ARMIS®

WHITE PAPER

The State of Cybersecurity in Education

Introduction

In today's digital age, educational institutions are not immune to cyber threats. In fact, the influx of digital tools and online learning platforms has made schools and universities prime targets for cyber-attacks. This whitepaper aims to provide a comprehensive overview of the current state of cybersecurity in education, highlighting the unique challenges and solutions for both K-12 and higher education sectors.

The State of Cybersecurity in Education

With the rise of online learning and digital tools, educational institutions have become increasingly vulnerable to cyber-attacks. From phishing scams to ransomware attacks, schools and universities are facing a multitude of cybersecurity threats. According to a report by the K-12 Cybersecurity Resource Center, there were over 1,100 publicly disclosed cyber incidents affecting schools and districts in 2023. Higher education institutions are also at risk, with recent data breaches exposing sensitive information of thousands of students, researchers, faculty and staff.

Unique Differences Between K-12 and Higher Education

While K-12 schools and higher education institutions face similar cybersecurity threats, their challenges and solutions can differ significantly.

K-12 Education

1. Resource Constraints: K-12 schools often have limited budgets and IT staff as well as potentially managing multiple campuses, making it difficult to implement advanced cybersecurity measures.

2. Device Management: The widespread use of Chromebooks and other devices in classrooms presents challenges in managing and securing these assets.

3. Compliance Requirements: Schools must adhere to regulations like the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA).

Higher Education

1. Complex Networks: Universities typically have more complex and decentralized networks, increasing the risk of unauthorized access.

2. Research Data: Higher education institutions often handle sensitive research data, making them attractive targets for cybercriminals.

3. Medical Device Security: Universities with medical facilities must ensure the security of connected medical devices, adding another layer of complexity.

4. Utility Services: Many large universities also have water or electrical generation plants within their campuses

Key Trends Shaping the Future of Higher Education and K-12 Schools

1. **Increased Adoption of AI and Machine Learning:** Institutions are leveraging AI to detect and respond to threats more swiftly.
2. **Zero Trust Architecture:** Schools and universities are adopting zero trust models to enhance security by verifying each access request.
3. **Enhanced Focus on Data Privacy:** With regulations like GDPR and CCPA, there is a growing emphasis on protecting student and staff data.
4. **Integration of Security Tools:** Educational institutions are consolidating their security tools to streamline processes and reduce costs.

Unique Trends in Cybersecurity in K-12 Education

1. Increased focus on student data privacy and protection.
2. Implementation of security training for staff and students.
3. Use of secure communication platforms for remote learning.
4. Adoption of multi-factor authentication for access to school systems.

Unique Trends in Cybersecurity in Higher Education

1. Growing threats from ransomware attacks targeting universities.
2. Enhanced security measures for research data and intellectual property.
3. Collaboration with law enforcement for threat intelligence sharing.
4. Investment in cybersecurity programs and training for students in tech fields.

Challenges in Cybersecurity in Education

Educational institutions face several challenges in maintaining robust cybersecurity:

1. **Lack of Resources:** Both K-12 and higher education institutions often struggle with limited budgets and IT staffing.
2. **Complexity of Networks:** The decentralized nature of university networks can make it difficult to enforce consistent security policies.
3. **Human Error:** Phishing attacks and other social engineering tactics exploit human vulnerability, posing a significant risk.
4. **Compliance:** Schools must comply with various data privacy regulations, which can be challenging to manage.

Educational institutions face several challenges in maintaining robust cybersecurity:

One of the most pressing challenges faced by K-12 and higher education institutions is the lack of resources. Many schools operate on tight budgets that limit their ability to invest in advanced technology and adequate IT staffing. This often results in outdated systems and insufficient cybersecurity measures, leaving institutions vulnerable to threats. Additionally, the shortage of skilled IT personnel can hinder the implementation of effective cybersecurity strategies, making it difficult to respond to emerging threats promptly.

The complexity of networks is another significant hurdle. Universities typically have decentralized networks, comprising multiple departments and campuses that operate independently. This can create inconsistencies in enforcing security policies, as each unit may have its own practices and protocols. The lack of a unified approach can lead to gaps in security, making it challenging to monitor and manage potential vulnerabilities across the entire institution.

Human error remains one of the most critical risks in educational environments. Phishing attacks and other social engineering tactics specifically target individuals, exploiting their vulnerabilities and lack of awareness. As faculty, staff, and students engage with various digital

platforms, they may inadvertently fall prey to malicious schemes that compromise sensitive data. Continuous education and training are essential to equip users with the knowledge to recognize and respond to such threats. Overextended security teams can also contribute to human error.

Lastly, compliance with data privacy regulations is a complex challenge for schools. Educational institutions must navigate a landscape of varying state and federal laws regarding student data protection, which can involve significant administrative burden. Ensuring adherence to these regulations requires robust policies and procedures, as well as regular audits and updates. The challenge lies not only in understanding the legal requirements but also in effectively implementing them across all levels of the institution, which can strain already limited resources.

Solutions to Cybersecurity Challenges

To address these challenges, educational institutions can adopt several strategies and technologies:

1. Complete Asset Visibility: Implementing advanced tools that provide comprehensive visibility into all connected devices and assets is crucial for effective risk management. These tools enable organizations to monitor device status, track changes in the network, and gain insights into asset performance, which helps in identifying vulnerabilities and ensuring that all assets are accounted for in real time.

2. Asset Management and Security: Effective asset management practices involve not only keeping an up-to-date inventory of all assets but also implementing robust security measures. This includes deploying encryption, access controls, and regular audits to protect against unauthorized access and data breaches. By combining these strategies, organizations can create a fortified defense against potential threats while maintaining operational efficiency.

3. Vulnerability Prioritization and Remediation: Utilizing specialized tools that assess and prioritize vulnerabilities based on their risk level and exploitability can significantly enhance remediation efforts. By focusing on the most critical vulnerabilities first, organizations can allocate resources more effectively, reduce potential attack surfaces, and ensure that remediation processes are both timely and efficient.

4. OT/IoT Security: Securing operational technology (OT) and Internet of Things (IoT) devices on campus is vital for preventing cyber-attacks that could disrupt operations or compromise sensitive data. This involves implementing network segmentation, continuous monitoring, and updating firmware regularly to protect these devices from vulnerabilities. Additionally, staff training on security best practices can further bolster defenses against potential threats.

5. Compliance Management: Leveraging cutting-edge technologies and streamlined processes is essential for ensuring compliance with regulations such as FERPA (Family Educational Rights and Privacy Act) and COPPA (Children's Online Privacy Protection Act). This includes automated reporting tools, data encryption, and regular compliance audits to ensure that all data handling practices meet regulatory standards, thus protecting both the organization and its stakeholders from legal repercussions.

How Armis Centrix™ Can Provide a Solution

Armis Centrix™ offers a comprehensive solution to the cybersecurity challenges faced by educational institutions.

Key features include:

Armis Centrix™ offers a comprehensive solution to the cybersecurity challenges faced by educational institutions. Armis Centrix™, the cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time. Our seamless, frictionless, cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats and protects your entire attack surface.

Key products and features include:

1. Time to Value: Work smarter, not harder. With high volumes of assets scattered across different departments and campuses, school districts need an end-to-end solution that hooks into their existing workflow to calculate risk scores creating operational efficiencies to tackle incident response despite headcount or budget issues.

2. Complete Asset Visibility: Armis Centrix™ delivers real-time visibility into all connected assets, ensuring comprehensive coverage across your organization. This visibility allows for prompt identification of potential security gaps and enhances overall asset management.

3. Asset Management and Security: With an asset-centric approach, the platform guarantees effective management and security of all devices. This not only streamlines operations but also fortifies defenses against potential threats, ensuring a robust security posture.

4. Vulnerability Prioritization and Remediation: Armis Centrix™ for Vulnerability Prioritization goes beyond mere identification; the platform prioritizes responses based on the severity of vulnerabilities, identifies accountable owners for each asset, and operationalizes a comprehensive remediation lifecycle.

5. Early Warning Threat Intelligence: Armis Centrix™ for Actionable Threat Intelligence, organizations can enhance their prioritization efforts. This feature leverages advanced early warning detection systems and actionable threat intelligence to specifically target vulnerabilities currently being exploited by threat actors, enabling timely and effective responses that minimize potential damage.

6. OT/IoT Security: The platform safeguards both Operational Technology (OT) and Internet of Things (IoT) devices, effectively preventing unauthorized access and mitigating cyber-attack risks. This layer of security is crucial as the number of connected devices continues to rise.

7. Compliance and Safety: Armis Centrix™ assists institutions in adhering to critical regulations such as FERPA and COPPA, ensuring data privacy and security. By maintaining compliance, organizations can avoid costly penalties and enhance their reputation.

8. Speed of Deployment: Featuring hundreds of integrations, Armis Centrix™ allows for rapid deployment and delivers immediate value. This swift setup ensures that organizations can quickly enhance their security posture without significant downtime.

9. Future-Proofed Cybersecurity: Armis Centrix™ equips organizations for future digital transformations and evolving cybersecurity threats. By staying ahead of emerging risks, companies can maintain resilience in an increasingly complex threat landscape.

ARMIS

Real-Life Examples

LEHIGH UNIVERSITY

Background

Lehigh University, a private research institution in Bethlehem, Pennsylvania, serves around 8,000 students.

Challenge

The university's security team struggled with ineffective vulnerability assessment processes, resulting in protracted remediation times and inconsistent prioritization outcomes.

Solution

By integrating Armis Centrix™ for VIPR Pro – Prioritization and Remediation, the team streamlined vulnerability management, reduced assessment times by 80%, and decreased tool costs by 40%.

Results

- **Improved operational efficiency for proactive security management**
- **Enhanced ability to identify and prioritize risks**
- **Minimized manual efforts for remediation**

Conclusion

Cybersecurity in education is a complex and evolving challenge, but with the right tools and strategies, institutions can protect their assets, data, and reputation. Armis Centrix™ offers a robust solution to these challenges, providing comprehensive visibility, effective asset management, and streamlined vulnerability remediation. By leveraging Armis Centrix™, educational institutions can enhance their cybersecurity posture and ensure a safe learning environment for students and staff.

Get Started with Armis Centrix™ Today

By implementing these comprehensive strategies and leveraging cutting-edge technologies like Armis Centrix, educational institutions can stay ahead of cyber threats and maintain a secure environment for their academic communities.

ARMIS.

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial