ARANCIA

SAFEGUARDING HIGHER EDUCATION

NAVIGATING THE CYBERSECURITY THREAT LANDSCAPE

WHY CYBERCRIMINALS TARGET HIGHER EDUCATION INSTITUTIONS?

Data is the crown jewel of higher education institutions, making them prime targets for cybercriminals seeking to infiltrate their systems. Higher education institutions face escalating cybersecurity risks due to the sensitive nature of their operations and data. The increasing reliance on virtual platforms for classes, exams, and communication has amplified vulnerabilities, particularly as students and staff often connect through unprotected home networks. Key Drivers of cybersecurity threats in Higher Education include, **abundance of sensitive information, valuable research data,** and **lack of cyber preparedness.**

Recent reports, such as Educause's 2024 Higher Education Trend Watch and NREN's national cyber threat assessment, emphasize the urgency of addressing these challenges. With data security and privacy ranked as top priorities, institutions must adopt robust cybersecurity strategies to protect their data.

NREN CYBER ASSESSMENT

KEY CONCERNS:

- INCIDENT RESPONSE GAPS
- SKILL SHORTAGES
- AGING INFRASTRUCTURE

75% INCREASE IN HIGHER EDUCATION CYBERATTACKS YEAR OVER YEAR

A Deloitte report highlights that Canadian higher education institutions are facing mounting cybersecurity threats. The shift to virtual learning environments during the COVID-19 pandemic exacerbated these risks.

80% UNIVERSITIES HIT BY PHISHING ATTACKS

15% DATA BREACHES CAUSED BY RANSOMWARE

THE MOST COMMON CYBERSECURITY THREATS LEVERAGED AGAINST THE EDUCATION SECTOR

MALWARE ATTACKS

Malware attacks on higher education rose by over 30% in 2023, with cybercriminals targeting internal systems to bypass security.

RANSOMWARE

Ransomware severely impacts education organizations due to prolonged disruptions, financial costs, and long-term effects.

PHISHING ATTACKS

In the education sector, phishing scams may target student data, research data, or the credentials of employees.

DDoS ATTACKS

With educational institutions relying more heavily on more devices than ever, this also has rapidly expanded the opportunity for cyber criminals to carry out DDoS attacks.

INSIDER THREATS

Insider threats in education stem from students and employees with access to networks, systems, or data. Their deep knowledge of processes, policies, and locations makes them a significant risk.

ARANCIA

PRIME TARGETS FOR THREAT ACTORS

RESEARCH DATA

Intellectual property, especially in higher education and cutting-edge technology fields, is a lucrative target.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Student, staff, and alumni records, including financial details, are at constant risk of exploitation.

IMPACT OF SECURITY BREACHES

DISRUPTION OF ACADEMIC ACTIVITIES

Cyberattacks often force system outages, halting operations like admissions, grading, and research submissions.

REPUTATION DAMAGE

Loss of trust may result in decreased student enrolment and partnerships.

LEGAL AND FINANCIAL RAMIFICATIONS

Institutions face potential class action lawsuits and regulatory fines due to privacy violations, further straining resources.

STRATEGIC RECOMMENDATIONS

Continued Technical Security Assessments

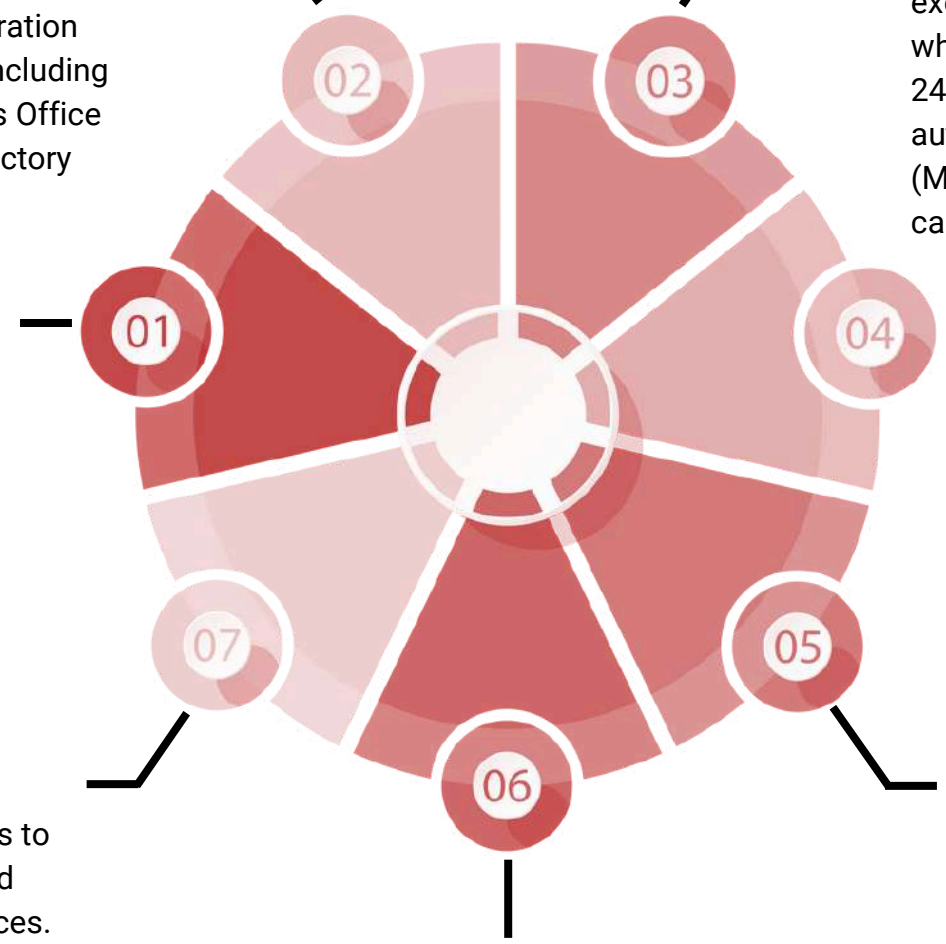
It's important to conduct Penetration Tests, Cloud Security reviews including collaboration platforms such as Office 365 or GCP, FW and Active Directory (AD) Security Reviews

Threat Detection & Response

Important to conduct a Threat Modelling exercise to understand all key security events which should be monitored in a centralized 24x7x365 days Managed SOC along with automated Managed Detection & Response (MDR) powered by AI Driven remediation capability.

Comprehensive Risk Assessments

Regular evaluations to identify vulnerabilities and prioritize mitigations. Collaborate with experts to incorporate advanced threat intelligence.



Multi-Layered Defence Mechanisms

Implement Zero Trust Network (ZTNA), Security Services Edge (SSE), intrusion detection systems, endpoint protection, and **multi-factor authentication (MFA).**

Awareness Training

Equip faculty, staff, and students to recognize phishing attempts and follow cybersecurity best practices.

Incident Response Plans

Establish clear procedures, test readiness via tabletop exercises, and ensure swift recovery post-attack.

Collaboration and Information Sharing

Partner with peer institutions and agencies to share intelligence and strengthen resilience collectively.

ARANCIA

Contact Us

Partner with experts who understand the intricacies of higher education cybersecurity. Secure your institution's future and protect critical assets from ever-evolving threats. Get to understand how lateral propagation in case of a Cyber event can be managed and stopped at the point of injection.