# K-12 CYBERSECURITY

## Best Practices, Enterprise Tools and LB 937 Assessment

*Presented to School Administrators & Technology Directors*
*April, 2026 Nebraska Department of Education Data Conference*

**Nebraska ESU Coordinating Council**

# TODAY'S AGENDA

01

## The Threat Landscape

Why cybersecurity matters for K-12 schools right now

02

## 10 Cybersecurity Best Practices

Technical safeguards & policy controls every district should implement

03

## Enterprise Products & Services

Tools available through statewide contracts and grants

04

## LB 937: The Assessment Project

Legislation, the tiers framework & implementation plan

# 01

## THE THREAT LANDSCAPE

*Why cybersecurity can't wait*


# WHY SCHOOLS ARE TARGETS

## Rich Data

Student records may contain SSNs, health info & financial data — highly valuable on the black market

## Large Attack Surface

Thousands of devices, staff accounts & students create many entry points for attackers

## Under-Resourced

Schools are often under-resourced for IT security compared to other sectors

## Maximum Disruption

Disrupting schools causes maximum community impact — exactly what ransomware groups want

# 2025 MS-ISAC K-12 CYBERSECURITY REPORT

*5,000 districts responded*

**82%**

Experienced Cyber Threat Impacts

**14,000**

Security Events Reported

**9,300**

Confirmed Incidents

**5,000**

Districts Responded

*Source: Center for Internet Security / CoSN · 2025*

# TOP CYBER THREATS FACING K-12 SCHOOLS

**1** **Ransomware Attacks**

Encrypts school files, demands payment — can shut down operations for days or weeks

**2** **Phishing & Social Engineering**

Deceptive emails/calls tricking staff into revealing credentials or transferring funds

**3** **Malvertisement**

Malicious ads through legitimate websites expose students and staff to malware

**4** **Data Breaches**

Unauthorized access to student/staff PII for identity theft or sale on the dark web

**5** **Denial-of-Service Attacks**

Overwhelming school networks to disrupt instruction and operations at critical times

## Trends

**Focusing on the human element**

**Acting at critical times to maximize disruption**

***Trend: Cybercriminals now focus on the human element and time attacks during critical school periods.***

# 02

# 10 CYBERSECURITY BEST PRACTICES

*NATA / ESU-NOC Joint Letter*

TIER 1 — TECHNICAL & PROCEDURAL SAFEGUARDS

# 1. Multi-Factor Authentication (MFA)

1

## The single most effective control against account compromise

**Applies To:** All systems housing PII or sensitive data — email, SIS, remote access
**What it does:** Requires a second verification step — even if credentials are stolen, attackers cannot log in
**How to start:** Cisco Duo is available statewide — 10,000 licenses at $8/user; Class Link
**Tip:** *Begin with email, student information systems, and remote access first*

# 2. Vulnerability Scanning & Pen Testing

2

## Find your weaknesses before attackers do

**Vulnerability Scanning** identifies unpatched software, misconfigured systems, and exposed services
**DHS NCATS** service is free to schools and ESUs and provides a weekly scan report
**Make a plan** to address vulnerable items

## *Advanced*

**Ethical Penetration Testing** simulates a real attack to test your defenses before attackers do
Penetration testing services are **more costly** than many districts are able to afford/sustain
**ESUs** have pursued group purchasing of penetration testing services

# 3. Endpoint Detection & Response (EDR)

3

## Next-generation protection for every device on your network

**EDR goes beyond antivirus:** Detects and blocks modern malware, ransomware, and infostealer threats in real time
**Behavioral detection:** Identifies suspicious patterns even from unknown, new threats
**Automatic response:** Can isolate an infected device before malware spreads across the network
**Priority for:** *Staff workstations, servers, and any device accessing student data*

# 4. Air-Gapped, Immutable Backups

4

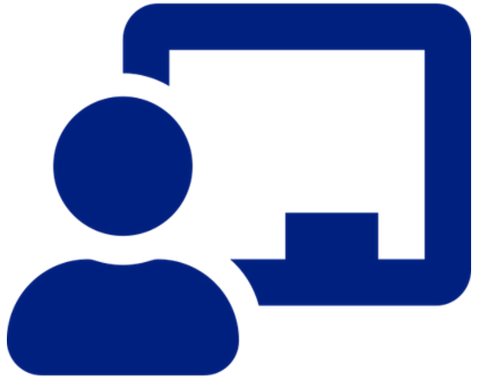
## Your last line of defense — and your fastest recovery path

**Air-gapped:** Backups physically or logically isolated from the network — ransomware cannot encrypt them
**Immutable (WORM):** Write-Once-Read-Many storage cannot be modified — even by attackers with admin access
**Test regularly:** An untested backup is not a backup — schedule quarterly restore tests
**SLCGP Year 3 Priority:** *Enhanced off-site, immutable backup services are proposed for Year 3 grant funding*

# 5. Staff Cybersecurity Awareness Training

5

## Humans are both the biggest vulnerability and the best defense



**Core topics:** Phishing recognition, credential hygiene, data handling, reporting suspicious activity
**Simulated phishing:** Regular test campaigns keep staff vigilant and show where training is needed most
**Trend:** Cybercriminals increasingly target the human element — technical controls alone are insufficient
**Under evaluation:** *KnowBe4, CyberNut, and Zenguide — NOC decision by August 2026. ZenGuide currently at $3.69/staff member per year*

# Practices 6 & 7

6

## Principle of Least Privilege

**Dedicated admin accounts:** IT staff must use separate admin accounts — 'daily use' accounts must never carry admin rights

**No local admin rights:** Building/district admins should not have admin privileges on their own devices

**Why it matters:** *Limits blast radius if an account is compromised*

7

## Network Segmentation

**Separate subnets:** Students, staff, servers, facilities, and security systems must be on separate network segments

**Prevent lateral movement:** Rules between segments stop attackers from spreading across systems

**Guest WiFi:** *Student/visitor networks must never reach administrative systems*

# Practices 8 & 9

8

## Centralized Patch Management

**Automated patching:** Systems keep all OS and apps up to date across every device

**Most successful attacks:** Exploit known vulnerabilities with patches already available

**Goal:** *Critical patches applied within 24–72 hours of release*

9

## Secure Password Management

**Enterprise password manager:** Reduces insecure passwords and password reuse across all staff accounts

**Password reuse danger:** One breached credential can unlock many systems

**Policy tip:** *Unique passwords for every school system; the manager removes burden from staff*

# 10. Incident Response Planning

10

**When — not if — an incident occurs, a plan is the difference between hours and weeks of downtime**

1. **Prepare**
   Document contacts, systems, and escalation procedures before any incident occurs

2. **Detect & Analyze**
   Know how to identify a breach and determine its scope quickly

3. **Contain & Eradicate**
   Isolate affected systems; remove the threat before reconnecting anything

4. **Recover**
   Restore from clean backups; verify integrity before resuming operations

5. **Post-Incident Review**
   Document lessons learned and update controls to prevent recurrence

*SLCGP Year 3 Proposal: Incident Response Planning Workshops for all participating ESUs*

# 10 BEST PRACTICES — QUICK REFERENCE

### Technical & Procedural Safeguards

1. Multi-Factor Authentication (MFA)
2. Vulnerability Scanning & Pen Testing
3. Endpoint Detection & Response (EDR)
4. Air-Gapped, Immutable Backups
5. Staff Cybersecurity Awareness Training

### Policy & Configuration Controls

6. Principle of Least Privilege (PoLP)
7. Network Segmentation
8. Centralized Patch Management
9. Secure Password Management
10. Incident Response Planning

- Source: NOC-NATA Joint Letter December, 2025

# 03

# ENTERPRISE PRODUCTS & SERVICES

*Statewide tools for Nebraska schools*

# CISCO DUO

MFA Group Purchase

**10,000**

Licenses Available

**$8 / user**

Current cost · Renewal: Annually in March

## Why Cisco Duo for Your District?

- Protects a wide variety of systems through already-built integrations
- Easy self-enrollment for staff — minimal IT overhead
- Works with Microsoft 365, Google Workspace, and many school systems
- Available to all Nebraska districts through the statewide agreement. Renewal is annually in March. Licenses are still available.
- **Alternative: ClassLink also provides MFA features for many school districts**

# NOC Evaluation — Decision in Summer 2026

**Three platforms are under evaluation. Current cost: $3.69/staff member. Proposed for SLCGP Year 3 subsidy.**

## ZenGuide

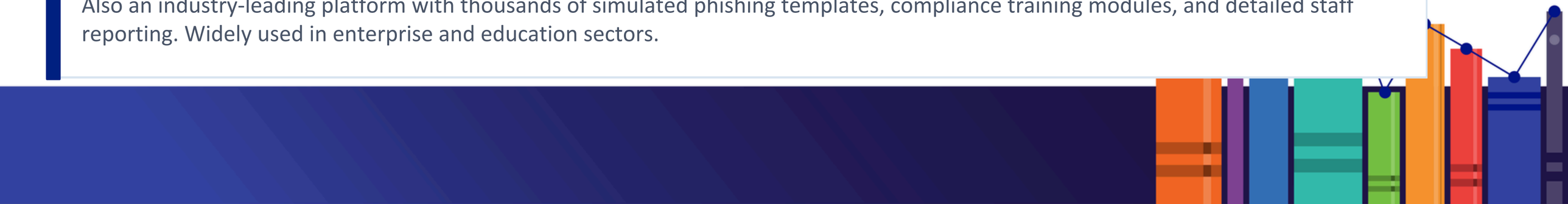
Current statewide contract. Streamlined awareness training with a strong analytics dashboard. Enables administrators to track completion rates and identify high-risk users across the district.

## CyberNut

Education-focused security training with age-appropriate content for K-12 staff and students. Gamified modules designed specifically for the school environment.

## KnowBe4

Also an industry-leading platform with thousands of simulated phishing templates, compliance training modules, and detailed staff reporting. Widely used in enterprise and education sectors.



# FEMA / CISA — Multi-Year Grant Progress in Nebraska

## Year 1
## FY2022

- NCNE training and assessments (10 ESUs)
- Resolute Guard (7 ESUs)

## Year 2
## FY2023

- Cyber event logging (Elastic)
- 16 ESUs participating

## Year 3
## FY2024

- Off-site immutable backups
- Incident Response workshops
- End-user training subsidy
- NE State Committee: May-June 2026 Review

## Year 4
## FY2025

- Develop & implement cyber plans
- NE priorities TBD
- Considering whole-of-state plan

# 04

# LB 937: THE K-12 CYBERSECURITY ACT

*Nebraska's Assessment Project*

THE K-12 EDUCATION CYBERSECURITY ACT

# LB 937 — What the Law Does

## Up to $250,000 for 1 year

2026–2027
Cybersecurity Assessment & Coordination
(NDE, ESUCC, OCIO)

## $?? / year

2027–2028 and future
Cybersecurity products & services for schools

# LB 937 — KEY REQUIREMENTS & GOVERNANCE

- Cyber assessment required for districts & ESUs to access future product/service funding
- (Future) Eligible products & services coordinated with OCIO, NDE & ESUCC
- ESUCC serves in a non-regulatory, supportive role — local control is preserved
- NDE, OCIO & ESUCC have already met and provided feedback to Sen. DeBoer
- **A Steering Committee is being formed (ESUs, NDE, OCIO, NATA, Non-Public Schools)**

# BROAD COALITION OF SUPPORT

## NDE

**Nebraska Department of Education**

Regulatory partner; collects baseline cybersecurity readiness data from all districts

## OCIO

**Office of the Chief Information Officer**

State technology oversight; coordinates eligible products and services statewide

## ESUCC

**ESU Coordinating Council**

Non-regulatory support; coordinates assessment process and facilitates workshops

## NATA

**Nebraska Assoc. of Technology Administrators**

Practitioner voice; co-authored cybersecurity best practices with ESU-NOC

## Non-Public

**Catholic Conference & Allies**

Ensuring private schools are included in the statewide approach

## NITC

**Nebraska Information Technology Commission**

Advising the partners on technical standards and practices

# TIERS OF CYBERSECURITY MATURITY

*Needs change as cybersecurity posture strengthens. Greater state support at foundational levels.*

**Tier 1: FOUNDATIONAL**

Basic protections are absent or minimal. Greatest need for state-level support and resources.

**Tier 2: DEVELOPING**

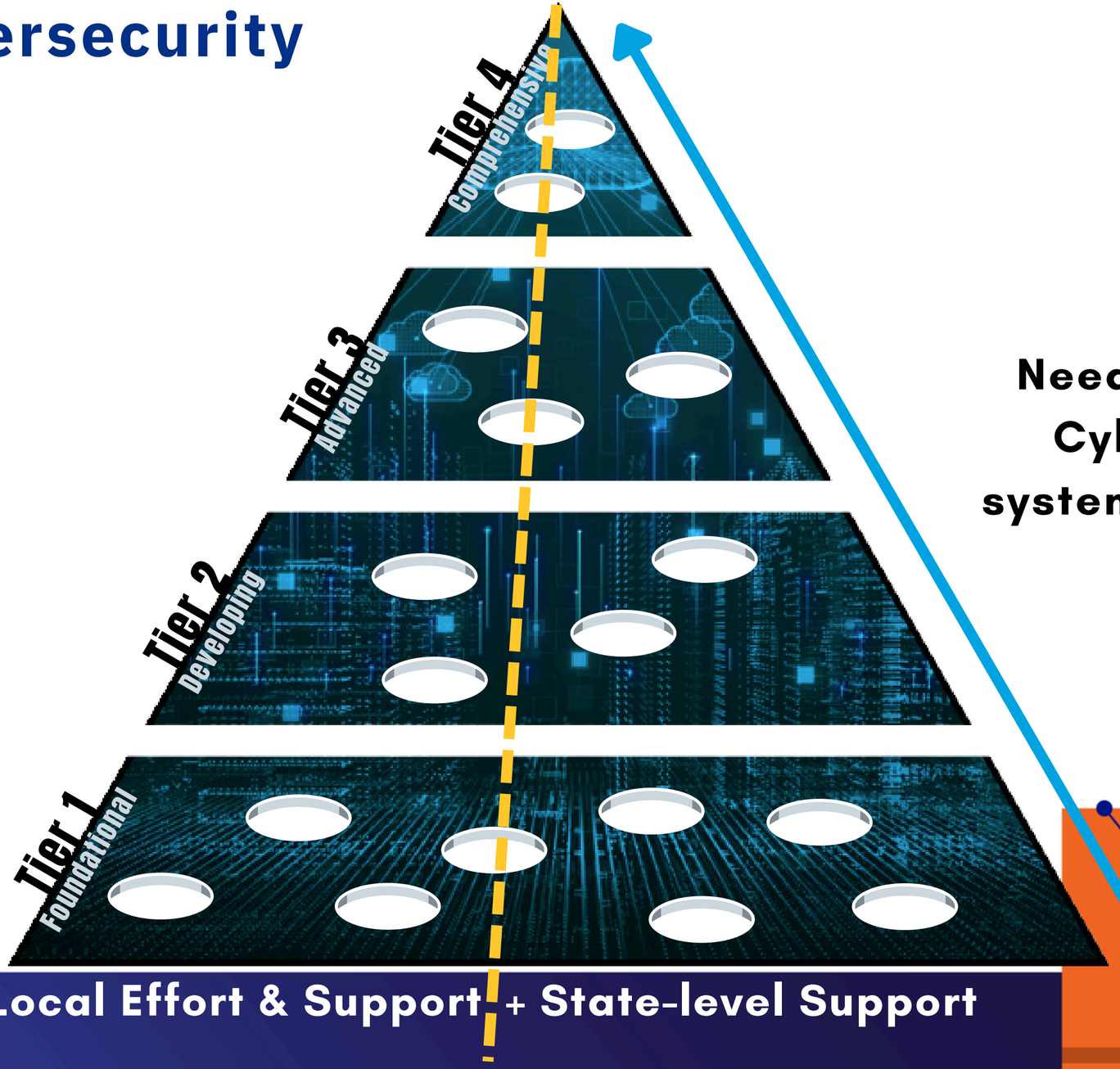
Some controls in place but gaps remain. Moving toward consistent implementation.

**Tier 3: ADVANCED**

Focus shifts to optimization, monitoring, and

**Tier 4: COMPREHENSIVE**

# Tiers of Cybersecurity




**Needs change as Cybersecurity systems strengthen.**

**Greater Need at Foundational Levels**

**Local Effort & Support + State-level Support**

# THE ASSESSMENT PROCESS — YEAR ONE

1

## Finalize Steering Committee

Establish governance with NDE, OCIO, ESUCC, NATA — outline timelines and decision points

2

## Select Assessment Framework

Review and choose a consistent framework and collection system usable across all districts

3

## Design Assessment Workshop

Target: 1 hour to complete — syncable with existing tech or already-scheduled meetings

4

## Test with Early Adopters

Pilot with volunteer ESUs and districts before statewide rollout — refine as needed

5

## Conduct Statewide Assessments

Facilitated workshops across all ESUs; funded by Education Improvement Fund Grant

6

## Compile, Report & Advocate

Analysis → stakeholder reports → Legislature reporting → advocacy for continued support

**Scott Isaacson**
Chief Information Officer
sisaacson@esucc.org
402-597-4933
www.esucc.org

# TOGETHER, WE RAISE THE CYBERSECURITY FLOOR FOR ALL NEBRASKA SCHOOLS.

## Questions & Discussion

www.esucc.org

Nebraska ESU Coordinating Council · NATA · NDE · OCIO