

Cybersecurity Essentials for School Boards

Purpose

With schools becoming increasingly dependent on technology, they are becoming prime targets for cyber threats. This session aims to highlight the critical need for an incident response plan (IRP) and the importance of budgeting for cyber defense services to effectively protect educational institutions from these evolving threats

Impact on Schools in New Hampshire

In recent years, several schools in New Hampshire have experienced significant cyber incidents such as ransomware attacks and data breaches. These events have led to:

- **Disruptions to Classes and Educational Services:** Operational interruptions affecting daily school functions.
- **Unauthorized Access to Sensitive Information:** Breaches of personal data for students and staff.
- **Financial Costs:** Substantial expenses related to remediation and recovery.

The frequency of targeted cyber attacks on educational institutions in the region has increased significantly, underscoring the need for effective cybersecurity measures.

Importance of an Incident Response Plan

- **Rapid Response:** Enables a quick and coordinated reaction to minimize damage.
- **Clear Protocols:** Provides guidelines for managing various cyber threats, ensuring all staff are prepared.
- **Legal and Regulatory Compliance:** Helps meet legal requirements and avoid fines.
- **Protection of Sensitive Data:** Safeguards personal information from unauthorized access.
- **Maintains Trust:** Demonstrates a commitment to security, reinforcing trust with students, parents, and the community.

Importance of Budgeting for Cyber Defense Services

Investing in cyber defense services is essential for preventing and managing cyber threats. This investment offers:

- **Prevention:** Regular security assessments and threat monitoring to avert incidents.
- **Expertise and Resources:** Access to specialized skills and tools not available in-house.
- **Continuous Monitoring:** 24/7 surveillance to detect and address threats in real-time.
- **Incident Support:** Immediate guidance and support during and after incidents.
- **Cost-Effectiveness:** Proactive measures are often more economical than dealing with the aftermath of cyber attacks.

Call to Action

To strengthen cybersecurity and protect our educational institutions, we must:

1. **Develop and Implement an Incident Response Plan:** Create a tailored IRP to address specific needs.
2. **Allocate Budget for Cyber Defense Services:** Invest in cybersecurity measures and expert support to enhance overall protection.



NH Municipal Cyber Defense Program

The New Hampshire Municipal Cyber Defense Program (MCDP), managed by The ATOM Group, is a key initiative for enhancing New Hampshire's Cybersecurity Defense Services. Funded by the NH Department of Information Technology and the State and Local Cybersecurity Grant Program, it aims to protect public trust in technology by providing comprehensive Cybersecurity training.

The MCDP is critical to New Hampshire as it enhances cybersecurity readiness across municipal and public sector entities. This program stands out because it is customized based on the municipality's type, job description, and organization's existing cybersecurity readiness.

For more information, please contact:

Emily McGovern

Cyber Operations Specialist
NH Municipal Cyber Defense Program (MCDP)

Email:
emily@theatomgroup.com

Phone:
603.501.0003 x107

Website:
theatomgroup.com/mcdp



New Hampshire

DoIT

