Cyberis

The Case for Real-World Attack Simulation in Schools:

Technical Briefing Paper

Technical Background

Cyber-attacks against educational institutions are on the rise.

Our educational institutions have rapidly innovated in response to the COVID-19 pandemic and the requirement to provide distant learning solutions to students and staff. These requirements have also demonstrated that schools have a unique problem when it comes to cyber security.

The adoption of cloud-based platforms has pushed the traditional external boundary within the reach of external attackers. This presents attackers with a route to potentially compromise these services which schools just are not equipped to deal with. In many ways, schools cannot enforce some of the common security controls found in commercial and government deployments due to user requirements and access to devices. Education cannot always take advantage of security controls for logistical reasons.

Governors and school leadership first need to understand the problem from both a technical and a deployment perspective if they are to be able to make informed decisions about how to secure their establishments and where the boundaries of those responsibilities lie. There is guidance available, but the learning curve is steep. The pressure to provide ubiquitous access to learning resources means that more of the establishment is extended beyond the school gates and into the digital realm. Leadership may not be aware of some of the potential challenges associated with cloud-centric models and therefore are solely reliant on the internal capabilities of internal personnel. As trusts, new guidelines related to funding requirements clearly define an understanding of cyber risks as a condition of receiving money from the public purse.

Whilst there is some support guidance about best practice for deployment, the responsibility relies on the establishment to understand these risks with limited options for measurement and assurance of these controls. NCSC (National Cyber Security Centre) has a dedicated section for education[1] on their website which gives schools access to planning resources, best practices and engagement tools that can be used to gain some level of understanding. However, the same challenge is still present; establishments require some level of internal technical capability to first implement and then to understand the outcomes of using these resources.

In other government and commercial sectors there is a strong culture of cyber assurance services that organisations can take advantage of to gain an understanding of the security posture. The CHECK[2] scheme is an example whereby establishments undergo simulated attacks looking for vulnerabilities and exploitation routes. This then allows an organisation to understand the security posture and plan to remediate or reconfigure the environment to mitigate these attack routes. As the CHECK scheme is operated via government channels, personnel delivering this assurance must meet stringent requirements for delivering such testing. With the emergence of Cyber Essentials for Schools, the trend is to provide verification certification that allow the measurement of several key cyber security controls; however, these approaches do not fully frame the risk from a criminal attack, either externally or with internal access. Whilst Cyber Essentials for Schools is a clear step forwards, it does not provide schools with adequate cyber security assurance alone; more work is needed to provide the robust security expected.

Our initial appraisal of the market demonstrated that there are no controls related to how establishments can tender third-party services. Any third-party can currently perform security assessments for educational establishments without the need to demonstrate any level of proficiency or experience via for example, accredited government schemes. The obvious risk is that providers expose the organisation to greater risk through mishandling data or that important technical gaps are not fully reviewed, creating a false sense of security.

[1]https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools
[2]https://www.ncsc.gov.uk/information/check-penetration-testing

Challenges for Schools

Education establishments face unique cyber security challenges that are not easily solved.

Controlling access to content and features is a key requirement for serving the needs of students, but it is often difficult to implement the kind of controls that many businesses take for granted.

On top of that, schools face challenges in budget allocation, trying to organise complex supply chains with several different integration levels, and managing security with limited internal resources

Practical Challenges When Implementing Controls

Regardless of the organisation type, user accounts and credentials are always a point of consideration for the IT (Information Technology) department, and often a target for attackers. Attackers who gain access to user accounts have access to privileges that the account holds. In assurance practices this is referred to as 'account context.'

Multi-factor authentication (MFA) is widely considered an effective tool in reducing the attack surface of an organisation because the use of weak or predictable passwords is so common.

Cloud deployment – something which has been essential for many schools to facilitate remote working during the pandemic - puts user accounts within easy reach of external attackers. It is very difficult, however, for schools to adopt MFA with student accounts, because of the practical difficulties around providing and managing a secondary authentication factor. Do all students have phones? Can a school manage and maintain a pool of physical authentication tokens? Does the school have the resources and capability to manage secondary authentication factors?

Whilst it is logistically difficult to implement those types of controls for the student group, applying MFA to staff accounts should be achievable and a goal. An adversary gaining access to an account in the context of a staff member could have serious ramifications, not just for the integrity of the data that they have access to but also in terms of compliance with data protection legislation.

A staff account will inevitably have access to student records with all the responsibilities of controlling how this data is accessed. It is far easier to implement MFA associated with staff accounts but support for these initiatives must come from the senior leadership.

When assessing cyber security risk, schools also need to consider the separation of staff accounts and student accounts, and the controls that are in place to protect staff areas from student access. If student accounts are inherently weaker than staff accounts (which will often be the case), then an attacker will much more easily be able to achieve access to a school within a student account context. If separation controls between student access and staff access are weak, or poorly-implemented, this could lead to an attacker with a student account context gaining access to systems and data that should be restricted to staff only.

The risks of reduced controls are acknowledged by network managers when asked about the freedom to implement changes and the barriers faced in the role:

"(I have) Full scope to implement change based on budget and potentially perceived barriers if any of the requirements are seen to potentially impact on learning. MFA would be a good example of this with a significant challenge seen by end users not having or wishing to use techniques such as SMS for authentication. Investment is made as required and would compete with other organisational requirements."

Controls implemented need to balance usability and security, and if a control such as MFA is seen to impede teaching and learning there is resistance to change. Teaching day to day is schedule and results-driven and so any control that slows down that momentum is inevitably going to be challenged as a value proposition.

Shortages of Dedicated Expertise

Training technical staff is not just an issue schools face; there is a global shortage of qualified IT professionals, and the available workforce reduces even more when looking at more specific roles such as cloud or cyber security specialists.

In-house capability is a challenge, and it is rare to have onsite personnel with specific knowledge in security domains. There is no doubt that schools want support and to gain a level of understanding about the gaps.

In many ways, schools are playing catchup and the problem is not just about investment of recent technology, it is about how deployment has changed.

The pandemic forced schools down the route of embedding cloud technology but a lack of understanding of the implications of such decisions can leave schools open. Speaking to a deputy head about the technology solutions that had been implemented with remote learning in mind:

"We have used Teams since it launched and prior to the organisation opening (pre-build phase) so were primed for remote learning from the off. The risks are, as always, people. This is in terms of password security and habits. In addition, 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. For example, we figured out early on those students could create teams of their own (a huge safeguarding risk), so we have our tenant configured so that you have to be a member of a specific group in order to be able to create new Teams. Again, not all schools will know how to or think to do this."

Budgeting

Our research has shown that there are fragments of information about what 'best practice' looks like when considering schools and so a mechanism for external validation could allow schools to measure where they are against a defined baseline. However, investment in cyber security is not seen as a priority in terms of budget according to executive leadership,

"I think a standard benchmarking process would be great, but schools' budgets are so tight that it worries me that many schools won't be able to meet standards expected."

Budget drives everything and so schools continue to build learning objectives on a foundation of technology, but the assurance around the state of the deployments is not sought. The NCSC have released alerts[3] related to the ransomware threat with an expectation that this will only continue.

The Academy Trust Handbook[4] defines priorities based on "must" and "should" and are conditions of the Academy funding agreement. This handbook now states that schools should have an awareness of the cyber security posture as a condition of budget with the responsibility for understanding this problem residing with the Academy.

"Academy trusts must also be aware of the risk of cybercrime, put in place proportionate controls and take appropriate action where a cyber security incident has occurred."

It is left to Academies to define what those proportionate controls are and what appropriate action looks like. Given the difficulties in budget allocation for controls, and the skills shortages facing Academies, external assistance is required to improve resilience.

The Academy Trust Handbook 2021 also underlines the impact that ransomware attacks can have on Academies,

"The final area to emphasise is cyber security. Many of you will be aware of the increasing number of cyber-attacks involving ransomware which are affecting the education sector and others. I know that these events can have devastating effects on organisations and individuals, and the Department continues to work with crime prevention agencies to help trusts protect themselves. The handbook highlights the National Crime Agency's advice not to pay ransoms, and to approach us if your trust finds itself in the very difficult position of contemplating such a payment."

When it comes to ransomware, prevention is always better than a cure from a budgetary point of view – the costs of recovery can be astronomical.

[3]https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector
[4]https://www.gov.uk/guidance/academy-trust-handbook

An Unmet Need

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 involving chaining together a series of smaller focussed attacks to compromise IT systems – these form an attack path.

Many of the cyber security controls which can be easily audited aim to prevent an account or laptop becoming compromised in the first place. Understanding how your defensive layers function together, however, means exploring the whole attack path. Penetration testing approaches are extremely effective at exploring these attack paths and identifying weak points 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. We also believe this is a need which is not currently being met.

Our Hypothesis

We believe schools and colleges would benefit from an adversary-led approach towards assessing their cyber security resilience posture via active real-world simulation, using penetration testing approaches.

Introducing real-world simulation of cyber-attacks to a school environment will allow us to identify which controls work well, and which need enhancement, and to provide feedback to schools and academies which educate them about their cyber security resilience posture and provide them with an actionable way forward when focussing their cyber security spend and investment. By focussing on realistic attack paths, and emulating common threat actors, we will be able to provide advice which is both pragmatic and reasonable.

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

Our pilot worked alongside the MAT leadership to devise and deliver an appropriate assurance service. The Deputy Head and Cyber Lead for the school was involved in the project to provide an insight and overview of technology that is implemented and how this is used day-to-day for the delivery of the curriculum.

The technical point of contact was a third-party services provider to the MAT and was involved in supporting the overall delivery and reviewing any findings from our testing delivery. The project benefited from the perspective of the MAT leadership in providing the executive viewpoint, the educational perspective through staff that are tasked with curriculum delivery and the technical management overview that allows the school to plan and deploy technological solutions.

The executive stakeholders have a clear view of the overall challenges that MATs face when looking at standardisation across the members within a trust and accept that it is often difficult for the MAT to fully understand the security implications:

"The Trustees have no formal IT review process, though the SLA for IT services for the Trust is reviewed annually, and review of security is a key remit of the IT services."

It was good to see that a review of the security services is part of the service level agreement although how this is effectively measured is unclear. When asked how well they felt that cyber security challenges are understood in the sector, they summed up their feelings in one word: "Inconsistently."

The output of the stakeholder meetings determined that a practical approach to cyber security assurance would be beneficial, and that the school had implemented some security controls which could be tested in line with a standard assurance model commonly found in other sectors such as the commercial and government spaces.

Outcomes, and value for money, are very important for schools, and so we were keen to ensure that the output of our cyber security assurance testing could be leveraged into actionable advice. Actionable advice is key for schools to formulate development plans that support an adequate cyber security baseline and also to demonstrate clear business cases for processes changes and additional funding.

When asked how well, from an education perspective, cyber security challenges are understood it was outlined by the deputy head that getting the executive conversation correct is vital:

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

The key factors driving our project were based on the following observations:

- Whilst the ramifications for disruption are significant and the current narrative is orientated to ransomware attacks, unauthorised access to school data (pupil details, staff details) is also a considerable concern.
- Cloud-based platform adoption has expediated and is the only feasible way an academy can facilitate platforms that support education in the future.
- Official bodies such as NCSC provide practical advice to educational establishments, but the implementation of this advice can be more difficult if the academy lacks support. Validation of these controls can also be a challenge for education environments.
- The emergence of a market that focuses on cyber security delivery within the education sector is welcomed, but this needs to be regulated and controlled. Providers of assurance services will need to demonstrate that they have suitable controls in place to safely provide a level of assurance and data handling when dealing with the sensitive data that naturally resides within a school.

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 was hardening applied to staff and student laptops and how effective would it be at preventing infection by malware?
- How good were controls were at preventing unauthorised access to data if a breach occurred?
- Did segregation controls designed to protect staff data areas from student accounts function as they expected?
- What privilege escalation routes might an attacker be able to use to install ransomware into the school systems?

To address these questions, we adopted a scenario-based penetration testing methodology. Working with the MAT and school technical teams, we used our expertise and experience to emulate the threat actors 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 zero-knowledge position, 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 credential theft or via a phishing attack. Given the prevalence of breaches experienced by educational institutions, this is a reasonable starting assumption which allows much greater efficiency in exploration.

Delivery

Collaborating with the MAT and school leadership teams, we were able to perform a comprehensive simulation of a real-world attack. We were able to explore elements such as the ability for an attacker to gain access to a public building, access rights of staff and students and the impact should an attacker successfully identify a route to compromise.

Following a successful infiltration, an adversary will commonly attempt to probe internal systems and networks to identify valuable sources of data, credentials, and trust relationships, which would allow onward access to other systems and weaknesses that can be exploited to gain further access.

To determine the risk faced should a low-level account compromise occur, Cyberis delivered an end-to-end scenario-based penetration test. This also served to address concerns around insider threats and the wider network exposure.

The simulation assessed stages across the whole attack chain, ensuring the assessment was holistic.

Target Analysis

- Identify target hosts
- Identify available services
- Assess functionality of each host and its role

Vulnerability Identification

- Perform automated vulnerability scanning
- Manually review available services for vulnerabilities
- Manually review available services for configuration weaknesses

Exploitation and Further Access

- Exploit issues identified
- Determine impact to the business of these vulnerabilities
- Determine what further data assets could be at risk from this point

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

Gaps in control implementation	The school had followed best practice advice closely when implementing their device hardening standards for staff and student laptops, demonstrating a proficient level of maturity in these controls. Using adversary simulation tactics, however, we were able to identify several gaps in these implementations and demonstrate how these gaps could allow the introduction of malware and ransomware.
Weak segregation	We identified weaknesses in segregation controls which could mean that a compromise of a staff or student device would lead to access to wider, and more sensitive, network resources and data.
Legacy protocol attacks	We identified susceptibility to network protocol attacks inside the network which could lead to account password theft.
Credential 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.
Data handling weaknesses	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 collaborative approach adopted during the assessment meant that we were able to brief and educate our onsite technical contacts about the tactics used by adversaries when operating within their networks. We are often fond of the adage that "offense informs defence" – ensuring that our contacts gain an understanding of how attackers operate is key to realising the benefit of these types of exercises.

As we were able to demonstrate the vulnerabilities and weaknesses we identified, we were able to clearly highlight the impact of these weaknesses in terms of the wider network and school data repositories. Several routes into sensitive areas of the network were found and this is a common theme in most penetration tests, regardless of sector.

We were able to demonstrate routes to gaining access over the environment with full administrative rights. Once an attacker gains these rights, there are no other barriers to data access internally as the attacker holds the ability to access any account. Holding these levels of privilege allow an attacker to deploy software across the estate, and this is where ransomware attacks are debilitating. Recovering from such incidents has a serious impact on the support teams and directly impacts learning.

Outcomes

The school 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 cyber security approach 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 measure 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