Securing Higher Education Against Advanced Cyberthreats

MDR is the leading Managed Detection and Response service for the education sector

Higher education providers such as colleges and universities are a prime target for cybercriminals. Adversaries are increasingly attracted by the valuable and sensitive information they hold, and the opportunity to extort payments using ransomware and the threat of breach exposure.

As cyberthreats grow in both volume and complexity, many higher education providers are turning to the Managed Detection and Response (MDR) service for protection against advanced attacks that technology alone cannot prevent. This solution brief explores the cybersecurity challenges facing the sector and introduces MDR, a service supporting higher education today.

The Cybersecurity Challenge Facing Higher Education

Higher education is a major target for cyberthreats

Almost two-thirds (64%) of higher education providers were hit by ransomware in 2021. In comparison, across the education sector as a whole, 44% of organizations fell victim to an attack in 20201. This 45% rise over the course of a year demonstrates the rapid acceleration of the cyberthreat challenge facing the education sector.

More broadly, the majority of IT managers within higher education reported an increase in the volume (53%), perceived complexity (50%) and impact (50%) of cyberattacks over the last year. As cyber criminals continue to leverage automation and the 'malware-as-a-service' model in their attacks, these numbers are only set to increase.

64% hit by ransomware in 2021

53% report an increase in attack volume

50% report an increase in attack complexity

50% report an increase in the impact of cyberattacks

The impact of advanced cyberthreats on higher education is severe

A major cyber incident has very considerable financial and operational repercussions for higher education providers. In 2021, the average ransom paid by the sector was a crippling $905,000. While this includes a small number of very large payments, almost one quarter (24%) paid between $50,000 and $100,000. Furthermore, the average overall cost to remediate a ransomware attack came in at $1.42 million, with well over one third (39%) of the encrypted data remaining unrecovered after the incident.

Recovery costs are just part of the story. Nearly all (97%) higher education establishments hit by ransomware said the attack impacted their ability to operate, while 96% of those in the private sector said it caused them to lose business/ revenue. In both cases, these are the highest impact figures reported across all industry sectors. If IT systems go down, providers' ability to deliver teaching and learning is often severely inhibited, with major repercussions for students and staff.

Compounding the challenge, higher education reported the slowest ransomware recovery across all sectors with only 60% of victims fully recovered one month after the attack; 31% required 1-3 months to recover and 9% reported a recovery period of 3-6 months.

US$1.42M ransomware recovery cost

97% of attacks impacted ability to operate

96% of attacks resulted in lost business/ revenue (private sector only)

Higher education is struggling to keep pace with well-funded adversaries

The reality is that technology solutions alone cannot prevent every cyberattack. To avoid detection by cybersecurity solutions, malicious actors increasingly use legitimate IT tools, exploit stolen credentials and access permissions, and leverage unpatched vulnerabilities in their attacks. By emulating authorized users and taking advantage of weaknesses in an organization's defenses, malicious actors can avoid triggering automated detection technologies.

The only way to reliably detect and neutralize determined cyber attackers is with 24x7 eyes on glass delivered by expert operators who leverage diverse security alerts and real- time threat intelligence to identify and stop threats before the damage is done.

However, the complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organizations to successfully manage threat detection and response on their own. Illustrating this point, the average intruder dwell time in the education sector was **34 days**, more than double the 15-day cross- sector average.

Organizations across all sectors, including higher education, are struggling to keep pace with well-funded adversaries who are continuously innovating and industrializing their ability to evade defensive technologies.

MDR:
Securing Higher Education

As the cybersecurity challenge continues to grow, higher education providers are increasingly turning to an MDR service to help them stay ahead of today's advanced threats.

24/7/365 ransomware and breach prevention service

Managed Detection and Response (MDR) is a fully managed service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

Detect: Monitor your environment 24/7, collecting, contextualizing, and correlating security data from an Adaptive Cybersecurity Ecosystem and your existing cybersecurity investments to identify suspicious activities

Investigate: Expert human operators investigate potential incidents, leveraging deep education sector and threat expertise to hunt for signs of adversarial activities

Remediate: Analysts quickly remediate attacks across the broad range of your environment, before they turn into something more damaging such as ransomware or a wide scale data breach

Review: Comprehensive root cause analysis of incidents together with regular health checks and weekly and monthly reporting enable you to improve security posture and prevent future recurrence

With an average time to detect, investigate and remediate of just 38 minutes, MDR is more than 5 times quicker than even the fastest in-house security operations team.

With MDR, you benefit from A team of over 500 security operations specialists who provide expertise across all elements of the detection and response cycle, from threat hunting and neutralization to malware engineering and security automation.

A service designed around you

We understand that each higher education provider is different with their own existing security investments, IT/cybersecurity staff, and IT environment. MDR meets you where you are: you choose the level of support required, whether you want to be notified of threats so your team can take remedial action, contain threats on your behalf, or provide full incident response and root cause analysis. Our partners security specialists will work with you to identify the right approach for your organization.

Elevate your protection using your existing investments

Today's advanced threats can come from any direction, and adversaries often deploy multiple tools, tactics and procedures in the course of their attacks. MDR analysts detect and respond to attacks across your entire environment. We can use your:

- Endpoint telemetry to spot malicious activities and attack behaviours
- Firewall data to detect intrusion attempts and beaconing
- Network telemetry to identify rogue assets, unprotected devices, and novel attacks
- Email alerts to pinpoint initial entry into the network and attempts to steal access data
- Identity data to detect unauthorized network entry and attempts to escalate privileges
- Cloud alerts to indicate unauthorized network access and efforts to steal data

The more we see, the faster we act. By detecting and responding to advanced attacks using your existing security tools, MDR reduces cyber risk while increasing return on your security investments.

Next Steps

TO LEARN MORE ABOUT MDR AND THE SELECTED PARTNERS WE WORK WITH, SPEAK TO US TODAY

E: SOLUTIONS@IT-B.CO.UK | T: 01865 595510

itb