INDUSTRY BRIEF

THREATQUOTIENT™

ThreatQ for Education

Education covers a vast range of institutions, from primary and secondary school to community colleges, trade schools, and universities. Whether in-person or online, these institutions face similar challenges. From primary schools to higher education, they are vulnerable due to sensitive personal data, inadequate defenses, and extensive research. Many fall prey to phishing, ransomware attacks, and DDoS. To combat these threats, these organizations must arm themselves with the right knowledge and tools.

KEY CHALLENGES

RESOURCES

School systems of all sizes are under siege from cyberattacks, often due to limited cybersecurity resources, weak password policies, inconsistent multifactor authentication (MFA) and inadequate cybersecurity training. Budget constraints further exacerbate the problem, leaving many educational institutions vulnerable. Without essential cybersecurity measures, schools struggle to stay ahead of ever-evolving threats.

OUTDATED INFRASTRUCTURE

Outdated legacy systems and software are prime targets for threat actors. These systems manage transportation, attendance, grades, personal information, and more. Attackers know that institutions, crippled without their systems, are likely to cave to demands.

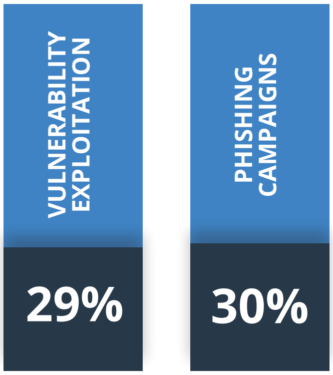
THREAT LANDSCAPE

Education systems simply can't afford disruptions, especially with so much of their operations being remote. This makes them prime targets for ransomware attacks, as they're likely to pay up. These attacks don't just mess with schedules—they hit students, teachers, faculty, and staff hard, both in terms of time and money.

INCREASING PROTECTION OF EDUCATION

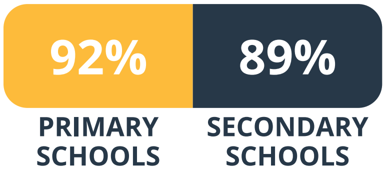
According to SWGfL, 75% of primary schools and 81% of secondary schools have implemented a cybersecurity policy.[2]

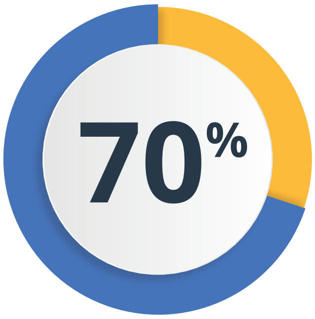
Many schools were found to have taken proactive measures to detect potential cybersecurity risks, including conducting audits, penetration tests,



IN 2023, K-12 SCHOOL ATTACKS[1]

IDENTIFIED A PHISHING ATTEMPT[2]



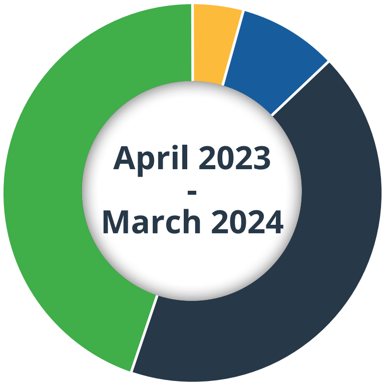


In higher education specifically, attacks were up 70 percent (68 in 2022 to 116 in 2023) compared to 2022.[3]

and investing in threat intelligence. Primary schools were observed to employ the least sophisticated approaches despite these efforts.

Investing in threat intelligence is key for these institutions to stay protected. Making sure that students and staff have the resources necessary to stay updated on policies and practices to stay safe.

KNOWN RANSOMWARE ATTACKS[4]



K-12 Education - 45%
Higher Education - 42%
Professional Education - 9%
Other - 4%

CREATING A LEADING THREAT INTELLIGENCE OPERATION

The ThreatQ Platform gives education providers the context and security they need to make better decisions, accelerate threat detection and response, and advance team collaboration and learning for continuous improvement. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with the ThreatQ open architecture.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** all sources of external & internal threat intel and vulnerability data in a central repository.
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets & vulnerabilities.
- **PRIORITIZE** what matters most for your environment.
- **PROACTIVELY HUNT** for malicious activity which may signal malicious activity, denial of service attacks, other disruptions and potential harm to customers, employees and constituents.
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status and security posture.
- **ACCELERATE ANALYSIS AND RESPONSE** to attacks through collaborative threat analysis that enables shared understanding and coordinated response.
- **AUTOMATING** threat detection and response.

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

[1] Infosecurity Magazine, https://www.infosecurity-magazine.com/news/exploitation-29-education-sector/

[2] SWGfL, https://swgfl.org.uk/magazine/new-data-reveals-impact-of-cyber-security-attacks-on-schools/#:~:text=Among%20these%20attacks%2C%20phishing%20continued,-schools%20identifying%20a%20phishing%20attempt.

[3] EdTech, https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows#:~:text=The%20grim%20statistics%20include%20a,2022%20to%20116%20in%202023).

[4] ThreatDown, https://www.threatdown.com/blog/alabama-state-department-of-education-stops-ransomware-attack-but-the-assault-on-us-education-continues/

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data.

ThreatQuotient's industry leading integration marketplace, data management, orchestration and automation capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

For more information, visit www.threatq.com.