The Growing Threat of Cyberattacks on Education

Educational institutions have become highly attractive targets for cybercriminals due to a confluence of factors. The vast quantities of sensitive data they handle, including personally identifiable information, financial records, and intellectual property, make them lucrative targets for data breaches and ransomware attacks. Moreover, the intricate IT infrastructures often found in these institutions, coupled with limited cybersecurity budgets, create opportunities for exploitation. The increasing prevalence of remote learning and Bring Your Own Device (BYOD) policies further complicates the security landscape.

Cybercriminals are motivated by the potential for financial gain through data extortion, sale of stolen information, or disruption of services. Ransomware has emerged as a particularly lucrative avenue, with attacks on educational institutions surging by 37% since 2023. The financial toll is substantial, with average recovery costs reaching $2.73 million per incident—a staggering 48% higher than the global average. The significant impact of data breaches on an institution's reputation and the public's trust underscores the urgent need for robust cybersecurity measures to protect these vital institutions.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.