

Incident Response Planning

Preparing, Detecting, and Reacting to a Data Breach for K-12 Schools

A cybersecurity incident response plan covers what to do and identifies who is responsible for doing it when there is a cyberattack. Creating a plan, updating it regularly, and revisiting it annually with new hires and in refresher sessions with your entire staff can help you maintain business continuity and minimize reputational damage in case of a cybersecurity incident. Use this checklist as a tool to help create and maintain your school's cybersecurity incident response plan.

Before a Breach: Preparation

Teacher and Staff training - outline typical phishing tactics and the school's Cyber Security Policies

Maintain a detailed and comprehensive hardware database, including all devices connected to the network. Don't forget about printers!

Define roles and responsibilities in the event of a data breach

Outline the School's Incident Response Plan

During a Breach: Containment and Recovery

Contain the breach to prevent the spread to other connected devices

Activate protocols to access any backup systems to critical student and staff information

Review all access credentials, and change passwords for each account

Apply all security patches and updates to software or applications

After a Breach: Response and Recovery

Conduct an after-action meeting to review the recovery tactics, potential vulnerabilities, and prevention measures to put in place

Clearly report to the students and staff steps they can take to secure their personal information in the coming months

Review how the data breach was discovered and when to determine the source of the depth of the breach

Continue staff and teacher education to ensure a similar breach doesn't happen again



How Arista Can Help

Arista's Cognitive Unified Edge (CUE) solutions help enable school IT administrators to monitor, protect and control their networks while also providing protection from evolving threats. CUE products provide enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Block students from accessing inappropriate content
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for learning
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

Arista Benefits

- Gain visibility into all the devices connecting to the network
- Advanced threat protection from malware, spam, phishing and emerging threats
- Block students from accessing inappropriate content
- Create detailed reports to prove CIPA compliance



Santa Clara—Corporate Headquarters

5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500

Fax: +1-408-538-8920

Email: info@arista.com

Ireland—International Headquarters

3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office

9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office

Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office

9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989



Copyright © 2023 Arista Networks, Inc. All rights reserved. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. February 24, 2023