modern engineering and cyber security qualifications, running from Year 10 through to sixth form. Students that attend have a natural curiosity for cyber security topics, and the technical stakeholders involved have a mature awareness of cyber security risk and threats, making this an ideal setting for us to collaborate.

The Pilot Project

We worked closely with the MAT and school leadership teams to understand their key concerns and the cyber security questions they most wanted answers to:

- How robust were the configuration settings applied to staff and student laptops and how effective would they be at preventing infection by malicious software during a cyber attack?
- How good the controls were at preventing unauthorised access to data if a breach occurred?
- Did the security controls designed to protect staff data areas from student accounts function as they expected?
- Once a computer is compromised, how can a criminal find and exploit further vulnerabilities to take control of the network and then install ransomware or similar malicious software?

To address these questions, we used a scenario-based penetration testing methodology. Working with the MAT and school technical teams, we used our expertise and experience to emulate the criminals targeting schools - exploring potential attack paths and identifying control gaps and security weaknesses.

Assessing these scenarios in an end-to-end manner in some settings could mean starting from an external position without any knowledge of the school, but this can be costly and inefficient. To ensure the best value in our offering, we focussed on the assumption that a staff or student account had already been compromised by an adversary – either via the theft of a username and password or via the introduction of malicious software to a laptop. Given the prevalence of breaches experienced by educational institutions, this is a reasonable starting assumption which allows much greater efficiency in exploration of the impact.

The Delivery

Collaborating with the MAT and school leadership teams, we were able to perform a comprehensive simulation of a real-world attack.

During the assessment, we identified multiple weaknesses and vulnerabilities, which could be demonstrably exploited.

- The school we worked with had followed best practice advice closely when implementing their device hardening standards for staff and student laptops, demonstrating a good level of maturity in these controls. Using tactics which emulated the criminals, however, we were able to identify several gaps in these implementations and demonstrate how these gaps could allow the introduction of malicious software and ransomware.
- We identified weaknesses in the controls separating different data areas which could mean that a compromise of a staff or student device would lead to access to wider, and more sensitive, network resources.
- We identified susceptibility to network protocol attacks inside the school network which could lead to account password theft.
- We identified the extent to which the school was potentially exposed to account password theft due to the adoption of weak passwords, and the way in which the school's use of cloud services extended the potential attack surface area for this type of attack outside the network perimeter. This was compounded by the inability of the school to enforce multi-factor authentication for student accounts.
- We identified several data storage and data handling weaknesses inside the network which could, in the event of an incident, exacerbate the impact of a breach or further an attack.

For each vulnerability and weakness identified during the attack, we provided the school with targeted and prioritised remediation advice which they could implement to improve overall resilience.

The Outcomes

The school we worked with during this pilot had a strong understanding of their threat environment and their cyber security challenges, but they still benefitted from the external support and guidance provided by our assessment.

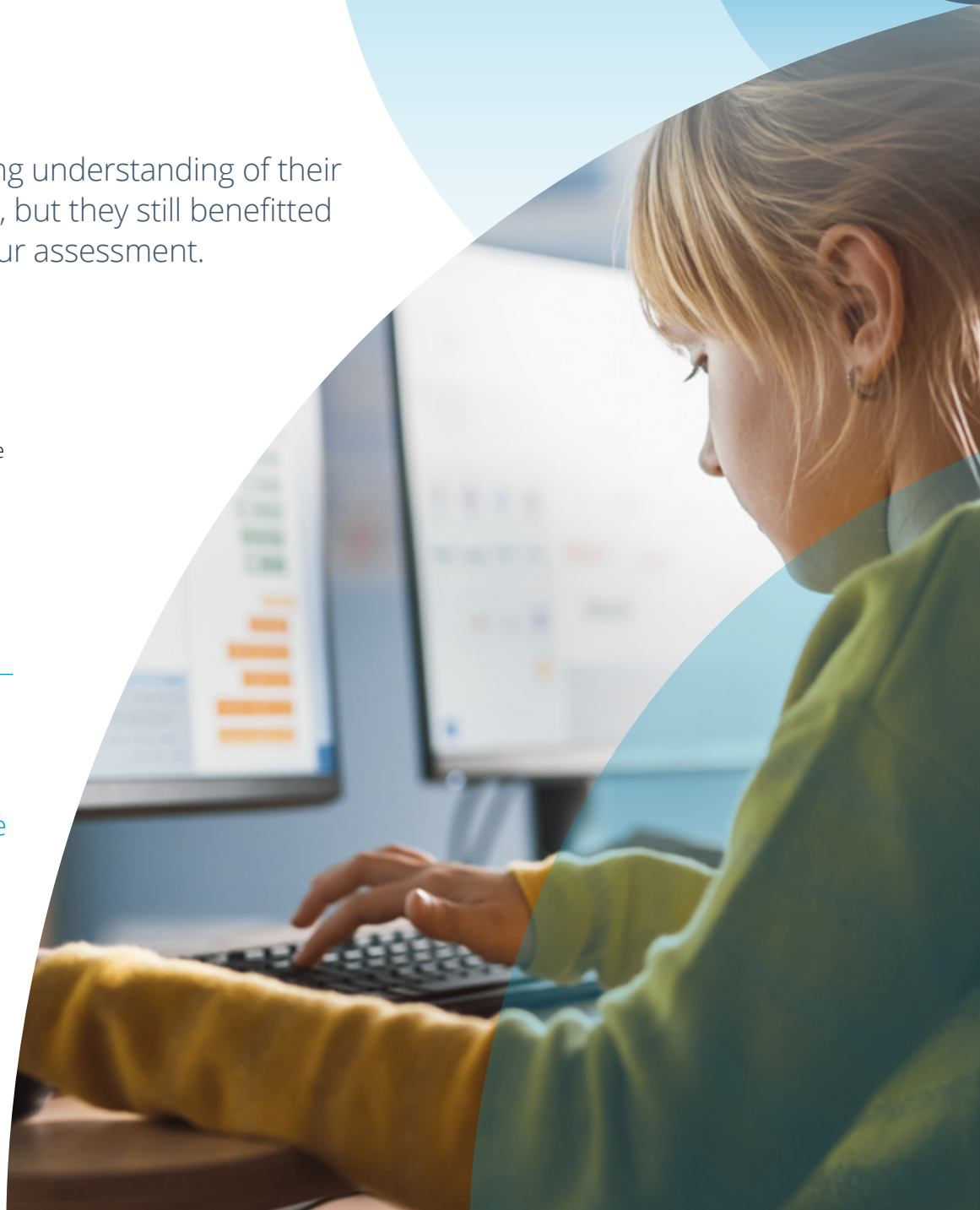
As we suspected, even a school with a mature approach to cyber security needs their controls and assumptions challenged by real-world simulations to achieve cyber security resilience.

The collaboration was effective at testing implementation decisions made by the school to support learning outcomes, and our advice was helpful in focussing future security improvements.

The pilot sought to benchmark the effectiveness of security controls and how they could assist internal teams with the day-to-day management of the network. The technical point of contact for the school was an advocate of this approach as the outcomes allowed him to benchmark the effectiveness of their implementation:

> We've already had a re-think on this as a real positive from the pilot project - previously we had looked at a range of tools to assess effectiveness but had probably been too narrow in our choice and too trusting of the results. By expanding this out we have been able to identify a number of software tools aren't reporting as accurately as we hoped.

Expert-led, real-world attack simulations represent a next step in building cyber security resilience within our educational institutions. Enacted by qualified and accredited technical assurance providers, these exercises have the potential to provide real value for schools in preventing data breaches and focussing cyber security budgets in the areas which provide the best return on investment.



Cyberis

Unit E, The Courtyard, Tewkesbury Business Park,
Tewkesbury, Gloucestershire, GL20 8GD
T: +44 1684 353514 E: info@cyberis.com W: cyberis.com