

# Coordination & Cooperation

K12 Information Security



# Introductions



- Mike Potter (he/him)  
IT Security Analyst, CISSP  
NWRESD & CTA
  - Hasan Ali (he/him)  
District Systems & Security Engineer  
MESD & CTA
  - Jacob Doxtator (he/him)  
District Systems & Security Engineer  
NWRESD & CTA
-

**We are honored to present today at Erb Memorial Union  
(EMU), a famous location in academia...**

The site of the Fishbowl, setting for *Animal House's* food fight



# Coordination & Cooperation

K12 Information Security

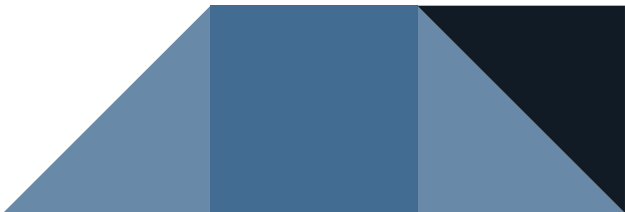




What cybersecurity threats do K12 organizations face?

# All of them!

Malware, ransomware, email compromise, phishing, data leaks, malvertising, third party provider risks, denial of service, insider adversaries...

- Check Point's 2022 mid-year report showed a 44% increase on cyber attacks on K12 organizations since 2021.
  - Ransomware group Akira claimed Edmunds, WA SD as a victim; one of 11 US schools attacked by ransomware groups in August 2023
  - Disruptive attacks like DDos and service abuse like "Zoombombing" interrupt K12 instruction more severely as our use of digital tools grows
- 



Cyber attackers specifically target K12

# More to protect, harder to defend

- K12 IT supports an open, collaborative environment with limited resources, and yet has sensitive information and people to protect:

“In fact, while most companies only have employees, academic institutions don’t just have teachers...; they also have students, making networks in the sector much bigger, more open and more difficult to protect.” [Infosecurity Magazine, Oct 14, 2022.](#)

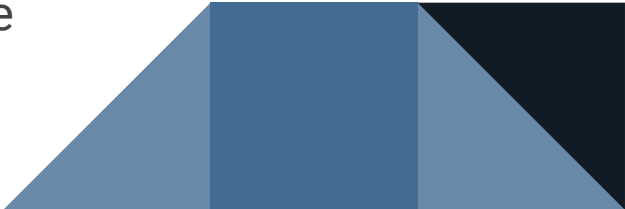
- As students are learning how to use technology responsibly and about the concepts of privacy, they also have access to tools and services that can cause far more disruption and harm than pulling a hallway fire alarm.






# Willie Sutton & K12 data

**Why attack K12 systems and resources? Because identity and credit thieves want student information and K12 is where it lives.**

- Personal identifiable information (PII) from school employees, district families, past students, and students under the age of 18.
  - Students whose information is stolen and used for credit fraud often don't find out until applying for financial aid for college.
  - Cyber insurance policies and a desire to prevent the release of student information leave some K12 organizations vulnerable when targeted by ransomware.
- 



What resources does K12 have to face these challenges?

# Resources vary by district, but the needs are often the same

## How many people, how many devices


Districts with 200 or 500 students, teachers, and their devices face the same cyber threats as districts 1000x larger, but with tighter budgets and fewer tech workers.

**Shifting cost landscape:** enhanced security features require paid licenses from providers like Google and Microsoft, which not all districts can afford.

MFA deployment, for example, could be a huge lift or an easy project for a district, a huge new cost or something already included in what they have, but it's required by cyber insurance just the same.



# Oregon's Education Service Districts

- ORS 334.005 Mission...to assist school districts and the Department of Education in achieving Oregon's educational goals by providing equitable, high quality, cost-effective and locally responsive educational services at a regional level.
  - Technology support with member districts is a listed core function for ESDs.
  - Working together can include buying together as a coalition, sometimes with pre-negotiated privacy policies for K12 accounts.
  - Cascade Technology Alliance, which includes technology professionals from Northwest Regional and Multnomah ESDs, started a pilot project in 2022 to share information security resources with member school districts.
- 



# From pilot project to cybersecurity journey

# What is a CTA IT Security Assessment?

- School districts request an IT security assessment from CTA
- CTA meets with district technology staff to review the process and schedule when we conduct the review and vulnerability scans. By necessity, these scans are designed not to interrupt normal school technology use.
- Afterward, CTA creates a report of findings and recommendations, working with the district to identify any follow-up actions or projects that CTA and the district could tackle together
- Future assessments phases will build what we found before and expand the scope of review



# What are we looking for?

- Using cybersecurity guides from CISA and K12SIX along with vulnerability scanning, we try to identify **critical IT security issues**. In other words, what needs our attention first?
- We don't attempt to find all security vulnerabilities that we can. The assessment is just the first phase of CTA's ongoing IT security assistance and partnership with member districts. It's a way to get started and build momentum.



# K12SIX Cybersecurity Essentials for Schools

1. Sanitize network traffic to/from the Internet
    - 1.1. Block malicious web content
    - 1.2. Defend against email attacks
    - 1.3. Segment [network] and limit exposed services
  2. Safeguard student, teacher, and staff devices
    - 2.1. Restrict administrative access
    - 2.2. Apply endpoint protection
  3. Protect student, teacher, and staff identities / accounts
    - 3.1. Protect user logins: MFA
    - 3.2. Improve password and account management
    - 3.3. Minimize third party risk
  4. Practice continuous improvement
    - 4.1. Install security updates
    - 4.2. Manage sensitive data
    - 4.3. Train to improve cybersecurity awareness
    - 4.4. Plan for cyber incidents
- **Aligned with the NIST Cybersecurity Framework & CIS Controls**

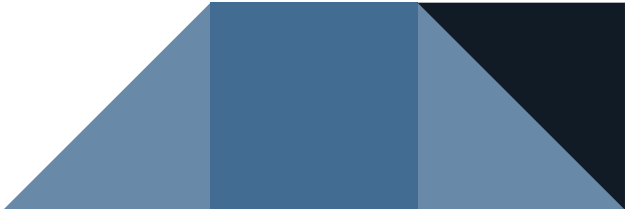




# Project Roadblock

# Roadblock: Dozens of Different Networks

CTA has 36 member school districts, each with its own servers, systems, and networks.

- Working with district technology staff, we were able to get some systems ready for scans, but not every district had staff available to do all the preliminary work needed.
  - We learned technicians in each district needed time to review and figure out what configuration changes were needed and how to apply them.
  - We needed a way for us to make configuration changes on different district networks more efficiently and quickly, especially if we wanted to return for more scanning in future assessment phases.
- 

# Repeatable Recipe for Success

1. **Least intrusive (yet helpful) scans**
2. **GPO/Script for consistency**
3. **Clean up!**



# Agentless Vulnerability Scans

## 1. Nessus Credentialed Check

- Needs AD setup, great for reporting Windows vulnerabilities.

## 2. Nmap Vulnerability Scan

- Works especially well for Linux systems.



# GPO/Script For Consistency

1. **Open Windows Firewall ports on devices to be scanned using a new Group Policy Object setting.**
2. **Ensure needed services are enabled via script.**
3. **Consistent and easy to import into district domains.**



# Clean Up!

1. **Disable scanner account after scan.**
2. **Revert GPO settings, disable unneeded services.**
3. **Make sure district systems are green.**



The background is a solid dark blue. In the top right corner, there is a decorative pattern of overlapping squares and triangles in various shades of blue and black. The text "What's next?" is centered on the left side of the slide.

What's next?

# What's next for our IT Security Assessments?

- If you think this sounds like Cybersecurity 101—assessing system settings according to cybersecurity standards and vulnerability scanning—well, **you're right!**
- CTA's goal is to bring essential cybersecurity protections to all school districts because every school community, regardless of size or location, needs them.
- For our assessments, that means running more scans on more systems at more schools.
- Most importantly, it also means more conversations with more people about what we can do to keep improving K12 cybersecurity together.





# Coordination & Cooperation

K12 Information Security

