LBL CYBERSECURITY

Cyber Ready 365

Board Preparedness Guide



Helping Every School Board Member Stay Cyber Ready.

Cyber incidents can interrupt education, jeopardize data, and diminish public confidence. Effective cybersecurity leadership begins at the top.

Developed by LBL Cybersecurity, Oregon's trusted partner for K–12 cybersecurity readiness.

We help schools, cities, and special districts stay protected 365 days a year.

A GROWING THREAT

Cyberattacks on K–12 schools have increased by more than 80 percent in the past two years, making education one of the fastest-growing targets for cybercrime.

RANSOMWARE SURGE

Over 5,000 U.S. schools were affected by ransomware in 2023 alone.

BACKUPS COMPROMISED

In 2024, 71% of educational institutions had their backups successfully compromised during cyberattacks.

SOCIAL ENGINEERING

Cyber threat actors now target human behavior 45% more often than technical vulnerabilities.

TARGET

Schools are now the #1 target for ransomware in the public sector.

IDENTITY THEFT

One in eight U.S. children has experienced a compromise of their identity as part of a data breach in the past six years.

$3.65 Million

FINANCIAL STRAIN

The average cost of a data breach in the education sector was $3.65 million in 2023, underscoring the significant financial risks schools face.

LACK OF RESOURCES

75% of school IT leaders say they lack the resources to fully secure their networks.

RANSOMWARE SURGE

The number of K-12 school districts directly impacted by ransomware attacks more than doubled from 2022 to 2023, indicating a troubling trend.

PROACTIVE MEASURES

Implementing comprehensive cybersecurity training for staff can reduce the risk of data loss by up to 70%.

AWARENESS & PREPAREDNESS

Seeing individuals as cybersecurity assets rather than liabilities contributes to the enhancement of school defenses.

COMMUNITY TRUST

A strong cybersecurity posture helps maintain community trust, ensuring that parents and students feel confident in the school's ability to protect personal information.

RESPONSE PLANS

Having an incident response plan is essential for schools to effectively handle cyber threats and minimize damage.

PLAN AND PREPARE

Cyber incident response plans reduce downtime by 50% or more.

CASE STUDY:

How a School Board Navigated a Ransomware Crisis

Based on a real incident | Names changed to protect the district

A board's perspective on navigating a critical cyber crisis

The District

Riverside School District serves approximately 5,000 students in a suburban community. Like many school districts, they had implemented standard cybersecurity measures and carried cyber insurance, but no district truly expects to face a ransomware attack—until it happens.

The Incident

In July, during the summer break, the district's IT staff discovered that their financial system and email had been encrypted by ransomware. Staff couldn't log into critical financial systems. Email services went dark. An investigation quickly revealed that hackers based in Eastern Europe had infiltrated the network and locked down essential district operations.

The timing could have been worse—with schools closed for summer, there was no immediate disruption to instruction. But the financial system contained years of critical records, and the beginning of the school year was just weeks away.

The Ransom Demand

The attackers demanded payment in Bitcoin—initially 42 Bitcoin (valued at approximately $420,000 at the time). The ransom note was clear: pay up, or lose access to the district's financial data permanently.

The Board's Critical Decision

Superintendent Dr. Sarah Mitchell convened an emergency session with the board. They faced an agonizing choice:

- Pay the ransom: No guarantee the hackers would actually decrypt the files, and it would fund criminal activity
- Don't pay: Recovery could take months, potentially delaying the school year and losing years of financial records

What the Board Considered:

- Insurance Coverage: The district had cyber insurance, which could potentially cover ransom payment
- Law Enforcement Advice: State police strongly advised against paying, warning it encourages further attacks
- Recovery Timeline: IT staff estimated that rebuilding systems from scratch would take several months—well past the start of school
- Hacker Reputation: This particular ransomware group had a track record of actually decrypting systems after payment

- Student Impact: Delaying school opening would disrupt education for 5,000 students and create hardship for working families

The Decision: A Pragmatic Approach

After consulting with legal counsel, insurance representatives, and IT experts, Dr. Mitchell made a difficult recommendation to the board: authorize the cyber insurance company to negotiate and handle the payment. This was not a decision taken lightly.

Dr. Mitchell's rationale to the board: "The state police told us not to pay their ransom. But we needed our financial data back. Without it, we cannot operate. This is about weighing short-term and long-term costs to our students and community."

The board voted to give the cyber insurance company broad control over the technical and tactical response, including negotiation with the attackers.

The Negotiation and Resolution

The insurance company's cybersecurity team took charge:

- Negotiated the ransom down from 42 Bitcoin to approximately 20 Bitcoin (about $200,000)
- Made the payment in cryptocurrency as demanded
- Received the decryption key—and it worked. The district regained access to all financial systems

The insurance policy covered the ransom payment. The district's out-of-pocket costs were limited to the insurance deductible and some additional IT remediation expenses.

Communication Strategy

Throughout the incident, the board and superintendent maintained transparency with the community:

- Day 1: Immediate notification sent to staff explaining the situation and instructing them not to use work email
- Week 1: Public statement released explaining the ransomware attack, the district's response, and that an investigation was ongoing
- After Resolution: Board held public meeting explaining what happened, how it was resolved, and steps being taken to prevent future incidents

Key Communication Principle: The board chose to be honest about the difficult decision to pay the ransom, rather than trying to hide it. This transparency built community trust.

What the Board Did Right

- Had Cyber Insurance: The insurance policy was critical—covering not just the ransom but also providing expert negotiators and legal guidance
- Acted Quickly: Convened immediately and made decisions without unnecessary delay
- Consulted Experts: Relied on insurance company's cybersecurity team rather than trying to handle negotiations themselves

- Weighed All Options: Considered law enforcement advice, insurance coverage, recovery timelines, and student impact
- Maintained Transparency: Communicated honestly with staff and community throughout the crisis
- Made Pragmatic Decision: Chose the path that best served students and community, even when it meant going against law enforcement recommendations

Lessons Learned & Board Actions

Following the incident, the board took immediate action to strengthen the district's cybersecurity:

- Conducted complete forensic analysis to identify how hackers gained access
- Scrubbed all hard drives and rebuilt systems from clean images
- Implemented multi-factor authentication for all administrative accounts
- Enhanced email security with better phishing protection
- Upgraded backup systems to include offline, immutable backups
- Increased staff cybersecurity training—from annual to quarterly sessions
- Reviewed and increased cyber insurance coverage limits

Key Takeaways for Your Board

- There are no easy answers: The decision to pay or not pay a ransom involves difficult tradeoffs. This board made a pragmatic choice that prioritized students and operational continuity
- Cyber insurance is essential: Insurance provided not just financial coverage but also expert negotiators, legal counsel, and incident response guidance
- Timing matters: The summer timing reduced immediate educational disruption, giving the district time to respond without closing schools
- Transparency builds trust: Being honest about the difficult decision—rather than hiding it—maintained community confidence in board leadership
- Learn and improve: Every incident should drive immediate improvements to prevent recurrence
- Board leadership matters: Clear decision-making, expert consultation, and unified communication were critical to successful crisis management

The FBI's Guidance on Paying Ransoms

The FBI does not recommend paying ransoms because it encourages criminal activity. However, the FBI also states: "When businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers." Each district must weigh its unique circumstances.

Is Your District Prepared?

LBL ESD Cybersecurity offers CyberReady 365 services to help Oregon School Districts prepare for, respond to, and recover from cyber incidents.

CYBER INCIDENT:

A Board Member's Role

Essential guidance for Oregon School Board members on cybersecurity preparedness and response

Understanding Your Role

School board members play a critical governance role in cybersecurity—not as technical experts, but as strategic leaders responsible for oversight, policy, and resource allocation. When a cyber incident occurs, your decisions directly impact how quickly your district recovers and how well you maintain public trust.

Why Board-Level Involvement Matters

- Student Safety & Privacy: Cyber incidents can expose sensitive student data and disrupt critical services
- Financial Impact: Downtime, recovery costs, and potential ransom demands can quickly exceed budgets
- Educational Continuity: Incidents can halt instruction and disrupt operations for days or weeks
- Public Trust: How you respond determines community confidence in district leadership

Before an Incident: Preparedness

Essential Questions for Your Board

- Does our district have a written cyber incident response plan?
- When was it last reviewed and tested?
- Do we have adequate cyber insurance coverage?
- Who is our designated incident response coordinator?
- Are staff trained on cybersecurity awareness?
- Do we have reliable data backups that are tested regularly?

Board Responsibilities for Preparedness

- Policy Oversight: Approve cybersecurity policies and ensure they're regularly updated
- Budget Allocation: Fund adequate cybersecurity resources, staff, and training
- Insurance Review: Ensure cyber insurance aligns with district risk profile
- Regular Reporting: Request quarterly cybersecurity updates from IT leadership

During an Incident: Response

Immediate Board Actions

When notified of a cyber incident, the board should:

- Convene Promptly: Meet in executive session if necessary to receive briefings
- Activate Response Plan: Ensure the incident response plan is being followed
- Contact Insurance: Notify cyber insurance carrier immediately
- Authorize Resources: Approve emergency spending for response and recovery
- Legal Consultation: Engage legal counsel for liability and compliance guidance

Communication Strategy

Effective communication is critical during a cyber incident:

- Single Spokesperson: Designate one person to communicate publicly (usually Superintendent)
- Transparent Updates: Provide timely information to families and staff without compromising investigation
- Board Unity: Speak with one voice; avoid conflicting messages from individual board members
- Media Coordination: Work with communications team on press releases and media inquiries

What NOT to Do

- Do NOT make technical decisions—defer to IT and response team
- Do NOT discuss incident details on social media or with unauthorized parties
- Do NOT make ransom payment decisions without legal and insurance consultation
- Do NOT minimize or delay notification requirements

After an Incident: Recovery & Learning

Post-Incident Board Responsibilities

- Comprehensive Review: Request a detailed after-action report identifying what happened and why
- Process Improvements: Approve updates to policies and procedures based on lessons learned
- Investment Decisions: Fund necessary security improvements to prevent recurrence
- Staff Support: Ensure IT and leadership have resources and training they need
- Community Accountability: Communicate transparently about steps taken to strengthen security
-

Key Takeaways

- Cybersecurity is a governance responsibility, not just an IT issue
- Preparation and planning are far more valuable than reactive responses
- Board leadership and clear communication protect public trust during incidents
- Every incident is an opportunity to strengthen your district's resilience

For more information about CyberReady 365 and district support, visit lblcybersecurity.com

CYBER ESSENTIALS FOR SCHOOL BOARDS

Self-Assessment Checklist

Use this checklist to assess your district's cyber readiness and identify areas for improvement

#	Essential Practice	Yes	No	Unknown
GOVERNANCE & PLANNING				
1	Our district has a written cybersecurity policy approved by the board			
2	We have a documented cyber incident response plan that includes roles and responsibilities			
3	Our incident response plan has been tested or reviewed in the past 12 months			
4	The board receives regular cybersecurity updates (at least quarterly)			
5	We have designated a cybersecurity coordinator or lead			
INSURANCE & LEGAL				
1	Our district has cyber liability insurance coverage			
2	We understand what our cyber insurance covers and its limitations			
3	We have legal counsel available to advise on cyber incidents and data breaches			
4	We know our notification obligations under Oregon and federal data breach laws			
TECHNICAL CONTROLS				
1	We have reliable, tested data backups that are stored offline or off-site			
2	Multi-factor authentication is enabled for all administrative accounts			
3	Our district uses email filtering to block phishing and malicious attachments			
4	Software and systems are updated regularly with security patches			

#	Essential Practice	Yes	No	Unknown
5	We have endpoint protection on all district computers and devices			
TRAINING & AWARENESS				
1	All staff receive cybersecurity awareness training at least annually			
2	New employees receive cybersecurity training during onboarding			
3	Board members have received training on their cybersecurity responsibilities			
4	Students receive age-appropriate digital citizenship and safety education			
COMMUNICATION & RESPONSE				
1	We have a communication plan for notifying families about cyber incidents			
2	We know who to contact first if we suspect a cyber incident (IT, insurance, law enforcement)			
3	We have contact information for cyber incident response resources			
4	Our board knows its role and limitations during a cyber incident			

Scoring Your Assessment:

Count your 'Yes' responses:

20-24 Yes: Strong cyber readiness. Continue regular reviews and testing.
15-19 Yes: Good foundation, but gaps exist. Prioritize addressing 'No' and 'Unknown' items.
10-14 Yes: Significant vulnerabilities. Immediate action needed to improve cyber posture.
Below 10 Yes: Critical gaps. Request immediate cybersecurity evaluation and response plan development.

Next Steps: Request a Cyber Readiness Evaluation

LBL ESD Cybersecurity offers comprehensive assessments and support for Oregon school districts.

Resources & Contacts

In a cybersecurity incident, every minute counts. Having the right contacts ready ensures your agency can request help quickly, escalate issues to the right level, and meet reporting requirements. Below are trusted state, federal, and national resources for incident reporting and support.

PACE Reporting

When a cybersecurity incident occurs, members can reach out to the PACE teams for claims support, legal consultation, and incident assistance.

PACE (Property & Casualty Coverage for Education)
Claims Hotline (toll-free): 1-800-305-1736
Email for Claims: claims@sdao.com

State of Oregon
Cyber Security Services (EIS)

The State of Oregon's Enterprise Information Services (EIS) operates a Security Operations Center (SOC) to coordinate incident response across agencies.

Phone: (503) 378-3175
24-Hour SOC Hotline: (503) 378-5930
Address: 550 Airport Rd SE, Suite C, Salem, OR 97301

Resources & Contacts

CISA — Cybersecurity State Coordinator

Region 10 – Oregon
Your federal point of contact for infrastructure security coordination and incident response.

Name: Leslie Ann Kainoa
Email: Leslie.kainoa@cisa.gov
Phone: (503) 462-5626

You can also report incidents directly to CISA:
Reporting Site: cisa.gov/report
Direct Form: cisa.gov/forms/report
Email: report@cisa.gov
Phone: (888) 282-0870

The Cybersecurity and Infrastructure Security Agency offers toolkits, tabletop templates, ransomware response guides, and threat advisories.

Website: https://www.cisa.gov/topics/cybersecurity-best-practices

FBI — Cyber Incident Reporting

The FBI investigates cybercrime and supports victims during active incidents.
Reporting Site: ic3.gov
Direct Complaint Form: ic3.gov/Home/ComplaintChoice
Local Field Offices: fbi.gov/contact-us/field-offices
Portland Field Office (Oregon): (503) 224-4181

National Institute of Standards and Technology

The National Institute of Standards and Technology's Cybersecurity Framework provides a flexible, risk-based approach built around five core functions: Identify, Protect, Detect, Respond, and Recover.

Website: https://www.nist.gov/cyberframework
Document: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

K12 CYBER SAFETY TRAINING

DATA PROTECTION & PRIVACY

Protect your data at school and at home.

Prevent Data Loss

Regularly backing up your data ensures you won't lose important files due to cyberattacks, hardware failure, or accidental deletion. Use cloud storage or an external hard drive to keep your backups secure and accessible.

Protecting Personal Information

Oversharing on social media can expose personal details to cybercriminals and identity thieves. Be mindful of what you post and adjust privacy settings to limit who can see your information.

Don't Trust Unknown Devices

Plugging in unknown USB devices can expose your computer to malware and data theft. Only use trusted storage devices and consider disabling auto-run to prevent unauthorized access.

Stay Secure Online

Always use websites with HTTPS to ensure your data is encrypted and secure. Pay attention to browser security warnings, as they help you avoid malicious websites that can steal your information.

K12 CYBER SAFETY TRAINING

SAFE COMPUTING HABITS

Keep your Devices & Data Secure

Lock your Screen

Leaving your computer unlocked, even for a short time, can expose sensitive information to unauthorized users. Always lock your screen when stepping away to prevent data breaches and keep your workstation secure.

Restart Regulary

Regularly restarting your computer helps apply critical security updates, clear temporary files, and improve system performance. A simple reboot can fix vulnerabilities, preventing cyber threats from exploiting outdated software.

Use Secure Wi-Fi

Public Wi-Fi networks are often unsecured, making it easy for attackers to intercept your data. Use a VPN when connecting to public networks and ensure your Wi-Fi is password-protected with strong encryption.

Think Before Clicking

Malicious software often disguises itself as legitimate downloads or email attachments. Always verify the source of a file before downloading and avoid clicking suspicious links to keep your system safe from malware.

K12 CYBER SAFETY TRAINING

PHISHING SCAMS

Protect yourself at School and at Home

Urgent Language

Messages claiming your account will be locked or require immediate action.

Stay Calm – Scammers use urgency to pressure you into acting quickly. Always verify urgent requests through official channels.

Suspicious Links

Links that look odd or don't match the sender's website.

Verify Before Clicking – Hover over links to check their destination before clicking. Ensure the URL is legitimate.

Unexpected Attachment

Attachments you weren't expecting, especially with strange file types.

Think Before Opening – Do not open attachments from unknown or unverified senders. If in doubt, confirm with the sender directly.

Misspellings or Errors

Spelling mistakes or poor grammar in emails or messages.

Look for Red Flags – Professional organizations proofread their communications. Errors in emails may indicate a phishing attempt.

Request for Sensitive Information

Asking for passwords, Social Security numbers, or financial details.

Don't Share Sensitive Info – Legitimate organizations will never ask for sensitive information via email or text.

Generic Greetings

Messages starting with "Dear Customer" instead of using your name.

Check the Sender – Examine the sender's email address carefully. Scammers often use similar addresses to legitimate ones.

K12 CYBER SAFETY TRAINING

MALWARE AWARNESS

Protect yourself at School and at Home

Malware is harmful software that can damage your device or steal your personal information.

Here's how to stay safe:

Install Antivirus Software

Keep your device safe by using trusted antivirus programs to block threats.

Keep Software Updated:

Always update your system and apps to fix security weaknesses.

Avoid Unknown Links

Don't click on links or open attachments in emails or pop-ups from unknown sources.

Download Carefully

Only get software from trusted sites to avoid installing malware.

Turn on a Firewall

A firewall blocks dangerous traffic and helps keep malware out.

Backup Your Files

Save copies of important files so you can restore them if malware attacks.

K12 CYBER SAFETY TRAINING

RANSOMWARE AWARNESS

Protect yourself at School and at Home

Ransomware is harmful software that locks or encrypts your files and demands money to unlock them.

Here's how to stay safe:

Install Antivirus Software

Use trusted antivirus software to detect and block ransomware before it can infect your system.

Update Your Software

Keep your operating system and apps updated to fix security weaknesses that ransomware can exploit.

Back up Your Data

Regularly save your important files in secure, offline backups so you can restore them if ransomware attacks.

Be Careful with Emails:

Don't open attachments or click on links from unknown or suspicious sources, as they might contain ransomware.

Enable Multi-Factor Authentication:

Add an extra layer of protection to your accounts by using MFA to make it harder for attackers to get in.

Turn Off Macros and Scripts:

Disable these features in your email client and office software to avoid ransomware attacks through attachments.

Educate Yourself! Learn how to spot phishing emails and other tricks so you can stay safe online.

LBL CYBERSECURITY

CyberReady365

YEAR-ROUND CYBERSECURITY COVERAGE FOR SCHOOLS, CITIES & SPECIAL DISTRICTS

OVERVIEW

CyberReady365 provides always-on access to expert incident responders and proactive cybersecurity support. Our team coordinates identification, containment, recovery, and communications, helping your organization respond quickly, minimize impact, and meet insurer and regulatory requirements.

Beyond response, CyberReady365 equips your organization with readiness checklists, cyber awareness tools, and threat-intelligence updates, empowering your team to strengthen defenses and stay prepared before incidents occur.

INCIDENT RESPONSE SUPPORT

Immediate access to LBL's cybersecurity team for containment, recovery, and insurer or regulator coordination.

PROACTIVE PROTECTION

Use hours for proactive services — risk assessments, policy & insurance reviews, tabletop exercise seats, staff training, or leadership briefings.

24/7 EMERGENCY COVERAGE

If an incident strikes after hours, our team responds immediately. You'll never face a breach alone — day or night.

CyberReady365

CyberReady365 combines proactive protection, rapid response, and expert support in one simple annual plan — giving you peace of mind, coverage, and continuity every single day.

CONTINUITY MATTERS
Work never stops mid-incident.

PUBLIC-SECTOR EXPERTISE
Our responders understand education, local government, and insurance requirements.

PREDICTABLE BUDGET
Annual coverage replaces unplanned emergency costs.

PEACE OF MIND
Readiness, response, and recovery all in one plan.

#1 TARGET
Schools are now the #1 target for ransomware in the public sector.

PLAN AND PREPARE
Cyber incident response plans reduce downtime by 50% or more.

IDENTITY THEFT
One in eight U.S. children has experienced a compromise of their identity as part of a data breach in the past six years.

"Nearly half of ransomware reports in 2024 targeted critical infrastructure—threatening essential public services.

By partnering with us, your district gains access to expert-led cybersecurity strategies, proactive monitoring tools, and the essential support needed to protect your students, staff, and sensitive data. With comprehensive assessments, rapid recovery solutions, and ongoing educational initiatives, we ensure that your district remains secure in a constantly evolving digital landscape.

LBL CYBERSECURITY

lblcybersecurity.com

MORE SECURITY SOLUTIONS

CyberSentinel365
Continuous cybersecurity governance and oversight from seasoned experts. We help your organization stay compliant, strategic, and secure—every day of the year.

SentinelView360
A comprehensive NIST-aligned assessment that identifies gaps, benchmarks controls, and provides a clear roadmap to strengthen your cybersecurity posture.

ReadyLab360
Interactive, real-world tabletop exercises that build confidence, improve coordination, and prepare your team to respond effectively to cyber incidents.

Cyber Ready 365

LBL
CYBERSECURITY

lblcybersecurity.com