LBL

CYBERSECURITY

K-12 Cybersecurity Evaluation Report

Sasquatch School District

LBL CYBERSECURITY

EVALUATION SUMMARY

Executive Summary

This cybersecurity evaluation offers a districtwide overview of essential security practices across areas such as account security, password policies, multi-factor authentication, endpoint protection, backups, patch management, vulnerability scanning, and incident response. It supports strategic planning to improve student safety, data protection, and digital continuity.

Key Strengths

- Password policy includes minimum length and complexity requirements for staff.
- Endpoint Detection and Response (EDR) is deployed and centrally managed.
- Vendor-managed backups are in place.

Opportunities for Improvement

- Incident Response Plan exists, needs updating and testing.
- Phishing reports are not triaged using a defined process.
- No scheduled vulnerability scanning occurs.
- Offboarding user accounts is inconsistently enforced.
- Patch management is not centrally tracked.

Why This Matters

Cybersecurity gaps can lead to learning disruptions, exposure of sensitive data, and loss of community trust. Strengthening cybersecurity practices improves district cybersecurity resilience, supports instructional continuity, and protects critical digital assets which are critical in education environments.

LBL CYBERSECURITY
EVALUATION FINDINGS

Executive Summary for IT Leadership

Sasquatch School District engaged in a qualitative cybersecurity assessment aligned to NIST CSF 2.0 and NIST 800-53r5. Strengths were observed in backups and EDR deployment. Improvement opportunities exist in incident response planning, phishing response procedures, patch management, and account offboarding.

Technical Findings and Actionable Steps:

- Update and test a district-wide incident response plan.
- Standardize phishing reporting and triage.
- Enforce timely patching and track compliance.
- Implement a structured offboarding process tied to HR systems.
- Schedule recurring internal and external vulnerability scans.
- Implement MFA for all accounts and across all systems

1. Local Administrator Rights Management

- CSF 2.0: PR.AA-05
- NIST 800-53r5: AC-2, AC-3, AC-6
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "Have partially removed local administrator rights."
- Recommendation: Fully implement least-privilege enforcement; review local admin access quarterly and manage through centralized tools.

2. Password Policy

- CSF 2.0: PR.AA-01, PR.AA-02, PR.AA-03
- NIST 800-53r5: IA-2, IA-5, IA-8
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "A password policy exists requiring minimum length, special characters, and a 90-day expiration policy for staff only. Enforcement across systems is not fully standardized."
- Recommendation: Enforce standardized password policies across all systems; audit for compliance.

3. Multi-Factor Authentication (MFA)

- CSF 2.0: PR.AA-03, PR.AA-04
- NIST 800-53r5: IA-2, IA-8
- Summary: [Little to no evidence of consistent practice.] Evaluator noted: "MFA is only enabled for district administrator accounts."
- Recommendation: Expand MFA to all privileged and remote access accounts, including teaching staff where feasible.

4. Endpoint Protection / EDR

- CSF 2.0: PR.PS-05, DE.CM-09
- NIST 800-53r5: SI-3, SI-4
- Summary: [Strong practice.] Evaluator noted: "All systems have EDR installed and centrally managed. Admins receive email alerts for any endpoint issues."
- Recommendation: Maintain EDR coverage and ensure alerting/playbooks are tested periodically.

5. Patch Management

- CSF 2.0: PR.PS-01, PR.PS-02, PR.PS-03
- NIST 800-53r5: SI-2, CM-3, CM-4
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "Patching is occurring but there is no centralized tracking or reporting. Devices are updated manually by techs or by users. No service-level agreement on patch timelines."
- Recommendation: Develop SLAs for patch timelines and automate compliance reporting.

6. Backups

- CSF 2.0: PR.DS-11
- NIST 800-53r5: CP-9, CP-10
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "Backups are managed by our MSP."
- Recommendation: Conduct quarterly restore tests and retain logs as evidence.

LBL CYBERSECURITY
EVALUATION FINDINGS

7. Vulnerability Scanning

- CSF 2.0: ID.RA-01, ID.RA-03, ID.RA-06, DE.CM-09
- NIST 800-53r5: RA-5, SI-2
- Summary: [Little to no evidence of consistent practice.] Evaluator noted: "We aren't doing any vulnerability scanning right now."
- Recommendation: Schedule internal/external scans monthly; track remediation.

8. Critical Systems & Recovery Order

- CSF 2.0: ID.AM-05, RC.RP-01, RC.RP-03
- NIST 800-53r5: CP-2, CP-10
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "We know the recovery order internally, but it hasn't been formally documented or tied to a business impact analysis."
- Recommendation: Perform a business impact analysis and document recovery priorities and order.

9. Account and Access Management (Joiners/Movers/Leavers)

- CSF 2.0: PR.AA-01, PR.AA-05
- NIST 800-53r5: AC-2
- Summary: [Little to no evidence of consistent practice.] Evaluator noted: "Offboarding sometimes gets delayed if HR forgets to notify IT. No formal process exists for movers and role changes."
- Recommendation: Integrate HR-IT workflows and conduct quarterly access reviews

10. Phishing Reporting & Response

- CSF 2.0: DE.AE-06, RS.MA-01
- NIST 800-53r5: IR-4, IR-5, IR-6
- Summary: [Little to no evidence of consistent practice.] Evaluator noted: "Staff do forward suspicious emails to techs, but there's no defined response or tracking process."
- Recommendation: Create a standard phishing report path and define triage actions.

11. Security Awareness Training

- CSF 2.0: PR.AT-01, PR.AT-02
- NIST 800-53r5: AT-2, AT-3, AT-4
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "Cyber training inconsistent. Staff get onboarding training, but annual refreshers aren't always enforced or documented."
- Recommendation: Require annual cybersecurity training for all staff and track participation.

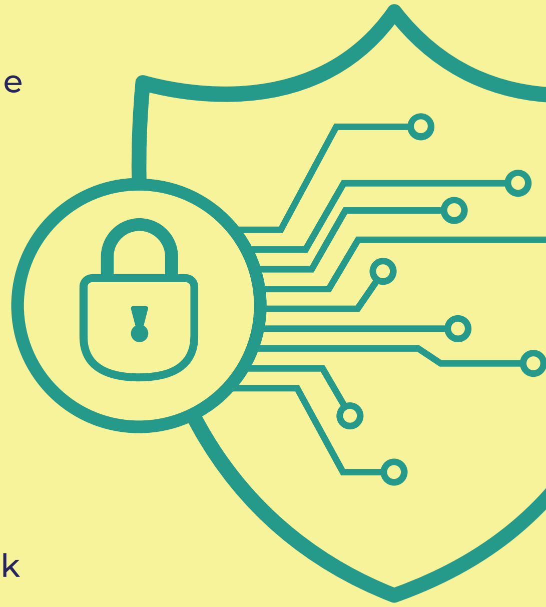
12. Incident Response Plan (IRP)

- CSF 2.0: RS.MA-01, RC.RP-02
- NIST 800-53r5: IR-1, IR-3, IR-8
- Summary: [Practice exists but may be inconsistently applied.] Evaluator noted: "Basic IRP exists. It outlines contacts but lacks clear roles and responsibilities."
- Recommendation: Formalize the IRP to include specific roles, response procedures, and escalation paths; conduct tabletop exercises to validate readiness.

LBL CYBERSECURITY

RECOMMENDATIONS / NEXT STEPS

1. Update and rehearse a district-wide incident response plan.
2. Implement phishing reporting workflows and triage protocols.
3. Schedule and document recurring vulnerability scans.
4. Track patching deadlines and validate completion.
5. Formalize HR-offboarding processes and conduct audits.
6. Standardize annual cybersecurity training and track participation.



CONCLUSION

Sasquatch Home School District's current cybersecurity posture is in the early stages of maturity, with some controls and processes showing positive movement. While there is evidence of effort and intent to improve, key gaps in areas such as incident response, phishing mitigation, access control, and patch management indicate a need for more structured and consistent implementation. Addressing these vulnerabilities will be critical to reducing risk and supporting a more secure, resilient learning environment.

LBL CYBERSECURITY

RECOMMENDATIONS / NEXT STEPS

How LBL Cybersecurity Can Help

Based on our recent consultation, we've identified several areas where LBL Cybersecurity can provide targeted, high-impact support to strengthen your overall security posture. Our team offers trusted tools, real-world expertise, and a partnership approach to help you move from assessment to action.

Internal Vulnerability Scanning

While many districts rely on external scans, internal threats often go unnoticed. We can provide monthly internal network scans that uncover misconfigurations, outdated systems, and other security gaps inside your environment. It's a proactive step that helps your team stay ahead of issues before they become incidents.

Cybersecurity Risk Assessment

Using SecurityStudio's proven framework, we'll evaluate your current cybersecurity posture across access, endpoint, data, and governance domains. You'll receive a clear, prioritized roadmap to guide improvements based on real-world risk.

Incident Response Services

Custom Tabletop Exercise

Preparedness doesn't happen by accident. Our district-specific tabletop simulation puts your leadership and tech teams through the paces of a real-world incident—phishing, malware, data compromise, or all of the above. With built-in systems integration, two expert facilitators, and a detailed after-action report, you'll gain clarity, coordination, and confidence in your response capabilities.

LBL CYBERSECURITY

RECOMMENDATIONS / NEXT STEPS

Cybersecurity Awareness Training

We offer in-person or virtual cybersecurity training tailored to your district's needs. Whether you're looking to train all staff on phishing and social engineering, or provide targeted sessions for leadership, tech, or business teams we make training practical, approachable, and impactful. We also offer simulated phishing to help reinforce habits and assess readiness.

Each of these services is designed to support your district's growth by building resilience, reducing risk, and aligning with national standards in a way that fits your people and systems.

We're here to help. Let us know what feels like the right next step, and we'll take care of the rest.

Erin Baston
Director of
Strategic Relations

☎ 503-602-5580

🌐 lblcybersecurity.com

✉ erin.baston@lblesd.k12.or.us

LINN BENTON LINCOLN
EDUCATION SERVICE DISTRICT

CYBER SAFETY SERVICE

The LBL Cyber Safety Service is specifically designed for K-12 districts, ensuring the safety and security of your educational environment. From proactive defense strategies to rapid recovery, each component of the service provides your district with the help you need to stay ahead of emerging cyber threats while fostering a culture of cybersecurity awareness among staff and students.

Assessment and Strategic Planning

Assess your district's cybersecurity posture, identify gaps, and develop a roadmap for improvement. This assessment aligns with industry best practices and insurance requirements, enabling ongoing enhancements to your cybersecurity strategies.

- **Insurance Compliance Review**
- **Cybersecurity Risk Assessment & Reports**
- **Mitigation Roadmap**
- **Third-Party Vendor Audits**

Threat Detection and Testing

Proactively detect and defend against emerging threats in your district by utilizing advanced tools and regular testing. We address the unique challenges K-12 districts face regarding data privacy, ransomware, and other cyber risks that target educational technologies.

- **Threat Landscape Report**
- **Internal Vulnerability Scans**
- **External Vulnerability Scans**
- **Penetration Testing**
- **Managed SIEM**

Incident Response and Recovery

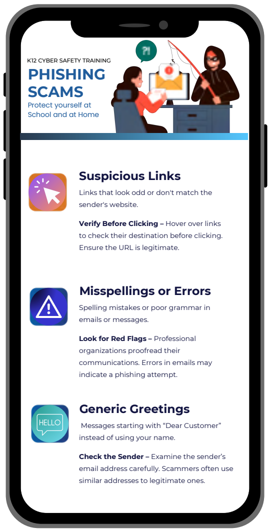
When a cybersecurity incident occurs, time is of the essence. Ensure your district can quickly recover from any breach with minimal downtime and disruption, leveraging expert incident management services and custom recovery plans.

Our IT team is trusted by more than 100 school districts across Oregon and Washington.

Education and Training

Foster a culture of cybersecurity awareness across your district by empowering staff and students with the knowledge and tools to prevent security incidents.

- **Best Practices Guides**
- **Annual Cyber Awareness Campaigns**
- **Role-Based Training**
- **In-Person Staff Training**
- **Tabletops and Custom Scenario**



K12 CYBER SAFETY TRAINING

PHISHING SCAMS

Protect yourself at School and at Home

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.

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.

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.

Meet our Cyber Team

Richard Thomas

Director of Cybersecurity

Tim Jones

Executive Information and Technology Officer

Triston Mikutaitis

Security Engineer

Jairo Beas

Security Technician

Jennifer Kessel

Senior Director of IT Services

Erin Baston

Director of Strategic Relations

Your Trusted IT Team

Our IT team consists of more than 35 skilled professionals, including 6 systems engineers, who are committed to providing our districts and clients with secure, dependable, and responsive technology solutions.

Our Commitment

We're more than a cybersecurity provider we're your partner in protecting what matters most. Our commitment is built on trust, transparency, and a deep understanding of your unique challenges. We deliver proven expertise, clear guidance, and responsive support to strengthen your security posture, minimize risk, and help you stay focused on your mission. With us, you're never navigating cybersecurity alone.

Dear Sasquatch School District,

Thank you for taking the time to meet with us for your complimentary cybersecurity consultation. We're grateful for the opportunity to support your team in this important work.

Cybersecurity in education is more than just firewalls and updates. It's about safeguarding the systems that allow students to learn, educators to teach, and communities to thrive. Every login, every database, every connection has the potential to impact a child's educational journey. That's why we take this work seriously.

Our team is deeply committed to protecting the environments our students depend on. Whether it's reviewing practices, identifying vulnerabilities, or helping you build a more resilient system, we're here to partner with you—not just as technicians, but as people who care about what you care about: safety, learning, and trust.

Thank you again for your time and for the work you do each day. It's our privilege to walk alongside you as you strengthen your systems and continue to serve your community.
Sincerely,

Tim Jones
Executive Information & Technology Officer
Linn Benton Lincoln ESD

Thank You!

For partnering with us

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