Cyber attacks are on the rise

Did you know...

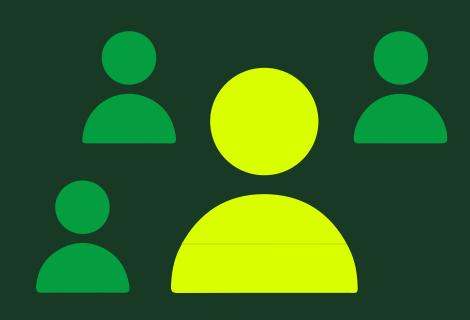


Since 2016, there have been over

publicly disclosed school cyber attacks in the US.1

Averaged out over the past six years, that's MORE THAN ONE K-12 cyber incident PER SCHOOL PER DAY.1





Over half of those K-12 data breaches resulted from actions taken by school staff and stuudents.⁵

A Strong Cybersecurity Program Starts with

Cyber Governance Planning

What should digitally responsive educational organizations do to establish a strong cyber governance program?

- Develop proactive policies for cybersecurity.
- Provide cyber hygiene training for staff.
- Teach students best practices for online safety.
- Take advantage of the K-12 Cybersecurity Learning Standards to enrich students' skills and knowledge in three core concepts: Computing Systems, Digital Citizenship, and Security.

What is cyber governance?

Cyber governance is the shared ownership and accountability to design, implement and improve key contingency management practices and to operate a cybersecurity program that supports the district's cyber needs.

How can Bluum help?

Conduct an after-action review session to evolve

the planning documents and institutional knowledge.

Facilitate a tabletop exercise to test and drill key aspects of the contingency plans.

Create core documents to establish & test contingency management.

> Review policies for contingency management and create plans.

Cyber Governance Planning Process:

Identify organizational structures related to cyber governance.

> Use a Business Impact Analysis (BIA) to build the business continuity and

Leverage the NIST Cybersecurity Framework (CSF) or the CIS Controls as the foundational cyber framework for contingency management for the district.

disaster recovery plans.

Cybersecurity in education Where should you start?



Plan Processes & Practices



Pinpoint **Vulnerabilities**



Build Resiliency

For more information on Bluum's Cybersecurity solutions

www.bluum.com/cybersecurity

