M.A. Polce
IT & CYBERSECURITY

A Strategic Resource for IT Directors and Personnel

K-12 Cybersecurity Planning Worksheet

As your district finalizes its budget for the upcoming year, it's essential to ensure that cybersecurity investments align with the most pressing security needs. This document will help you assess whether your budget effectively covers key areas critical to protecting student data, staff, and infrastructure.

Instructions: For each security area listed, rate how well your current budget addresses it on a scale from 0 to 3 (0 = not at all, 3 = fully covered). At the end, you will be given rating that breakdowns the strength of you plan and if there are areas needing additional investment. Use these insights to assist in your budget preparation and, if needed, to present a data-driven case to district leadership on where additional funding is needed to reduce risk and enhance your security posture.

Threat Detection & Response

Funds have been allocated for continuous, 24x7 monitoring and rapid response to cyber threats. The solution actively hunts threats to neutralize them in their earliest stages.

0 1 2 3

Security Testing & Assessments

Your budget accounts for at least one simulated cyberattack to evaluate your network's resilience, and there is funding available for periodic security assessments to measure your district's overall cyber health.

0 1 2 3

Compliance & Strategic Guidance

Resources are allocated for accessing strategic cybersecurity leadership, specifically for expert guidance on meeting regulatory requirements and shaping long-term security initiatives.

0 1 2 3

Access Controls & Identity Management

Your budget accounts for the full implementation of MFA to secure critical systems and accounts. There is also funding for identity and access management solutions to enforce least-privilege access.

0 1 2 3

Vulnerability Management

0	1	2	3
○	○	○	○

You have budgeted for regular assessments to identify and address security weaknesses. A component of your solution involves detecting outdated software, missing patches, and misconfigurations. You also have resources dedicated to remediating vulnerabilities when discovered.

Security Awareness & Training

0	1	2	3
○	○	○	○

Your budget accounts for ongoing training to keep staff and faculty informed about emerging threats. Trainings include phishing simulations and awareness programs to reduce human risk.

Network & Endpoint Security

0	1	2	3
○	○	○	○

Your budget includes investments in network and endpoint security solutions for staff and student devices that protect against unauthorized access and advanced threats.

Backup & Disaster Recovery

0	1	2	3
○	○	○	○

There is funding for measures that ensure critical data is backed up and can be restored in the event of an attack. This includes having a disaster recovery/business continuity plan and a solution to test and validate your plans.

Incident Response Readiness

0	1	2	3
○	○	○	○

There is a dedicated budget for incident response planning and readiness. This includes funds to perform tabletop exercises or simulations to ensure preparedness and access to rapid expert support when an incident occurs.

Your Security Plan Score

Your score provides a data-driven snapshot of how well your district's cybersecurity budget aligns with essential protection measures. Use these insights to identify gaps, prioritize security needs, guide strategic planning, communicate risks, and, if needed, advocate for additional funding.

Your Net Total*
0

***Important:** The auto-calculation feature of this document may not function properly in certain web browsers. If you encounter issues, you may need to calculate your score manually. For optimal performance, we recommend using the Adobe Acrobat Reader app or enabling its browser extension.*

Score Breakdown & Next Steps

Rating	Explanation	How to Use This Data
0 – 6: High Risk – Critical Gaps Present	Your current budget leaves significant areas of your cybersecurity framework underfunded or completely unaddressed, increasing the district's exposure to cyber threats. Essential protections may be severely lacking.	Clearly identify the most critical gaps in your security plan and assess how each weakness increases the risk of a breach—potentially disrupting learning, exposing sensitive student data, and leading to financial and legal consequences. Prioritize funding for solutions that address the highest-risk areas first.
7 – 15: Moderate Risk – Substantial Gaps Exist	Your budget covers some critical security areas, but significant weaknesses remain. Certain protections may be partially implemented or insufficiently funded, leaving your district vulnerable to emerging threats.	Highlight the areas where partial coverage is creating unnecessary risk. Consider how strategic investments—such as enhancing monitoring capabilities, increasing staff training, or improving response readiness—can provide better protection and long-term cost savings by reducing incident-related expenses.
16 – 24: Managed Risk – Some Gaps to Address	Your district has a solid foundation for cybersecurity, with key protections in place. However, some areas may be underfunded or not fully aligned with best practices, limiting your ability to proactively defend against threats.	Plan to make targeted improvements in areas that could elevate your security posture. Collect data on evolving cyber risks affecting K-12 institutions and determine how additional investment in areas like proactive testing or security awareness can enhance resilience and compliance.
25 – 27: Strong Security Posture – Well-Funded & Proactive	Your budget is well-aligned with security best practices, covering the essential protections needed to safeguard student data, staff, and infrastructure. You are likely implementing proactive strategies to reduce risk and maintain compliance.	Reinforce the importance of maintaining this level of funding to district leadership. Cyber threats evolve rapidly, so continued investment is necessary to sustain protection. Consider budgeting for additional enhancements, such as advanced threat detection or security automation, to stay ahead of future risks.

Optimize Your Cybersecurity Budget for Maximum Protection

If your score is lower than you expected or if you're unsure whether your current budget allocations fully address these critical security areas—we're here to help. Schedule a complimentary consultation to have our team assess your district's cybersecurity strategy, fill gaps, and ensure your investments provide maximum protection and value.

Let's work together to ensure your budget covers the essentials this year and build a plan for future security investments—contact us today to get started.

Contact Us

info@mapolce.com

315.338.0388

mapolce.com

M.A. Polce

Schedule a Consultation