Getting Started with Cybersecurity

2 Incidents per week:
Since 2016, U.S. K-12 school districts have experienced more than two cyber incidents per week on average.

Fastest growing cyber incidents in K12 schools
Successful phishing attacks

Most common cyber incidents in K12 schools
Hacks + Unauthorized Data Breaches/ Disclosures

Incidents growing exponentially:
Right now, we are on pace in 2017 to see more than double the number of K-12 cyber incidents experienced in 2016.

The percent of cyber incidents involving K-12 schools due to the actions of school staff and/or students of those schools, sometimes resulting in criminal charges.

SOURCE for above statistics: edtechstrategies.com/map
Getting Started with Cybersecurity

What Should SCHOOLS Do?
Put reasonable protections in place, realize nothing is 100% breach proof.

Where should districts start to get the biggest improvement in security?

- **Patch software and operating systems**, and be ready to abandon software when it becomes obsolete
- **TRAIN, TRAIN, TRAIN!** Make sure everyone knows security awareness is their job and who to talk to if they make a mistake
- Educate district staff about social engineering
- Build a sustainable, long-range plan for security. Besides consistent training, create a rotation of other areas of security like technical hardware refreshes, application reviews/updates, assessing which vendors may have VPN access to your network, etc.
- Utilize resources like Department of Homeland Security (DHS) and MultiState-I Information Sharing and Analysis Center (MS-ISAC). They provide free monitoring and will help remediate in some cases; they have a host of resources and tools

Checklist for YOUR school. To get started, make sure your school has:
- Patched software systems and abandoned obsolete software
- Trained everyone so they know security awareness is part of their jobs
- Educate district staff about social engineering
- Built a sustainable, long-range plan for security
- Utilized resources that provide free monitoring for your school

More information can be found at CoSN.org
## TECHNOLOGY Preparedness

### Put technology appliances in place:
- Firewall
- DMZ: a “demilitarized zone” or subnetwork that contains and exposes the district’s external services to the Internet
- Make sure all your operating systems are up to date

### Put security processes in place:
- Traffic inspection
- Backups: Invest in hyperconvergence and robust disaster recovery systems
- Effective and up-to-date anti-virus
- Automated patching and maintenance
- Have a vendor or 3rd party partner audit district security
- Role-based permissions (defined based on network access role based permissions) Least amount of access possible to do their job - appropriate access level
- Password change schedule
- In case of network interruption, have a prioritized list of essential systems that need to be restored or started up again in order to keep your district afloat.
- Implement change management to ensure that you know what is approved for change and what is not
- Conduct tabletop exercises

More information can be found at CoSN.org
Getting Started with Cybersecurity

What Should DISTRICTS Do?

PEOPLE Preparedness

• Minimize the staff’s ability to be compromised
• Training
• Security awareness (every month)
  > Social engineering
  > Phishing: General and spear phishing
  > Who to tell when something goes wrong (“oops i clicked the link!”)
• Password management
  > Balance usability and security
  > Consider implementing 2-factor authentication
• Practice: Have department drills around specific security incidences
• Consider outsourcing some security tasks if capacity is an issue

BREACH Preparedness

• Have a conversation with your insurer before you have an event to understand your responsibilities
  > Purchase a policy that also includes forensic work
  > Consider hiring a firm on retainer so they can provide immediate assistance when needed
• Consider having a breach coach - a breach coach works with the insurance carrier to triage the event and help districts navigate the process, including notification requirements
• Work with your communications department for messages to your staff/community
• Prepare document templates ahead of time
• Know where your data is and what is protected class data, i.e., PII, Special Ed status, medical status

More information can be found at CoSN.org
Getting Started with Cybersecurity

What Should DISTRICTS Do?

INCIDENT DETECTION + RESPONSE

- Have a baseline of what a normal day looks like to compare with current operation
- Have the tools at your disposal to troubleshoot the incident
  > IT management software and monitoring tools
  > Good SNMP reporting system
  > Have reports ready to go (e.g. is the switch down or exceeding threshold, are ports exceeding their throughput threshold, are non-standard ports being contacted, etc.)
  > Consider a Security Incident Event Management system

ASSET MANAGEMENT

- Know your assets and devices
- Know where your data is for recovery purposes

PUBLIC RELATIONS

- Have communications plans established in advanced
  > Don’t use alarming words or phrases
  > Build response templates for common incidences

Together, we can help keep our schools safer!

More information can be found at CoSN.org