cyberlab

Defending Education: Navigating Cyber Security Challenges

Top Cyber Threats to the Education Sector

cyberlab

On-Demand Webinar

Defending Education: Navigating Cyber Security Challenges

Supported by

SOPHOS FORESCOUT LOGPOINT mimecast SecurEnvoy

Join a panel of industry experts as they explore the unique risks educational institutions face and provide actionable strategies for protection. This session is tailored to equip IT leaders, administrators, and educators with the tools to enhance their cyber security posture within budget constraints.

In this webinar we cover:

- The top cyber threats in education, including ransomware and phishing, and how to combat them.
- Best practices for managing and securing diverse networks of devices, from laptops to IoT.
- The role of AI and automation in detecting and mitigating threats in real time.

Visit Cyberlab.co.uk or scan QR Code

Introduction

Cyber security is a crucial concern for education institutions, largely due to their unique, open network environments. Academic institutions tend to operate on shared networks accessed by numerous users from diverse devices such as laptops, tablets and smartphones, as well as from a variety of locations.

Additionally, the growth of remote learning and cloud-based services has expanded the attack surface, increasing the challenge of managing cyber security across campuses. This communication, learning and working environment makes academic institutions particularly vulnerable to cyber attacks and threats including phishing scams, ransomware, Distributed Denial of Service (DDoS) attacks and data breaches.

This whitepaper explores the evolving cyber threat landscape for the education sector, identifies key security challenges, and outlines effective strategies to mitigate risks.

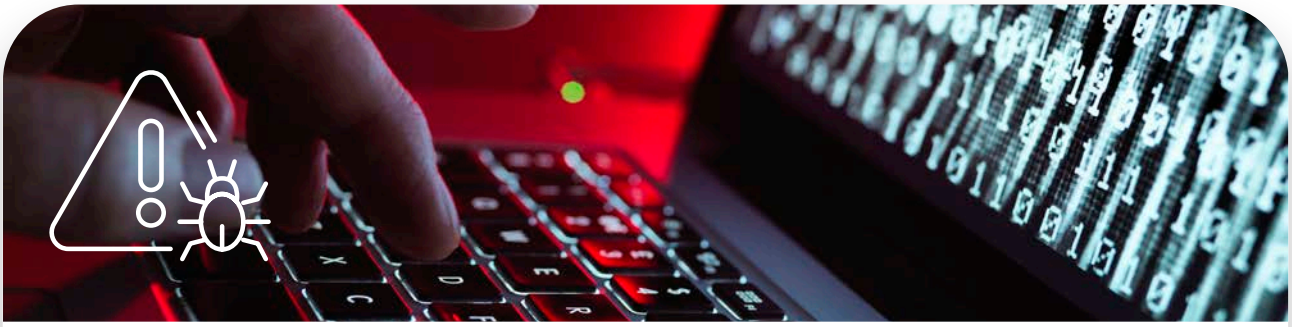
Contents

Understanding the Threat Landscape

The Most Prevalent Threats

The decentralised structures, large user bases and diversity of data stored by education institutions all make them attractive targets for malicious threat actors.

Further education institutions in particular tend to operate large networks to support collaboration and research, which are prone to vulnerabilities and exploitable gaps in infrastructure. By their very nature, they store intellectual property, cutting-edge research information and financial and personal data.



Ransomware – the number one threat

Ransomware remains one of the most significant threats across all sectors, with education being no exception. According to **The Sophos State of Ransomware Report 2024**, 63% of organisations are likely to fall victim to this threat.

Particularly worrying threat modes are evolving, for example Living Off the Land (LotL) attacks which exploit legitimate tools and software already present in the target's environment to conduct malicious activities, making detection very challenging for security teams.

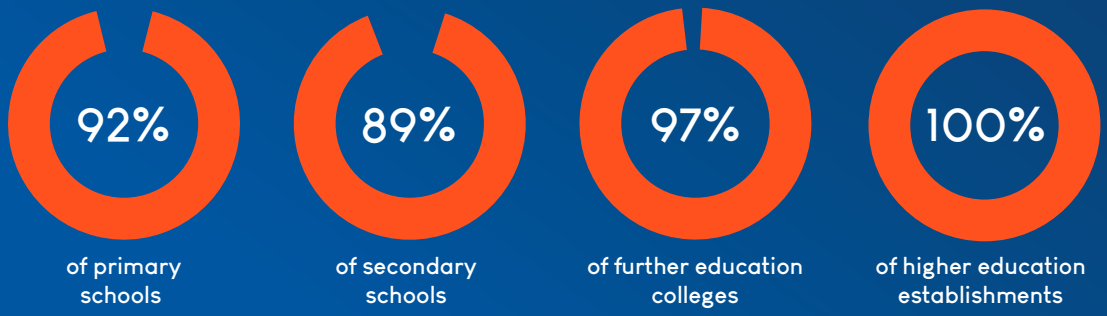
These tactics enable attackers to "blend in" with normal network activity to bypass traditional security measures, using tools like Remote Desktop Protocol (RDP) and Powershell to attack organisations rather than the more usual file- and malware-based vectors. The challenge for security teams is distinguishing between legitimate and hostile use of these tools.

Cyber Security Guide for the Education Sector

Find out more

Phishing

Research published in the **UK Government Cyber Security Breaches Survey 2024** shows that educational institutions at all levels report phishing as the dominant cause of attacks:



These statistics compare with 84% of businesses reporting phishing attacks.

Payloadless attacks

A further threat facing education establishments is impersonation via social engineering, with use of brand impersonation, QR codes and payloadless attacks preceding a phishing attack.

To network users, these forms of attack are often very convincing, as rather than carrying a link or malware-infected attachment, they arrive in the form of an urgent request to take a corrective action such as transferring funds ahead of an expiring deadline.

Expanding Attack Surfaces: Mitigating Threats from Diverse Devices

Increased attack surface

Educational institutions face unique challenges in securing their networks due to their inherently large and diverse attack surfaces. These environments often support hundreds or thousands of students and staff, each accessing the network from a wide variety of devices including laptops, tablets, phones and IoT devices. Additionally, the threats that institutions face are incrementally more difficult to control where educational institutions operate a BYOD policy.

This increases the attack surface, making it harder to monitor and secure endpoints. With as many as 50% of endpoints being unmanaged, IT managers don't always know what devices are connecting to the network or what their status and function is.

Decentralised campus networks

Decentralised campus networks are becoming increasingly common in educational institutions. The merging of individual institutions into larger organisations often results in networks comprising hundreds of vendors and operating systems. This diversity can lead to inconsistent defences across the organisation, creating significant challenges for maintaining a robust security posture.

Data theft, espionage and extortion

These complex, distributed network set-ups, with large numbers of disparate connected devices and users, along with the potentially rich pickings in the shape of intellectual property and personal data, makes educational establishments an attractive target for malicious actors.

According to researchers at **Forescout's Vedere Labs** which track hundreds of these players, 10% are specifically targeting education, many state-sponsored Chinese, Russian, North Korean or Iranian attackers target education for the purposes of espionage, financial gain or ransomware, usually gaining access via network devices.

Adopting a zero-trust approach

One solution is to adopt a **zero-trust architecture**. This approach assumes no user or device is trusted by default, even if they are already inside the network. This approach is especially crucial for higher education institutions, given their vast, open networks, with users accessing resources from diverse locations and devices.

With this model, access control is based on trust levels. Devices attempting to sign into the network are subject to checks to:

- Assess whether they have the correct credentials
- Ensure they have the right agents installed
- Ensure they have endpoint protection installed and running
- Be assigned to the right VLAN and firewall groups based on the ID of the owner

In the case of non-IT or IoT devices, authentication protocols can be run and certificates added. Only once security status is assessed, will devices be authorised if recognised, or quarantined if identified as rogue of unknown.

BYOD challenges

The widespread adoption of Bring Your Own Device (BYOD) policies introduces significant challenges for educational institutions. Managing the variety of devices connecting to networks makes it difficult to track which individuals have access and where sensitive data resides.

Phishing attacks for exfiltration of data are a constant risk and require the use of logs, network defence and response (NDR) solutions and user and entity behaviour analytics (UEBA) solutions which incorporate machine learning to look for anomalous behaviour.

The key is not necessarily to deploy the technology in the first instance, but to be able to do so at scale, for example to manage or allow 15,000, 20,000 even 30,000 or more devices on the network.

Integrating security information and event management (SIEM) systems with existing infrastructure is another critical step. This enables real-time threat detection, response, and remediation—forming a cornerstone of any robust security posture in education.

Who is who and what is what?

Understanding who and what is connected to a network, how they accessed it, and what they are doing is critical for maintaining security in educational environments. Ensuring proper identification and control is essential as institutions manage a growing variety of users and devices.

Multifactor authentication (MFA) solutions, combined with policy-based and device-type authentication controls, play a vital role in achieving this. Educational institutions are increasingly moving away from smartphone-based authentication, prompting discussions about the best alternatives, such as hardware or software tokens, and the criteria for granting access to users, machines, or devices.

However, not all MFA solutions provide equal security, and some can be bypassed. Choosing a robust and reliable solution is critical to safeguarding networks and ensuring the integrity of access controls.

How AI is Reshaping Cyber Security

Today, cyber criminals are using **Artificial Intelligence (AI)** to make cyber attacks more effective, for example by making emails look more authentic.

AI for better spelling and grammar

Often, a sign of a phishing email may be an obvious spelling mistake or an odd-sounding non-native phrase or sentence. AI can be used to correct spelling and grammar, localise language and introduce more colloquial phrases, making it seem more human and believable.

However, AI can also be used to protect against phishing emails by, for example, checking the brand content and sending email address of a sender against domains owned by the supposed sender, without there having to be a "rule" in place to tell it to do so.

Deconstructing and mitigating payloadless attacks

AI can take a payloadless attack email and deconstruct it, holding it at the gateway whilst alerting the user or manager. Meanwhile, the AI will:

- Analyse the email's content
- Look for a match between the email address and domain
- Identify any fake login pages
- Test any colloquialisms
- Verify requests for bank account details, or other sensitive information.

Combining AI with human intelligence

Phishing emails often originate from non-native English speakers, with AI commonly used by attackers to localise language and improve the plausibility of their messages. Detecting these threats requires advanced tools capable of recognising patterns and similarities in attack methods, which tend to remain consistent.

Yet no single AI software can both spot all attacks and contain them. Technology alone isn't enough. For this reason, the Sophos managed detection and response (MDR) service uses human experts to improve in the analysis of categories of risk.

AI offers several key advantages when paired with human intelligence:

- **Filtering Noise:** Be combined with a human expert element to provide a far more effective solution than either alone. For example, AI can sift through background noise to identify an attack event, then put it in front of a human expert for a final 'sanity check' and decision.
- **Identifying Patterns:** Group cyber attack types and events and spot repeat instances. Cyber agents move from machine to machine, leaving breadcrumb trail as they go. A small event will create multiple alerts, so AI can detect events and then put them in front of human experts for action.
- **Assessing Training Effectiveness:** AI can evaluate groups of trained users, quickly identifying weaknesses or gaps in understanding within seconds, enabling targeted improvements in training programs.

AI combined with machine learning for fast remediation

The combination of AI and machine learning (ML) are critical elements of a converged SIEM platform, and as an example Logpoint's solution incorporates:

1. SOAR (Security Orchestration and Response/ Remediation) based on "playbooks" (process flow charts) which make decisions from an AI and ML perspective aligned with a specific threat type - for example phishing - by isolating a user/email or a port on a firewall.
2. MDR using AI to baseline normal network behaviours and provide telemetry on unexpected behaviour in real time – like supercharged UEBA technology.

For example, in a phishing attack, a potential threat detected by a tool like Mimecast appears as an alert in the SIEM platform. The threat appears in the SIEM platform as an alert, kicking off a SOAR playbook, which then reaches out to an integrated threat platform with a risk score attached. The potential threat is then triaged and presented to a human analyst. The process is all automated and can involve human interaction according to requirement, customised to established best practice.

This AI-enabled process can take just a few minutes, compared to the normal time without AI, which could potentially be hours.

Enhancing Microsoft Security: Best Practices for Schools and Universities

Avoid single-technology solutions

A key best-practice approach for cyber security is to avoid relying on a single-technology solution. Putting all security measures in the same system creates a vulnerability.

For instance, if Microsoft email goes down, it can take the built-in security solution with it, creating a double headache for an IT Manager. To mitigate this, running two complementary systems side by side in a high-availability array is essential. This approach ensures that if one system goes offline, the other can maintain security and operational continuity.

Enhance and complement - don't replace

Where educational institutions already have some forms of cyber security in place, the ideal solution is to complement them and cover potential weaknesses. In the case of email security, solutions like Mimecast not only strengthen Microsoft's email security but also provide critical backup capabilities, ensuring continuity if email services experience downtime.

It provides threat intelligence about what people do with their email in the real world, and complements Microsoft's email solution by enhancing – not replacing - its security capability to deliver the best of both worlds.

Avoid overly complex security solutions

At the same time, it is important to avoid too much complexity. Trying to manage multiple, off the shelf security products to solve multiple problems is not the ideal solution. Many educational institutions do this and not only end up paying more but also juggling multiple support teams, subscriptions and renewal dates, thereby presenting a sizeable management overhead. CyberLab simplifies this process by acting as a centralised point of management and support, unifying disparate tools into a cohesive security ecosystem.

According to Mimecast's Email Security Risk Assessment, for every **1 million emails** delivered by Microsoft's Advanced Security, over **87,000 were bad or unwanted**.

Create intelligence trust with tight technology integrations

Building an intelligent trust model requires seamless integration between security technologies. For example, Forescout's partnership with Microsoft enables tight integrations with specialist email security products to enhance overall network security.

As this model becomes more intelligent, it can help make decisions in real time about device permissions on the network and specify actions that should be taken.

Deploy MFA hardware and software solutions as an alternative to the Smartphone approach

Many institutions rely on on-premise servers and RDP connections, where enforcing multifactor authentication (MFA) is becoming a priority.

MFA tokens, such as those provided by SecurEnvoy, offer a practical alternative to smartphone-based authentication. These hardware or desktop solutions address the needs of users who either do not own smartphones or prefer not to use personal devices for authentication. This flexibility ensures strong security measures without reliance on smartphone apps, making it a more inclusive and adaptable option for educational institutions.

Request a free Security Posture Assessment

Understand your security risks and how to fix them.

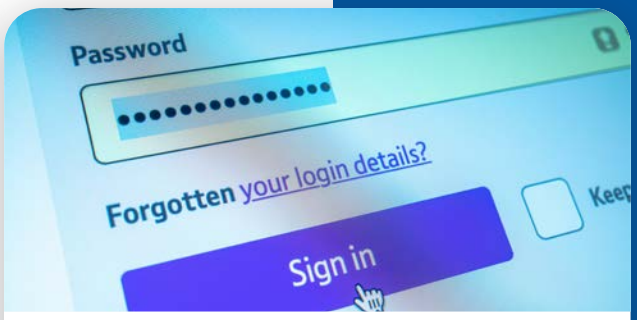
Find out more at **cyberlab.co.uk**

Detect, Protect, Support: Cyber Security Tips for Tight Budgets

With limited budgets and increasing cyber threats, educational institutions face unique challenges in protecting their networks and data. Success often depends on maximising existing resources, prioritising the most critical risks, and leveraging vendor expertise tailored to the education sector.

Make the most of existing resources

Leveraging existing investments is essential. For example, **Sophos integrates seamlessly with the Microsoft product suite**, utilising telemetry from each product to maximise value. This data is then analysed by Sophos security experts to detect early-stage signs of a cyber attack, enabling proactive responses.



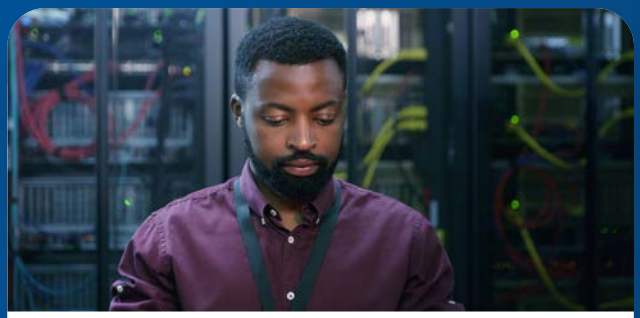
Focus on detecting attacks in early stages

The early stages of a cyber attack often leave subtle signs that can be identified with careful monitoring. Indicators such as unusual lateral movement within the network or privilege escalation often precede larger breaches. Detecting these early warning signs is critical to breaking the attack chain before significant damage occurs. By focusing on these early indicators, institutions can disrupt attacks at their onset and improve overall security outcomes.

Cyber Security for Education

Speak with an expert

In 97% of attacks, backups are targeted in the early stages



Protect backups

Cyber criminals frequently target backups early in their attacks. Sophos research reveals that backups are targeted in 97% of incidents, as compromising them increases the likelihood of ransom payments. The criminals' logic is that if they can get at backups, then it is more likely that organisations will pay out on ransom demands because the safety net provided by their backup solution has now gone.

Prioritise and weigh up risks

For budget-constrained institutions, prioritisation is key. Weigh the risks, learn what the threats are by reading industry case studies, and then select vendors on the basis of the expertise they can bring rather than just by their highly complex technology. Also, use vendors that have licensing packages and pricing models specially for education.

In Conclusion

To protect their valuable data and intellectual property, education institutions need a proactive, multi-layered cyber security strategy.

By tackling the specific challenges posed by decentralised networks and diverse user bases, academic institutions of all types can establish a robust defence against the ever-evolving landscape of cyber threats.

Request a free Security Posture Assessment

Understand your security risks and how to fix them.

Take the first step to improving your cyber security posture, looking at ten key areas you and your organisation should focus on, backed by NCSC guidance.

Claim your free 30-minute guided posture assessment with a CyberLab expert.

Cyberlab Protects 110+ Education Customers

Educational institutions count on us to defend their networks, protect sensitive information, and promote a secure learning environment.

Sheffield Hallam University

CITY UNIVERSITY OF LONDON EST 1894

SWC SOUTH WEST COLLEGE

About CyberLab

CyberLab is a specialist cyber security company that provides a wide range of security solutions and services.

Your one-stop cyber security advisor, the CyberLab team is equipped with the right technology, knowledge, and expertise to help businesses of all sizes, including large public sector organisations.

By leveraging world-class technology, decades of experience, and our vendor partnerships, we have helped to secure thousands of organisations across the UK.

Our unique Detect, Protect, Support approach makes us the perfect partner to review and reinforce your cyber security defences.

Speak With an Expert

hello@cyberlab.co.uk | cyberlab.co.uk

Awards and Accreditations

CREST

VA | PEN TEST

IASME CONSORTIUM

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

cyberlab

cyberlab.co.uk