CYBER SECURITY THREAT DETECTION IN EDUCATIONAL INSTITUTION

Abstract: Educational institutions are increasingly reliant on technology to support learning, research, and administrative operations. However, this increased dependence on technology has also introduced new cybersecurity risks. Cybersecurity threats in educational institutions pose a significant risk to sensitive data, intellectual property, and the overall learning environment. These threats can compromise student and faculty personal data, disrupt academic operations, and damage institutional reputation.

The study revealed that phishing, ransomware, and data breaches are the most common types of cybersecurity threats faced by educational institutions. Vulnerabilities and risks contributing to these threats include outdated software, weak passwords, and insufficient employee training. Cybersecurity breaches can have significant impacts on educational institutions, including financial losses, reputational damage, and disruption to academic operations.

We can implement recommended measures such as implementing firewalls, 1. intrusion detection systems, and encryption, provide regular employee training on cybersecurity best practice, promote a culture of cybersecurity awareness among students, faculty, and staff, develop incident response plans to quickly respond to cybersecurity breaches.

In future we must investigate the effectiveness of different cybersecurity measures in educational institutions and examine the impact of cybersecurity breaches on student learning outcomes. Develop a framework for cybersecurity awareness and training in educational institutions.

Keywords: Cybersecurity; Threat Detection; Educational Institutions; Phishing; Ransomware