THE ROADMAP TO DEVELOPING A K-12 DISTRICTWIDE CYBERSECURITY ECOSYSTEM

An Action Guide for Building Cabinet Buy-In

project tomorrow

NACC

K-12 National Advisory Council on Cybersecurity

iboss

PRIMARY AUTHORS:

Lenny Schad
Board Chair NACC
CITO Houston ISD (Retired)
Co-Founder K12 Strategic Advisory Group

Julie A. Evans, Ed.D.
CEO, Project Tomorrow

WITH SUPPORT FROM THE NACC BOARD:

Lenny Schad
Julie A. Evans, Ed.D.
Don Wolff, M.Ed.
Lesley Bruinton, APR
Mark Racine
Greg Ottinger, Ed.D.
Richard Quinones
Marlon Shears
Thomas Nawrocki
Rick Gaisford
Lakshmi S. Visvanathan

NATIONAL MISSION SPONSOR:

REPRESENTED BY:

Richard Quinones
NACC Senior Advisor
iboss SVP Public Education

Introduction

With cyber-attacks it's not a matter of if, but when. It will happen but the severity/extent of the attack, response, and remediation will show how well the district is prepared for it. With our district response plans everyone is involved and informed. I believe being upfront and honest in the event of an attack should be the general disposition of every district.

District Technology Leader (IL)

Welcome to the **Action Guide for Building Cabinet Buy-In on Cybersecurity**, a comprehensive resource designed to guide school districts in establishing robust, district-wide cybersecurity protocols.

This **Action Guide** has been developed under the auspices of the **K-12 National Advisory Council on Cybersecurity (NACC)** and represents the reality that the necessity for this toolkit has never been more urgent. As we navigate the complexities of an increasingly digital education landscape, the threat of cyberattacks looms larger, impacting not just the operational aspects of our schools but also the safety and privacy of our students.

The digital transformation in education has brought unprecedented opportunities for learning and collaboration. However, it has also exposed districts to new vulnerabilities, from data breaches and phishing scams to ransomware attacks that can cripple an entire school system's infrastructure. Recent findings documented in Project Tomorrow's annual report on cybersecurity in K-12 education underscore the critical challenges that districts face. A staggering 74% of technology leaders and similar proportions across other leadership roles report knowing a district that has faced a cyberattack within the past year, with 21% admitting their districts have been directly affected.[1]

Despite this awareness, there exists a significant gap between the recognition of cyber threats and the actions taken to mitigate them within district leadership ranks. This disconnect between concern and prepared implementation strategies is a major focus of this Action Guide. Our goal is to help you bridge this gap, shifting the narrative from mere awareness to proactive, strategic action with districtwide shared responsibility and accountability. But that work starts with you as the district technology leader.

[1] Project Tomorrow & iboss, "K12 Cybersecurity Speak Up Findings 2023"

Why an enterprise level approach is imperative today

This **Action Guide** advocates for a paradigm shift towards enterprise ownership of cybersecurity, where responsibility transcends the IT department to encompass the entire leadership team. This approach is not merely a recommendation but an imperative strategy to:

- Develop an integrated defense strategy that protects critical educational and administrative resources.
- Ensure strategic resource allocation to support robust cybersecurity measures, reflecting their high priority.
- Enhance the effectiveness of incident response and recovery efforts across all operational levels.
- Cultivate a district-wide culture of cybersecurity awareness, encouraging proactive security behaviors.
- Maintain compliance with increasing regulatory demands and safeguard the trust invested by students, parents, and the community.

Throughout this **Action Guide**, you will find data-driven insights, actionable strategies, and real-world applications that reflect the collective wisdom and practices recommended by cybersecurity experts. From setting up a cybersecurity framework to engaging with the community and enhancing staff training, each section is designed to equip district leaders with the tools needed to implement an effective cybersecurity strategy. Central to this process is to understand how to translate cybersecurity terminology and vocabulary so that it resonates with key leadership roles within your cabinet leadership and stimulates actions that are beyond what you can do yourself within the IT Department. While IT leadership is critical for implementing appropriate cyber protections, these efforts are insufficient on their own to appropriately safeguard district assets and protect data privacy. That work transcends the IT shop and must be embraced by all departments and divisions.

Our goal is clear: to empower K-12 districts to not only defend against cyber threats but to thrive in a digital era with confidence and resilience. Let this **Action Guide** be your roadmap as you advance the narrative from cybersecurity awareness to district-wide resilience. Together, we can transform the challenge of cybersecurity into an opportunity for strengthening our educational environments.

How to use this Action Guide

Our recommendation is to use this **Action Guide** as you would use a map when on a journey. The process of building district cabinet leadership buy-in for shared responsibility and accountability for cybersecurity is truly a journey. That buy-in will not happen overnight, even if your district unfortunately has a cyber-attack on your infrastructure. As part of this journey, it is

your task to decide if you, your leadership team, and your district is up for a transformation regarding your current cybersecurity preparations, or that you will be satisfied with making appropriate changes to current policies and programs. The key is to understand the difference between organizational change and organizational transformation. Chief Information Officers across all sectors often find themselves at this crossroads within their organization. In articulating the difference between change and transformation, a CIO Insights article identified the divergence in this way:

> *"Change is a response to external influences, where modifying day-to-day action achieves desired results. Transformation is about modifying core beliefs and long-term behaviors—sometimes in profound ways—to achieve the desired results."*[2]

This **Action Guide** can certainly support your change efforts, but it will be most effective for you if you embrace a journey of transformation.

Action Guide Structure:

The **Action Guide** is divided into three levels with multiple action steps within each level.

Level One defines the role and responsibilities necessary for today's district CIO or CTO to be highly effective in terms of addressing the cybersecurity threats that are circling around your district.

Level Two focuses on how to develop enhanced awareness within your district leadership team about real-world cyber incident vulnerabilities within K-12 districts. The approach in Level 2 is to translate our "technology speak" into language that will resonate with various leadership titles and roles, including Superintendent, Chief Financial Officer, Chief Academic Officer, and others. The resonance is built upon understanding the priorities of these officers and "what is waking them up in the middle of the night" as priorities. In most cases, they will not say that cybersecurity per se is one of those "wake-up issues," but the implications of a cyber attack will directly affect their priorities. To help with your discussions with colleagues, we have provided you with a **Glossary of Terms**.

Level Three builds upon what you have established in a new relationship with your colleagues in the cabinet based upon a shared vision for your district and a recognition of how a seemingly disparate set of priorities may converge around cybersecurity. With Level 3 we provide action steps to implement shared responsibility and accountability around cybersecurity. Some of these action steps may fall within the IT Department, but many others will require cabinet buy-in because the actions will live within various other departments and divisions.

[2] https://www.cioinsight.com/news-trends/the-difference-between-change-and-transformation/

Our recommendation is that you start with **Level One – CIO Responsibilities** and use the checklist within that section to understand the scope of your role for cybersecurity within your district.

Then, review the **Level Two** sections, which are structured to address specific roles and titles within a typical district leadership team. Think about each of these important roles within your district. What are your colleagues' critical priorities that are potentially "waking them up in the middle of the night?" What issues are top of mind for them every day within their responsibilities? Using our priority chart, identify what you think those "wake-up" priorities are. Connecting the dots between those priorities and cybersecurity preparation will help your colleagues better understand the need for a districtwide ecosystem for cybersecurity preparation. Select one colleague within your leadership team to approach with a discussion on how a cyberattack may impact their priorities. Remember this is a journey, not a sprint, to build cabinet wide buy-in for a district level cybersecurity ecosystem. These discussions may take time and need to evolve over the school year.

After building a new cybersecurity-focused relationship with your colleagues, select specific actions within the **Level Three** section as goals for the upcoming school year. These goals will require you to work closely with your colleagues in other departments and divisions. We have provided you with a strategic action chart to help organize your thoughts and plans. It is critical that you develop that collaborative working relationship with those colleagues before launching into specific action steps that require them to potentially re-think current policies or operational procedures. They need to fully embrace a new "why" around cybersecurity and its potential impact on their department or division.

Finally, engage with us to share your victories and potentially your short-term setbacks. We see this **Action Guide** as a living document and aim to continue to enhance it based upon your real-world experiences using it. Please contact us with your ideas at innovation@tomorrow.org.

GLOSSARY of TERMS

1. **Audit:** A systematic review or assessment of something. In the context of cybersecurity, it refers to the evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.
2. **Authentication:** The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
3. **Business Continuity Planning (BCP):** A proactive process to ensure that critical services continue during disruptions, including emergencies from technology failures, natural disasters, or human actions. Unlike disaster recovery, which focuses on restoring IT functions, BCP maintains all essential business operations.
4. **Compliance:** Adherence to laws, regulations, guidelines, and specifications relevant to the organization.
5. **Crisis Communication Plan:** A strategy developed to communicate with various parties when an issue that threatens the operations or credibility of a company or entity arises, especially during an immediate crisis.
6. **Cyber Insurance:** A product that is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery from a cyber-related security breach or similar events.
7. **Cyberbullying:** The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.
8. **Cybersecurity:** The protection of computer systems, networks, and data from digital attacks, unauthorized access, or damage.
9. **Cybersecurity Framework:** A structured set of guidelines and best practices to manage cybersecurity risks.
10. **Data Breach:** An incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.
11. **Data Privacy:** The aspect of information technology that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.
12. **DDoS (Distributed Denial of Service):** An attack that disrupts normal web traffic and overwhelms a website with a flood of internet traffic.
13. **Digital Citizenship:** Responsible use of technology by students and staff, including the norms of appropriate, responsible, and healthy behavior related to current technology use.
14. **Disaster Recovery Plan:** A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

15. **FERPA (Family Educational Rights and Privacy Act):** A federal law that protects the privacy of student education records.
16. **Governance:** The methods, processes, and relations by which an organization is controlled and directed.
17. **Incident Response Plan:** A set of instructions to help IT staff detect, respond to, and recover from network security incidents.
18. **Malware:** Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
19. **Network Security:** Measures to protect the usability and integrity of your network and data. It includes both hardware and software technologies.
20. **Parental Engagement in Cybersecurity:** The involvement of parents in understanding and supporting cybersecurity measures at school and at home to protect children.
21. **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.
22. **Regulatory Requirements:** Mandates imposed by a governing body that must be followed to achieve compliance with a regulation.
23. **School-wide Cybersecurity Policy:** Guidelines and procedures developed at the school level to ensure the cybersecurity of the school's networks, devices, and data.
24. **Security Audits (Educational Context):** Systematic evaluations conducted to assess how well a school adheres to a set of established security criteria, specifically around protecting educational data and technology.
25. **Stakeholders:** Persons or organizations who have an interest or concern in a business, often with the power to affect or be affected by the business outcomes.
26. **Strategic Planning:** An organization's process of defining its strategy or direction, and making decisions on allocating its resources to pursue this strategy.
27. **Tabletop Exercises:** Discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation.

Chapter 1

Level One

Understanding your role and responsibilities as a K-12 District CIO today

As your district CIO you have multiple roles and responsibilities to manage and protect your district's technology assets. This section is meant to provide you with some new insights about those roles and responsibilities. If appropriate use our checklist to identify your current roles and responsibilities, and/or the activities and priorities that you feel would be most appropriate for you today and tomorrow. In this section, the **Action Guide** describes 10 common responsibility areas for a District CIO relative to cybersecurity. Each description includes an example and then a set of action stems to achieve the goals of that responsibility level.

The 10 common responsibility areas reviewed here include:

A. Technology Management and Infrastructure Security
B. Data Security and Privacy Compliance
C. Strategic IT Planning and Implementation
D. Cybersecurity Leadership and Staff Training
E. Adoption of a Cybersecurity Framework
F. Disaster Recovery Planning and Testing
G. Collaboration with External Cybersecurity Experts
H. Emerging Technologies and Innovation
I. Vendor Management and Security
J. Community Cybersecurity Education and Engagement

A. Technology Management and Infrastructure Security

Introduction:

As the Chief Information Officer, you are responsible for overseeing the technological infrastructure of the school district, ensuring that all systems are secure, efficient, and capable of supporting educational and administrative needs. Effective management of IT resources is crucial to protect against cyber threats and ensure seamless operation.

- Incident: System downtime due to outdated or poorly maintained infrastructure.
- Example: Server failures during critical testing periods.
- Scenario: Network vulnerabilities exploited due to lack of regular updates.
- Consequence: Disruptions in educational processes and potential data breaches.

Action Steps:

1. Implement a robust IT asset management system to track and maintain all hardware and software resources efficiently.
    - Challenges:
        - Ensuring comprehensive coverage of all IT assets across multiple campuses.
        - Keeping the asset management system updated with real-time changes and upgrades.
2. Regularly update and patch all systems to protect against known vulnerabilities.
    - Challenges:
        - Coordinating downtime for updates without interrupting school operations.
        - Ensuring all devices, including those used by remote learners, are consistently updated.
3. Conduct periodic security audits of the IT infrastructure to identify and mitigate risks.
    - Challenges:
        - Allocating resources for in-depth audits without straining the IT department's capacity.
        - Implementing changes based on audit findings in a timely and effective manner.

B. Data Security and Privacy Compliance

Introduction:

Protecting the privacy and security of student and staff data is a primary responsibility for the CIO. Compliance with federal and state regulations, such as FERPA, is essential to maintain trust and avoid legal repercussions.

- Incident: Unauthorized access to sensitive student records.
- Example: Breach of personal data due to insecure storage solutions.
- Scenario: Phishing attacks leading to compromised employee credentials.
- Consequence: Legal penalties and loss of trust from parents and stakeholders.

Action Steps:

1. Develop and enforce strict data security policies that comply with legal standards.
    - Challenges:
        - Balancing the need for accessibility with security requirements.
        - Training staff to adhere to security policies without compromising their workflow.
2. Implement advanced encryption and security measures for all data storage and transmission.
    - Challenges:
        - Introducing new technologies without disrupting existing IT systems.
        - Maintaining performance and usability while enhancing security measures.
3. Regularly review and update compliance practices to align with evolving regulations.
    - Challenges:
        - Keeping abreast of changes in cybersecurity laws and educational privacy regulations.
        - Quickly adapting systems and policies to meet new compliance requirements.

C. Strategic IT Planning and Implementation

Introduction:

Strategic planning in IT is crucial to align technology initiatives with the educational goals of the district. As the CIO, leading the development and execution of IT strategies ensures that technological capabilities support the district's long-term objectives.

- Incident: IT projects failing to meet educational or operational needs.
- Example: Over-investment in technologies that do not align with teaching goals.
- Scenario: Lack of coordination between IT initiatives and educational strategies.
- Consequence: Wasted resources and missed opportunities for enhancing educational outcomes.

Action Steps:

1. Develop a long-term IT strategy that supports the district's educational vision.
    - Challenges:
        - Ensuring stakeholder engagement and buy-in for strategic IT initiatives.
        - Aligning IT projects with educational outcomes and budget constraints.
2. Facilitate cross-departmental collaboration to ensure IT projects support diverse needs.
    - Challenges:
        - Bridging the communication gap between IT staff and educational personnel.
        - Managing project priorities and resources across different departments.
3. Monitor and adapt IT strategies based on feedback and technological advancements.
    - Challenges:
        - Continuously evaluating the effectiveness of IT strategies against set goals.
        - Remaining flexible to pivot or adjust strategies in response to feedback and new opportunities.

D. Cybersecurity Leadership and Staff Training

Introduction:

Leadership in cybersecurity is essential for cultivating a culture of security awareness throughout the district. The CIO must lead by example, promoting cybersecurity best practices and ensuring that all staff are trained to protect their digital environments.

- Incident: Widespread malware infection due to lack of staff awareness.
- Example: Social engineering attacks that trick staff into revealing sensitive information.
- Scenario: Inadequate response to security alerts by untrained staff.
- Consequence: Significant breaches leading to data loss and system compromise.

Action Steps:

1. Lead the development and regular updates of a comprehensive cybersecurity training program for all staff.
    - Challenges:
        - Creating engaging and effective training materials that cater to a range of technical skill levels.
        - Scheduling regular training sessions without disrupting daily school activities.
2. Establish a security incident reporting and response system that is easy for all staff to use.
    - Challenges:
        - Encouraging staff to promptly report incidents without fear of reprisal.
        - Ensuring the incident response system is efficient and effective in mitigating threats.
3. Promote a culture of security-first thinking across all levels of the district.
    - Challenges:
        - Integrating security practices into daily routines without creating resistance or hindrance.
        - Measuring the impact of cultural change on the district’s overall security posture.

E. Adoption of a Cybersecurity Framework

Introduction:

Implementing a standardized cybersecurity framework is crucial for structuring and managing cybersecurity efforts systematically across the district. This framework provides a guideline for assessing and improving the ability to prevent, detect, and respond to cyber incidents.

- Incident: Inconsistencies in cybersecurity measures across different schools within the district.
- Example: Varying levels of security protocols leading to uneven protection.
- Scenario: Lack of a unified approach to addressing common cybersecurity threats.
- Consequence: Increased vulnerability and inefficiencies in handling cybersecurity issues.

Action Steps:

1. Select and adapt a recognized cybersecurity framework, such as NIST (National Institute of Standards and Technology) or ISO (International Standards Organization), that best fits the district's needs.
    - Challenges:
        - Tailoring the framework to accommodate the specific operational and educational contexts of the district.
        - Ensuring that the selected framework aligns with existing IT and security policies.
2. Train IT staff and relevant stakeholders on the chosen cybersecurity framework to ensure proper implementation and adherence.
    - Challenges:
        - Developing effective training programs that communicate complex framework concepts in an understandable manner.
        - Achieving consistent implementation across all schools and departments.
3. Regularly review and update the cybersecurity framework implementation to keep pace with new technologies and emerging threats.
    - Challenges:
        - Staying informed about updates to the cybersecurity framework and relevant cybersecurity trends.

- Integrating new best practices and standards into the existing framework without disrupting established protocols.

F. Disaster Recovery Planning and Testing

Introduction:

Developing and maintaining a comprehensive disaster recovery plan is essential for ensuring that the district can quickly recover from cyber incidents with minimal disruption to educational activities.

- Incident: Critical data loss due to a cybersecurity breach.
- Example: Server crash resulting in the loss of instructional materials and student records.
- Scenario: Ineffective recovery efforts leading to prolonged system downtime.
- Consequence: Significant disruption of teaching activities and administrative functions.

Action Steps:

1. Develop a detailed disaster recovery plan that includes specific steps for data recovery, system restoration, and communication during and after an incident.
    - Challenges:
        - Ensuring the disaster recovery plan covers all critical systems and data.
        - Making the plan accessible and understandable to all staff members who need to execute it.
2. Conduct regular disaster recovery drills to test the effectiveness of the plan under simulated crisis conditions.
    - Challenges:
        - Organizing comprehensive drills that accurately reflect potential cyber incidents without causing undue disruption or alarm.
        - Analyzing drill outcomes and making necessary adjustments to the disaster recovery plan.
3. Evaluate and update the disaster recovery plan regularly based on drill feedback and evolving cybersecurity landscapes.
    - Challenges:

- Keeping the disaster recovery plan current with technological and organizational changes.
- Encouraging continuous improvement based on drill experiences and new cybersecurity practices.

G. Collaboration with External Cybersecurity Experts

Introduction:

Engaging with external cybersecurity experts and organizations can provide additional expertise and resources that enhance the district's ability to protect against and respond to cyber threats.

- Incident: Advanced persistent threats that exceed the internal capabilities of the district's IT staff.
- Example: Targeted attacks by sophisticated cybercriminal groups.
- Scenario: Need for specialized cybersecurity expertise not available within the district.
- Consequence: Potential for significant breaches that are difficult to detect and mitigate with internal resources alone.

Action Steps:

1. Establish partnerships with cybersecurity firms that offer expert consultation, threat monitoring, and response services.
    - Challenges:
        - Selecting a firm that offers services tailored to the specific needs of an educational environment.
        - Balancing the cost of external services with budget constraints.
2. Participate in cybersecurity consortiums and collaborative groups that share threat intelligence and best practices.
    - Challenges:
        - Actively engaging in consortium activities and applying learned practices to the district's context.
        - Ensuring data shared within these groups is handled securely and respects privacy concerns.

3. Regularly consult with cybersecurity advisors to review and enhance the district's security posture.
    - Challenges:
        - Integrating external advice with internal IT strategies and operations.
        - Keeping advisory interactions productive and focused on actionable outcomes.

H. Emerging Technologies and Innovation

Introduction:

Staying abreast of emerging technologies is crucial for CIOs to leverage new tools that can enhance learning and operational efficiency while ensuring cybersecurity. As technology evolves, so do the opportunities and threats, making it essential for the CIO to be proactive in integrating innovative solutions safely.

- Incident: Missing opportunities for enhanced learning due to outdated technology.
- Example: Failure to implement AI-driven personalized learning systems that could adapt to student needs due to cybersecurity concerns.
- Scenario: Competitors in the educational sector adopting blockchain for secure record-keeping, while the district lags behind.
- Consequence: The district falls behind in educational technology, impacting student outcomes and competitive positioning.

Action Steps:

1. Conduct ongoing research and pilot tests with new technologies before full-scale implementation.
    - Challenges:
        - Balancing the potential benefits of new technologies with inherent security risks.
        - Allocating resources for pilot programs without disrupting existing IT operations.
2. Establish a technology review board that includes IT experts and educators to evaluate the potential educational and operational impact of new technologies.
    - Challenges:

- Ensuring the board has a diverse range of expertise to make well-rounded decisions.
- Keeping the board's work aligned with the district's strategic goals and cybersecurity standards.

3. Develop partnerships with technology developers to tailor emerging technologies to the specific needs and constraints of the educational environment.
    - Challenges:
        - Negotiating with vendors to modify their products to meet the district's security requirements.
        - Integrating new technologies into the current IT infrastructure seamlessly.

I. Vendor Management and Security

Introduction:

Managing relationships with technology vendors is key to ensuring that the products and services they provide meet the district's cybersecurity standards. Effective vendor management protects the district from potential security vulnerabilities associated with third-party services.

- Incident: Data breach originating from a vendor's compromised system.
- Example: A cloud service provider experiencing a security flaw that affects the district's data.
- Scenario: A software update introduces vulnerabilities due to insufficient security testing.
- Consequence: Compromise of sensitive data, leading to trust issues and financial liabilities.

Action Steps:

1. Develop a comprehensive vendor security policy that all technology providers must adhere to.
    - Challenges:
        - Creating policies that are thorough yet flexible enough to accommodate a variety of technology solutions.

- Ensuring vendors comply with stringent security requirements without inflating costs.

2. Regularly audit vendor security practices to ensure compliance with the district's cybersecurity standards.
    - Challenges:
        - Conducting thorough audits without straining relationships with vendors.
        - Responding effectively to audit findings that require immediate action.
3. Incorporate security requirements into the procurement process to ensure all new contracts meet established cybersecurity criteria.
    - Challenges:
        - Updating procurement policies to include comprehensive cybersecurity evaluations.
        - Training procurement staff to recognize and enforce cybersecurity standards during vendor selection.

J. Community Cybersecurity Education and Engagement

Introduction:

Engaging the wider school community in cybersecurity education helps build a shared responsibility for digital safety. By educating parents, students, and community members, the CIO can extend cybersecurity awareness beyond the school walls, creating a safer digital environment for everyone.

- Incident: Increase in cyber threats targeting students and families.
- Example: Parents falling for phishing scams that lead to unauthorized access to school systems.
- Scenario: Widespread malware infections at home affecting students' devices used for schoolwork.
- Consequence: Broader network vulnerabilities and potential breaches affecting school operations.

Action Steps:

1. Host community cybersecurity workshops and seminars to educate about common threats and safe practices.

- Challenges:
    - Designing engaging content that caters to a broad audience with varying levels of technical knowledge.
    - Encouraging participation from the broader community, including busy parents and guardians.

2. Develop online resources and toolkits for families to improve their home cybersecurity.
    - Challenges:
        - Ensuring resources are accessible and understandable for non-technical users.
        - Keeping online materials up-to-date with the latest cybersecurity practices and threats.
3. Collaborate with local businesses and government agencies to promote community-wide cybersecurity initiatives.
    - Challenges:
        - Coordinating initiatives that align with the goals of various stakeholders.
        - Measuring the effectiveness of community engagement efforts in improving cybersecurity awareness.

Your Level One Self-Assessment:

This self-assessment checklist can be helpful in many ways. Use it to get clarity about your own accountability. It can also be helpful to increase the awareness of your executive leadership about the various tasks and actions needed to secure your district infrastructure. You can also use the checklist to learn more about your goals and the potential obstacles or barriers to those goals. This is your document. Use it in a way that supports your work and your vision.

Recommended Action	Doing this already	Would like to do this but cannot due to constraints – *what is that constraint?*	No desire to take on this responsibility today
Technology Management and Infrastructure Security			
Implement a robust IT asset management system.			
Regularly update and patch all systems to protect against known vulnerabilities.			
Conduct periodic security audits of the IT infrastructure to identify and mitigate risks.			
Data Security and Privacy Compliance			
Develop and enforce strict data security policies that comply with legal standards.			
Implement advanced encryption and security measures for all data storage and transmission.			
Regularly review and update compliance practices to align with evolving regulations.			
Strategic IT Planning and Implementation			
Develop a long-term IT strategy that supports the district's educational vision.			
Facilitate cross-departmental collaboration to ensure IT projects support diverse needs.			
Monitor and adapt IT strategies based on feedback and technological advancements.			
Cybersecurity Leadership and Staff Training			
Lead the development and regular updates of a comprehensive cybersecurity training program for all staff.			

Establish a security incident reporting and response system that is easy for all staff to use.			
Promote a culture of security-first thinking across all levels of the district.			
Adoption of a Cybersecurity Framework			
Select and adapt a recognized cybersecurity framework such as NIST or ISO that best fits the district's needs.			
Train IT staff and relevant stakeholders on the chosen cybersecurity framework to ensure proper implementation and adherence.			
Regularly review and update the cybersecurity framework implementation to keep pace with new technologies and emerging threats.			
Disaster Recovery Planning and Testing			
Develop a detailed disaster recovery plan that includes specific steps for data recovery, system restoration, and communication during and after an incident.			
Conduct regular disaster recovery drills to test the effectiveness of the plan under simulated crisis conditions.			
Evaluate and update the disaster recovery plan regularly based on drill feedback and evolving cybersecurity landscapes.			
Collaboration with External Cybersecurity Experts			
Establish partnerships with cybersecurity firms that offer expert consultation, threat monitoring, and response services.			
Participate in cybersecurity consortiums and collaborative groups that share threat intelligence and best practices.			
Regularly consult with cybersecurity advisors to review and enhance the district's security posture.			
Emerging Technologies and Innovation			
Conduct ongoing research and pilot tests with new technologies before full-scale implementation.			
(continued on page 21)			

Establish a technology review board that includes IT experts and educators to evaluate the potential educational and operational impact of new technologies.			
Develop partnerships with technology developers to tailor emerging technologies to the specific needs and constraints of the educational environment.			
Vendor Management and Security			
Develop a comprehensive vendor security policy that all technology providers must adhere to.			
Regularly audit vendor security practices to ensure compliance with the district's cybersecurity standards.			
Incorporate security requirements into the procurement process to ensure all new contracts meet established cybersecurity criteria.			
Community Cybersecurity Education and Engagement			
Host community cybersecurity workshops and seminars to educate about common threats and safe practices.			
Develop online resources and toolkits for families to improve their home cybersecurity.			
Collaborate with local businesses and government agencies to promote community-wide cybersecurity initiatives.			

Chapter 2

Level Two

Develop enhanced awareness within your district leadership team about the real world of cybersecurity vulnerabilities within K-12 districts by speaking to the concerns and priorities of your colleagues.

By its very nature, to be highly effective, cybersecurity preparations should be integrated within all aspects of your district's operations and instructional delivery. Thus, your colleagues across all divisions and departments are intrinsically involved with cybersecurity – even if they might not realize or articulate that today. Building a districtwide ecosystem where shared responsibility and accountability are part of the culture requires a new type of technology leadership. In Level Two of your journey, our recommendation is that you use your technology translation skills to help your colleagues see how cybersecurity impacts their priorities. To support that work, we have included information about potential priorities for different roles or titles within your district leadership team. A sampling of priorities is provided for the following roles and titles:

a) Superintendent
b) School Board Member
c) Communication Officer/Public Relations Director
d) Chief Financial Officer
e) Chief Academic Officer
f) Risk Management
g) School Building Leader/Principal

To prepare for your discussion with these colleagues about how cybersecurity impacts their responsibilities and priorities, we recommend reviewing these priority lists and identifying the top 2-3 priorities that apply for your colleagues.

A. Your **SUPERINTENDENT**: their priorities and potential connections to cybersecurity

Review the following list of Superintendent priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate "speaking their language" connections with your Superintendent when making the case for increased awareness and the need for a districtwide approach.

Student Safety Issue

Introduction:

As a superintendent, the safety of your staff and students, especially in today's digital world, is a major concern. Cyber threats are real and can significantly impact students' well-being by exposing them to risks like identity theft and cyberbullying. These threats can have enduring effects on both their personal lives and academic success. Therefore, a robust approach to cybersecurity is essential to protect students and ensure their safety online.

- **Incident:** A data breach leading to student personal information leakage, potentially exposing them to identity theft.
- **Example**: Cyberbullying or harassment facilitated through compromised school networks or systems.
- **Scenario**: Hackers manipulating school data, resulting in incorrect student records or compromised student welfare.
- **Consequence**: Risk of legal action and loss of trust from parents due to inadequate protection of student information.

Educational Continuity

Introduction:

Maintaining continuity in education relies heavily on digital infrastructure, which is vulnerable to cyber attacks. As a superintendent, ensuring robust cybersecurity measures will help minimize disruptions and uphold the integrity of educational delivery.

- **Incident**: Ransomware attacks that lock out access to digital learning platforms, causing significant disruptions in teaching.

- **Example**: DDoS (Distributed Denial of Service) attacks crippling school networks, making online resources inaccessible.
- **Scenario**: Malware infecting school computers, leading to loss of coursework and teaching materials.
- **Consequence**: Significant instructional time loss and potential compromise of students' academic progress.

Sound Financial Strategies and Operations

Introduction:

Cyber incidents can result in significant financial strain due to recovery costs and compliance penalties. Effective cybersecurity investment is not only proactive risk management but also a financially sound strategy for school districts.

- **Cost**: Expenses related to cybersecurity breach response, including IT forensic investigations and legal consultations.
- **Fines**: Penalties for non-compliance with data protection laws, like FERPA violations.
- **Insurance**: Increased premiums for cyber insurance due to poor cybersecurity practices.
- **Consequence**: Substantial unforeseen expenses impacting the school district's budget and potential redirection of funds from educational programs to cover these costs.

District Reputation

Introduction:

The reputation of your school district is a cornerstone of community trust and student enrollment. As a superintendent, prioritizing cybersecurity helps safeguard against the reputational damage that can follow cyber incidents.

- **Public Trust**: Loss of trust from parents and the community if student data is compromised.
- **Media Coverage**: Negative media attention following a cyber incident, impacting the school's public image.
- **Enrollment**: Potential decrease in student enrollment due to concerns over data safety and security.

- **Consequence**: Long-term damage to the school district's reputation, potentially affecting future student enrollment and community support.

Regulatory Compliance

Introduction:

Superintendents must navigate the complex landscape of regulatory requirements to protect student information. Effective compliance not only mitigates legal risks but also reinforces the district's commitment to student privacy.

- **Legal Requirement**: Ensuring compliance with FERPA for the protection of student education records.
- **Policy Adherence**: Developing and enforcing policies for data handling and privacy in line with state and federal laws.
- **Audit Readiness**: Maintaining readiness for audits on data protection and privacy practices.
- **Consequence**: Legal penalties and sanctions for non-compliance with education and data privacy laws, leading to additional financial burdens and administrative challenges.

Strategic Planning

Introduction:

Cybersecurity must be integrated into the strategic planning process to protect and future-proof educational technologies. As a superintendent, leading this integration can significantly enhance operational resilience and educational capabilities.

- **Risk Assessment**: Conducting regular cybersecurity risk assessments to identify and mitigate potential threats.
- **Long-term Investments**: Allocating budget for long-term cybersecurity measures, like secure infrastructure and software.
- **Future-Proofing**: Planning for the integration of emerging technologies with a focus on security.
- **Cybersecurity Framework Adoption**: Adopting and customizing a recognized cybersecurity framework to guide the district's cybersecurity policies and procedures.

- **Consequence**: Lack of preparedness for future cyber threats, leading to increased vulnerability and potential systemic failures in the school district's IT infrastructure.

Leadership and Culture

Introduction:

The culture of cybersecurity within a school district starts at the top. As a superintendent, your commitment to cybersecurity leadership sets the tone for the entire organization.

- **Top-Down Approach**: Superintendent leading by example in promoting cybersecurity awareness and practices.
- **Policy Leadership**: Establishment and enforcement of clear cybersecurity policies and protocols.
- **Culture of Awareness**: Creating a school culture where every staff member and student is aware of cybersecurity best practices.
- **Enterprise Cybersecurity Governance**: Establishing a governance framework that integrates cybersecurity into all levels of the school district.
- **Incident Response**: Developing a robust incident response plan that includes clear roles and responsibilities.
- **Consequence**: Creation of a reactive rather than proactive cybersecurity environment, leading to increased risk of breaches and inefficient response strategies.

Resource Allocation

Introduction:

Effective resource allocation for cybersecurity is vital for defending against threats and ensuring the safety of your school district's digital environment. As a superintendent, it's crucial to ensure that the district's cybersecurity resources are not only sufficient but also strategically deployed to efficiently address evolving cybersecurity threats. This involves managing the budget and resources carefully to maintain robust digital infrastructure and protect sensitive data.

- **Budget Allocation:** Dedicating a portion of the annual budget to cybersecurity initiatives and improvements.
- **Training Resources**: Investing in regular training for staff and teachers on cybersecurity awareness and practices.

- **Technology Upgrades**: Allocating funds for upgrading IT infrastructure to enhance security.
- **Appropriate Staffing**: Investing in knowledgeable and skilled cybersecurity personnel to manage the district's strategies.
- **Consequence**: Inadequate defenses against evolving cyber threats due to insufficient investment in cybersecurity resources and technologies.

Community Engagement

Introduction:

Community trust and participation are essential components of a superintendent's role. Engaging with parents and local stakeholders in your district's cybersecurity efforts not only raises awareness but also cultivates a collaborative approach to digital safety. Such partnerships are crucial for reinforcing the community's trust in the school's ability to protect their children both physically and digitally. Building strong relationships around cybersecurity efforts enhances transparency and boosts community confidence in the school district's commitment to safeguarding digital environments.

- **Parental Communication:** Regularly informing parents about the school's efforts in cybersecurity and how they can contribute.
- **Community Workshops:** Hosting community workshops on digital safety and cybersecurity awareness.
- **Collaboration with Local Law Enforcement:** Partnering with local law enforcement for cyber threat intelligence and response planning.
- **Consequence:** Weakened community confidence and cooperation, leading to challenges in implementing effective cybersecurity measures and policies.

Professional Development

Introduction:

Investing in your staff's cybersecurity training is essential for reducing your district's vulnerability to cyber threats. As a superintendent, prioritizing such educational opportunities demonstrates your commitment to excellence and continuous improvement, enhancing your team's ability to safeguard your educational environment effectively.

- **Staff Training Programs:** Regular cybersecurity training sessions for teachers and administrative staff.

- **Cybersecurity Workshops:** Organizing workshops on specific topics like phishing, password security, and safe browsing.
- **Certifications and Courses:** Encouraging staff to pursue cybersecurity certifications and courses for professional development.
- **Tabletop Exercises:** Conducting tabletop exercises to simulate cyber attack scenarios to help staff understand their roles during an incident and improve overall readiness.
- **Consequence:** Staff and faculty remain ill-equipped to recognize and respond to cybersecurity threats, increasing the likelihood of successful cyber attacks.

B. Your **SCHOOL BOARD**: their priorities and potential connections to cybersecurity

Review the following list of School Board priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate "speaking their language" connections with your School Board when making the case for increased awareness and the need for a districtwide approach.

Regulatory Compliance and Legal Oversight

Introduction:

School boards must ensure that the district complies with all applicable cybersecurity laws and regulations. This oversight is crucial to avoid legal penalties and ensure that student data privacy is maintained according to federal and state laws.

- **Incident:** Non-compliance with data protection laws resulting in fines.
- **Example:** Failure to comply with FERPA or state-specific privacy regulations.
- **Scenario:** An audit reveals lapses in data protection protocols.
- **Consequence:** Financial penalties and increased scrutiny from regulators, damaging public trust.

Cybersecurity Governance and Oversight

Introduction:

As school board members, overseeing the implementation of effective cybersecurity measures is crucial to safeguard the district's information assets. Cyber threats not only pose risks to student and staff data but can also jeopardize the entire district's operations. Effective governance is needed to ensure that cybersecurity policies and procedures are comprehensive and adhered to.

- **Incident:** Breaches resulting in the exposure of sensitive district operational data.
- **Example:** Targeted phishing attacks aimed at board members to gain unauthorized access.
- **Scenario:** Inadequate response to a detected intrusion, leading to escalated access breaches.
- **Consequence:** Legal repercussions and severe reputational damage affecting the district's standing and stakeholder trust.

Strategic Cybersecurity Leadership

Introduction:

School board members must champion cybersecurity not just as a technical issue, but as a strategic and integral part of the district’s overall operational integrity. Leadership in cybersecurity is crucial in setting the tone at the top and embedding a culture of security awareness throughout the district.

- **Incident:** High-level breaches due to overlooked security policies.
- **Example:** Mismanagement of user access rights leading to data leaks.
- **Scenario:** Failure to update and enforce security policies reflecting new technologies in classrooms.
- **Consequence:** Disruptions in educational delivery and loss of student trust and safety.

Financial Oversight and Cybersecurity Budgeting

Introduction:

Financial oversight is key to ensuring that adequate resources are allocated to cybersecurity initiatives. School boards play a critical role in budgeting for cybersecurity, balancing fiscal responsibility with the need to protect district assets.

- **Incident:** Budget constraints leading to underfunded cybersecurity initiatives.
- **Example:** Insufficient investment in updated technology and security measures.
- **Scenario:** An unexpected cybersecurity incident strains the district's financial resources.
- **Consequence:** Inadequate response capabilities leading to greater long-term costs.

Community Engagement and Public Communication

Introduction:

Engaging with the community on cybersecurity issues builds trust and reinforces the importance of protecting student data. School boards should lead initiatives to inform and involve parents, students, and the community in cybersecurity efforts.

- **Incident:** Community concerns following a data breach.
- **Example:** Misinformation spreading in the community about the district's handling of a cyber incident.
- **Scenario:** Parents expressing concerns about data privacy and security at public meetings.
- **Consequence:** Loss of community trust and potential decreases in student enrollment.

C. Your **COMMUNICATION OFFICER:** their priorities and potential connections to cybersecurity

Review the following list of Communication Officer priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate "speaking their language" connections with your Communication Officer when making the case for increased awareness and the need for a districtwide approach.

Crisis Communication and Incident Response

Introduction:

The Communication Department plays a crucial role in managing the district's response to cybersecurity incidents. Effective communication strategies are essential to maintain trust and manage public perception during and after cyber incidents.

- **Incident:** Disclosure of a data breach affecting student records.
- **Example:** A ransomware attack that disrupts school operations.
- **Scenario:** Unauthorized access to confidential communications.
- **Consequence:** Potential panic among parents, students and employees and damage to the district's reputation.

Public Relations and Media Management

Introduction:

Managing the narrative in the media is critical after a cybersecurity incident. The Communication Department must proactively engage with the media to shape public understanding and reassure stakeholders of the district's handling of the situation.

- **Incident:** Media leaks of a cybersecurity incident before the district is prepared to announce it.
- **Example:** Inaccurate reporting on the scope of a data breach.
- **Scenario:** Intense media scrutiny following a high-profile cyber attack.
- **Consequence:** Erosion of public trust and confidence in the district's ability to protect student information.

Internal Communications and Employee Awareness

Introduction:

Ensuring that all staff are informed and educated about cybersecurity practices is vital to prevent breaches from within. The Communication Department must facilitate ongoing internal communications that promote a culture of cybersecurity awareness.

- **Incident:** An employee inadvertently sharing sensitive information due to lack of awareness.

- **Example:** Phishing emails that successfully trick staff into revealing login credentials.
- **Scenario:** Widespread non-compliance with security protocols among employees.
- **Consequence:** Internal threats and breaches, potentially leading to external attacks.

Strategic Communication Planning

Introduction:

Strategic communication is essential for ensuring that all cybersecurity messages align with the district's overall communication goals and policies. The Communication Department must plan and coordinate these messages to reinforce the district's commitment to cybersecurity.

- **Incident:** Mixed messages sent to the public during a cybersecurity incident.
- **Example:** Conflicting statements from different departments about the impact of a cyber attack.
- **Scenario:** A lack of a unified communication strategy leading to confusion and panic.
- **Consequence:** Damage to the district’s credibility and authority in managing cybersecurity issues.

Collaboration with IT and Cybersecurity Teams

Introduction:

Effective collaboration between the Communication Department and IT/cybersecurity teams is crucial to ensure accurate and timely dissemination of information regarding cybersecurity.

- **Incident:** Delayed communication response due to poor coordination with IT.
- **Example:** Inaccurate information released due to misunderstandings of technical details.
- **Scenario:** IT department implements new security software without informing the Communication Department.
- **Consequence:** Miscommunications leading to ineffective use of new security tools and policies by staff.

Digital Content Security

Introduction:

The security of digital content is paramount, especially content that is sensitive or confidential. The Communication Department must implement and manage security measures to protect digital communications.

- **Incident:** Hacking of digital content repositories.
- **Example:** Unauthorized access to scheduled but unpublished press releases.
- **Scenario:** Leakage of sensitive information through compromised digital channels.
- **Consequence:** Loss of control over the narrative and potential legal issues.

D. Your **CHIEF FINANCIAL OFFICER:** their priorities and potential connections to cybersecurity

Review the following list of Chief Financial Officer priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate “speaking their language” connections with your Chief Financial Officer when making the case for increased awareness and the need for a districtwide approach.

Financial Risks and Impacts

Introduction:

As a CFO, you must proactively manage the financial risks associated with cyber threats, which can lead to direct financial losses, undermine the district's credit rating, and necessitate costly recovery measures. Effective cybersecurity strategies reduce the potential for financial disruption and preserve the district’s financial health.

- **Incident:** Unauthorized transactions due to compromised financial systems.
- **Example:** Ransomware demanding payment to release encrypted financial records.
- **Scenario:** Phishing scams leading to significant financial fraud.
- **Consequence:** Immediate financial loss and long-term damage to the district's financial stability.

Insurance and Risk Transfer

Introduction:

Managing cybersecurity risks through insurance is a strategic approach that helps mitigate financial exposure from cyber incidents. Proper insurance coverage transfers significant risks to insurers, providing financial relief in case of cyberattacks and helping maintain operational stability.

- **Coverage Evaluation:** Regular assessment of insurance needs based on the current cyber risk landscape.
- **Policy Optimization:** Negotiating terms to include comprehensive coverage for cyber incidents.
- **Risk Management:** Integrating insurance into the broader risk management strategy to ensure financial stability.
- **Consequence:** Inadequate insurance coverage could lead to significant uncovered financial losses.

Cost Management and ROI

Introduction:

Effectively managing the costs associated with cybersecurity investments and demonstrating their return on investment are crucial. These practices ensure that the district's cybersecurity measures are not only cost-effective but also contribute to long-term financial stability.

- **Financial Planning:** Aligning cybersecurity investments with fiscal strategies and objectives.
- **ROI Analysis:** Developing metrics to quantify the financial benefits of cybersecurity initiatives.
- **Budget Impact:** Evaluating the impact of cybersecurity spending on overall financial planning.
- **Strategic Prioritization:** Aligning cybersecurity investments with the district's financial priorities.
- **Consequence:** Potential underfunding of necessary cybersecurity measures if ROI is not clearly demonstrated.

Vendor Management

Introduction:

Vendors often have access to sensitive information, making stringent cybersecurity requirements essential in vendor contracts. Effective vendor management ensures that third parties adhere to the same security standards as the district, mitigating potential risks from data breaches.

- **Vendor Security Requirements:** Establishing high cybersecurity standards for vendor selection.
- **Contractual Compliance:** Ensuring vendor contracts include enforceable cybersecurity clauses.
- **Audit and Review:** Regularly auditing vendor compliance to security standards.
- **Consequence:** Security lapses in vendor practices can lead to significant data breaches and financial losses.

Disaster Recovery and Business Continuity

Introduction:

Cyber incidents can significantly disrupt critical financial operations, making effective disaster recovery and business continuity planning essential. These plans ensure that financial services can continue with minimal disruption, safeguarding the district's operational and financial integrity.

- **Recovery Strategy:** Developing actionable and specific recovery plans for financial systems.
- **Continuity Preparation:** Ensuring continuity of critical financial functions in any incident.
- **Plan Testing:** Regularly testing and updating recovery plans to adapt to new threats.
- **Consequence:** Inadequate disaster recovery planning can prolong system downtime, impacting financial operations and compliance.

Governance and Policy Management

Introduction:

Robust governance of cybersecurity policies ensures that they are practical, enforceable, and reflective of the latest cybersecurity practices. Effective policy management is essential for maintaining compliance with regulatory standards and safeguarding against cyber threats.

- **Policy Development:** Creating and updating cybersecurity policies that reflect current threats and regulatory requirements.
- **Stakeholder Involvement:** Engaging various stakeholders in policy creation and execution.
- **Compliance Monitoring:** Setting up mechanisms to monitor and enforce policy adherence.
- **Consequence:** Inconsistent policy enforcement can lead to vulnerabilities and non-compliance issues.

Employee Training and Awareness

Introduction:

Employees often represent the first line of defense against cyber threats. Regular training and awareness initiatives are crucial to equip staff with the knowledge and skills needed to identify and respond to cybersecurity challenges effectively.

- **Targeted Training:** Focusing on cybersecurity risks specific to financial operations.
- **Engagement Tactics:** Utilizing engaging and relevant training methods to maximize effectiveness.
- **Update Frequency:** Keeping training up-to-date with the latest cybersecurity threats and countermeasures.
- **Consequence:** Without effective training, staff may inadvertently become security risks, increasing the likelihood of successful cyber attacks.

E. Your **CHIEF ACADEMIC OFFICER:** their priorities and potential connections to cybersecurity

Review the following list of Chief Academic Officer priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate "speaking their language" connections with your Chief Academic Officer when making the case for increased awareness and the need for a districtwide approach.

Educational Continuity and Cybersecurity

Introduction:

As the Chief Academic Officer, ensuring the continuity of educational services in the face of cyber threats is critical. Cyber incidents can disrupt teaching and learning platforms, potentially halting academic activities. A robust cybersecurity strategy is essential to safeguard these educational technologies.

- **Incident:** A cyberattack that disrupts online learning platforms.
- **Example:** Ransomware infection that locks out access to digital curriculum resources.
- **Scenario:** Phishing attacks targeting faculty, leading to compromised system access.
- **Consequence:** Interruptions in instructional time and potential data loss affecting student learning outcomes.

Crisis Communication Plan

Introduction:

Developing a robust crisis communication plan tailored to the academic setting is vital to maintaining the trust and safety of students and staff during cybersecurity incidents.

- **Incident:** Miscommunication during a cybersecurity incident leading to panic among students and parents.
- **Example:** Delayed or unclear instructions on data breaches affecting student records.
- **Scenario:** Inadequate communication infrastructure fails to provide timely updates to stakeholders.
- **Consequence:** Loss of trust from parents, students, and potential legal complications.

Cybersecurity in Curriculum Development

Introduction:

Integrating cybersecurity education into the curriculum supports the development of digitally literate students who understand the risks and responsibilities of the digital world. As CAO, guiding curriculum development to include cybersecurity awareness is vital.

- **Incident:** Students encountering cyber threats due to a lack of awareness.
- **Example:** Sharing of sensitive information through unsecured digital platforms by students.
- **Scenario:** Use of compromised software or applications in classroom settings.
- **Consequence:** Potential breaches of student data and exposure to online risks.

Professional Development in Cybersecurity for Educators

Introduction:

Empowering educators with the knowledge and tools to teach and manage cybersecurity within their classrooms is crucial. As CAO, promoting ongoing professional development in cybersecurity is key to enhancing educators' proficiency and confidence in using and teaching digital tools safely.

- **Incident:** Educators lacking confidence in using technology tools securely.
- **Example:** Accidental disclosure of sensitive information during virtual classes.
- **Scenario:** Inadequate response to student inquiries about cybersecurity due to a lack of teacher training.
- **Consequence:** Reduced effectiveness of digital learning environments and potential risks to student safety online.

Student Data Protection

Introduction:

Protecting student data is a paramount concern, especially with the increasing use of digital platforms for education. As the CAO, ensuring that all student information is securely managed according to the highest standards of data protection is critical to maintaining trust and compliance.

- **Incident:** Unauthorized access to student records.
- **Example:** Data breaches involving personal student information.
- **Scenario:** Inadequate security protocols leading to data vulnerabilities.
- **Consequence:** Loss of student and parental trust, potential legal repercussions.

Community Outreach and Engagement on Cybersecurity

Introduction:

Building community awareness and involvement in cybersecurity efforts is essential to create a supportive environment for district-wide cybersecurity initiatives. The CAO plays a crucial role in leading these outreach efforts.

- **Incident:** Community members' lack of awareness contributing to cybersecurity risks.
- **Example:** Parents unknowingly compromising school systems through unsafe online practices.
- **Scenario:** Community-wide phishing attacks targeting school network users.
- **Consequence:** Increased vulnerability to cyber attacks affecting the entire school community.

Cybersecurity Integration into Student Support Services

Introduction:

Integrating cybersecurity awareness into student support services ensures that students not only understand how to protect themselves online but also know where to seek help if needed. This integration helps build a resilient student body equipped to handle the digital challenges of the modern world.

- **Incident:** Students encountering cyberbullying or other online harms.
- **Example:** Students sharing too much personal information online.
- **Scenario:** Lack of awareness about digital citizenship among students.
- **Consequence:** Students becoming victims of online scams, identity theft, or cyberbullying.

F. Your **RISK MANAGEMENT OFFICE:** their priorities and potential connections to cybersecurity

Review the following list of Risk Management Office priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate "speaking their language" connections with your Risk Management Office when making the case for increased awareness and the need for a districtwide approach.

Cyber Risk Assessment and Mitigation

Introduction:

The Risk Management Office plays a crucial role in identifying, assessing, and mitigating cybersecurity risks that could impact the district's operations and reputation. Effective risk management strategies are essential to safeguard the district from potential cyber threats.

- **Incident:** Discovery of vulnerabilities in the school's IT infrastructure.
- **Example:** Identification of weak points in the network that could be exploited by malware.
- **Scenario:** An annual risk assessment reveals insufficient protection against ransomware attacks.
- **Consequence:** Potential financial and operational disruptions, along with data loss.

Policy Development and Compliance

Introduction:

Developing robust cybersecurity policies and ensuring compliance are key responsibilities of the Risk Management Office. These policies must align with legal requirements and best practices to protect district data and technology systems.

- **Incident:** Non-compliance with data protection regulations.
- **Example:** Failure to adhere to state and federal cybersecurity regulations.
- **Scenario:** Audits find gaps in compliance leading to legal and financial repercussions.
- **Consequence:** Fines, legal actions, and damage to the district's credibility.

Cybersecurity Insurance Management

Introduction:

Managing cybersecurity insurance is critical to mitigate financial risks associated with cyber incidents. The Risk Management Office must ensure that the district's insurance coverage is adequate to cover potential losses from cyber threats.

- **Incident:** A cyberattack results in significant data loss and recovery costs.
- **Example:** A data breach exposes sensitive student information, triggering claims under cybersecurity insurance.
- **Scenario:** Inadequate insurance coverage limits the district's ability to recover financially from a cyberattack.
- **Consequence:** Financial strain and potential cuts to critical district programs.

Incident Response and Crisis Management

Introduction:

Effective incident response and crisis management capabilities are crucial for the Risk Management Office to swiftly address and mitigate the impacts of cybersecurity incidents. The office must coordinate responses to ensure minimal disruption to district operations.

- **Incident:** A successful cyberattack disrupts critical district services.
- **Example:** A phishing attack compromises several administrative accounts.
- **Scenario:** Slow or uncoordinated response exacerbates the impact of the attack.
- **Consequence:** Prolonged recovery times and increased costs, along with eroded stakeholder trust.

Cross-Departmental Collaboration

Introduction:

Cybersecurity is a district-wide concern that requires collaboration across various departments. The Risk Management Office must foster cooperation to ensure that cybersecurity measures are integrated seamlessly across all operations.

- **Incident:** Lack of coordination leads to inconsistent cybersecurity practices.

- **Example:** IT department implements software updates that are not communicated to other departments.
- **Scenario:** Fragmented approach to cybersecurity across the district.
- **Consequence:** Inefficiencies and vulnerabilities in the district's cybersecurity posture.

G. Your **SCHOOL BUILDING LEADER/PRINCIPAL:** their priorities and potential connections to cybersecurity

Review the following list of School Building Leader/Principal priorities and select 2-3 that you believe are most important for your district and leadership team. Focus your follow-up on discussions about cybersecurity within the district on these priorities and use appropriate "speaking their language" connections with your School Building Leader/Principal when making the case for increased awareness and the need for a districtwide approach.

Cybersecurity Awareness and School Culture

Introduction:

As a principal, fostering a culture of cybersecurity awareness within your school is essential. Cyber threats can compromise student safety and privacy, disrupt educational processes, and damage the school's reputation. Creating an environment where everyone understands their role in maintaining cybersecurity is crucial.

- **Incident:** Unauthorized access to student information systems.
- **Example:** Phishing attacks aimed at school staff.
- **Scenario:** Teachers or students inadvertently compromising systems through unsafe practices.
- **Consequence:** Loss of sensitive data, leading to mistrust among parents and students.

Security of Educational Technologies

Introduction:

Educational technologies are integral to modern teaching and learning but can introduce significant risks if not properly secured. As a principal, ensuring that all digital tools and platforms are secure protects both students and staff from potential cyber threats.

- **Incident:** Breach in a learning management system.
- **Example:** Unauthorized software installations leading to vulnerabilities.
- **Scenario:** Compromise of network security through outdated software.
- **Consequence:** Disruption of educational activities and potential data breaches.

Training and Development for Staff and Students

Introduction:

Training staff and students to recognize and respond to cybersecurity threats is key to preventing potential breaches. As a principal, you need to ensure that everyone in your school is equipped with the knowledge to protect themselves and the school's digital assets.

- **Incident:** Staff member falling victim to a phishing scam.
- **Example:** Students sharing passwords or sensitive information online.
- **Scenario:** A device infected with malware due to downloading unauthorized content.
- **Consequence:** Spread of malware across the school network, leading to data loss and system downtime.

Incident Response and Crisis Management

Introduction:

In the event of a cybersecurity incident, having a clear and effective response plan is crucial. As a principal, you are responsible for leading the response efforts, ensuring that the impact on school operations is minimized, and that normal activities can resume as quickly as possible.

- **Incident:** Ransomware attack locking out access to critical systems.
- **Example:** Student data breach requiring immediate action to secure systems and notify affected parties.
- **Scenario:** Discovery of unauthorized access to the school's administrative records.
- **Consequence:** Operational disruptions, legal implications, and damage to the school's reputation.

Parent and Community Engagement in Cybersecurity

Introduction:

Engaging parents and the wider community in the school's cybersecurity efforts is critical to creating a secure and supportive environment for students both at school and at home. As a principal, you play a key role in educating and involving parents in protecting their children's digital lives.

- **Incident:** Parents unknowingly compromising their children's digital security through unsafe home computing practices.
- **Example:** Use of unsecured networks by students at home leading to potential breaches.
- **Scenario:** Widespread phishing attacks targeting families of students.
- **Consequence:** Extended impact of cybersecurity threats affecting students beyond school, damaging trust within the school community.

Chapter 3

Level Three

For each colleague, collaboratively establish new action steps to implement shared responsibility and accountability around cybersecurity.

This Level Three section includes potential action steps for the same roles identified in Level Two. Under each role, we have identified a set of priorities. For each priority, there is a set of action steps that could address those role-specific imperatives, and the identification of some challenges that would need to be addressed as well.

Select 2-3 of the identified key priorities for each colleague and related action steps as a first step set of goals. For each colleague, build out this strategic action chart to use as your guide. See the first example that we developed for you for a Superintendent. This example can be helpful to understand how to complete this table and leverage these plans as a starting point for new discussions that can build into a districtwide ecosystem for cybersecurity.

Once you have identified the priorities and organized the action steps for each colleague, you can use this information to have those critical conversations across your district team. By focusing on the priorities of each colleague and connecting the cybersecurity actions to their priorities, you are establishing a strong foundation for gaining greater district wide buy-in for the activities and resources that you know are essential to protect your district's data and infrastructure appropriately and adequately from a cyber-attack. Good luck and don't forget to share your milestones and successes along this journey with us at innovation@tomorrow.org.

Colleague Role	What are their 2-3 key priorities within their role?	What action steps (per priority) do you think will get your colleague's buy-in?	What is your plan to build shared responsibility and accountability around these action steps?
Example:			
Superintendent	1. *Student safety* 2. *District reputation*	*Implement a district-wide cybersecurity education program.* *Develop a crisis communication plan to effectively address cyber incidents.*	*Demonstrate how easy it will be to implement this on a semester basis across the district.* *Work with our PR Director to show examples to the cabinet as an awareness building activity.*

A. Your **SUPERINTENDENT**: action steps that are within the purview of the Superintendent's responsibilities. These are organized around their priorities.

Student Safety Issue

Action Steps:

1. Establish strict data protection policies and conduct regular security audits to ensure that student data is securely managed, and access is granted only to authorized personnel.
    - Challenges:
        - Resistance from staff: Some staff may resist changes; clear communication about the importance of these policies is critical.
        - Budget constraints: Funding regular audits can be challenging; prioritize budget for critical security measures.
        - Lack of expertise: May need to hire or consult with cybersecurity experts, requiring budget allocation and careful selection.
2. Implement a district-wide cybersecurity education program for both students and parents to promote safe online behaviors and reduce risks, such as cyberbullying.
    - Challenges:
        - Inconsistent engagement: Ensuring active participation can be tough; engaging content tailored to different age groups helps maintain interest.
        - Updating materials: Cyber threats evolve rapidly; educational content must be regularly reviewed and updated.
3. Upgrade cybersecurity measures on student information systems by implementing stronger security protocols and technology to prevent unauthorized access and protect sensitive data.
    - Challenges:
        - High costs: Upgrading systems can be expensive; strategic planning and phased implementation may be required.
        - Integration issues: New security solutions must integrate seamlessly with existing systems; technical support may be necessary.

- Staff training: Employees need comprehensive training on new systems to ensure their effectiveness.

Educational Continuity

Action Steps:

1. Develop and regularly update disaster recovery plans that address cyber incidents, creating robust strategies to quickly restore educational services following such events.
    - Challenges:
        - Complexity of plans: Developing comprehensive plans covering various scenarios can be daunting. Break these down into manageable steps.
        - Stakeholder understanding: Ensure all parts of the organization understand their roles, requiring effective communication and training.
        - Keeping plans current: Continually update plans to address new cybersecurity threats, which requires ongoing attention and resources.
2. Create a Business Continuity Plan (BCP) that complements your disaster recovery strategy to ensure that critical business functions can continue during a variety of emergencies, including cyber attacks.
    - Challenges:
        - Integration with disaster recovery: Align the BCP closely with disaster recovery plans for seamless operation during incidents.
        - Scope and scale: Define the scope to cover all essential functions without overextending resources, which involves strategic decision-making.
        - Regular testing and updates: The BCP must be tested regularly to ensure its effectiveness, requiring time and cooperation from various departments.
3. Enhance network security to prevent and mitigate DDoS attacks by strengthening your infrastructure to withstand or quickly recover from such incidents.
    - Challenges:
        - Evolving attack methods: Cyber attackers continuously develop new techniques; staying ahead requires constant learning and system updates.
        - Cost of defenses: Implementing robust defenses can be expensive; budgeting wisely and demonstrating potential cost savings are key.

4. Implement secure access controls and robust authentication processes for all digital platforms to ensure that only authorized individuals can access sensitive information and systems.
    - Challenges:
        - Balancing security with convenience: High security can make systems less user-friendly; finding the right balance is crucial.
        - Secure credential management: Manage user credentials securely to prevent unauthorized access, requiring careful policy and technology choices.
        - Training users: All users need to understand and comply with security protocols, which requires ongoing education and reminders.

Sound Financial Operations

Action Steps:

1. Secure adequate cybersecurity insurance to cover potential risks and mitigate financial impacts from cyber incidents by sharing some of the risks with insurers.
    - Challenges:
        - High cost of premiums: Balancing the cost against the benefits is crucial. Shop around for the best rates and coverage.
        - Understanding coverage: Policies can be complex; fully understand what is covered to ensure there are no gaps in protection.
        - Finding the right provider: Evaluate different providers based on coverage quality and customer service.
2. Budget for and invest in advanced cybersecurity technologies and infrastructure to prioritize cybersecurity investments and protect against the latest threats.
    - Challenges:
        - Justifying ROI: Demonstrate the return on investment by showing how cybersecurity prevents more costly incidents.
        - Allocating budget: Competing priorities may challenge cybersecurity funding; clear presentations of needs and benefits can help.
3. Establish a financial reserve specifically for cybersecurity emergencies and responses, setting aside funds to quickly address any cybersecurity incidents without financial delay.

- Challenges:
    - Forecasting the right amount: Estimate the potential costs of incidents to ensure the reserve is adequate.
    - Maintaining the reserve: Keep the fund intact and prevent it from being redirected to other areas.

District Reputation

Action Steps:

1. Develop a crisis communication plan to effectively address cyber incidents by preparing strategies that enable swift and transparent communication during a crisis to manage public perception effectively.
    - Challenges:
        - Rapid response requirement: Creating a plan that allows for quick action is complex and demands pre-planning.
        - Training spokespersons: Designating and training specific individuals to handle communications ensures consistency and accuracy.
2. Regularly engage with the community about the district's cybersecurity efforts to build community trust through transparency in cybersecurity initiatives.
    - Challenges:
        - Sustaining engagement: Keeping the community interested in what may seem a technical topic requires making information accessible and relevant.
        - Combating misinformation: Actively managing misinformation involves ongoing vigilance and proactive communication.
3. Monitor social media and other digital platforms to manage public perception and respond to misinformation, staying informed about public sentiment to react appropriately.

- Challenges:
    - Continuous monitoring: Implementing and maintaining real-time monitoring systems can be resource-intensive.
    - Handling sensitive situations: Responding to negative feedback or misinformation sensitively to avoid escalating concerns.

Regulatory Compliance

Action Steps:

1. Conduct regular training sessions for all staff on regulatory requirements and data privacy to ensure that everyone is knowledgeable about compliance obligations and can help mitigate legal risks.
    - Challenges:
        - Ensuring attendance: Making sure staff attend and engage in training sessions can be difficult; scheduling during less busy times can help.
        - Resource-intensive updates: Keeping training materials current with evolving laws requires continuous investment.
2. Review and update privacy policies annually to ensure they align with current laws and regulations, maintaining legal integrity by reflecting the latest data protection laws.
    - Challenges:
        - Keeping up with changes: Regulations change frequently; staying informed is crucial but resource-intensive.
        - Implementing updates: Applying changes across the entire district requires coordinated efforts and clear communication.
3. Collaborate with legal experts to ensure all data practices meet statutory obligations, leveraging their expert knowledge to enhance your compliance strategies.
    - Challenges:

- Cost of expertise: Hiring legal experts can be expensive; justify the costs by highlighting the potential for severe penalties for non-compliance.
- Integrating advice into practices: Translating legal advice into actionable steps involves cross-departmental collaboration.

Strategic Planning

Action Steps:

1. Integrate cybersecurity into the school district's overall strategic planning to ensure that cybersecurity considerations are included in all major decision-making processes and strategic initiatives.
    - Challenges:
        - Balancing priorities: Cybersecurity must compete with other educational priorities for attention and resources.
        - Stakeholder alignment: Gaining consensus among school board members and other stakeholders on the importance of cybersecurity investments can be challenging.
2. Adopt and adapt a comprehensive cybersecurity framework tailored to the educational sector by implementing recognized frameworks, like NIST or ISO, to structure your cybersecurity practices and policies.
    - Challenges:
        - Customization: Adapting general frameworks to fit the specific needs and context of your school district requires in-depth understanding and expertise.
        - Comprehensive coverage: Ensuring the framework covers all potential vulnerabilities without overwhelming resources.
3. Form a cybersecurity task force to oversee strategic implementation and monitor progress by establishing a dedicated group of professionals who will drive cybersecurity initiatives and ensure adherence to strategic plans.
    - Challenges:
        - Recruiting qualified members: Attracting the right talent with cybersecurity expertise to the task force.
        - Effective coordination: Ensuring the task force works cohesively with existing IT and management structures.

- Ongoing engagement: Keeping the task force active and focused on long-term goals amidst changing cybersecurity landscapes.

Leadership and Culture

Action Steps:

1. Establish and regularly review a comprehensive cybersecurity policy that encompasses all aspects of district operations, creating a policy framework to guide the district's cybersecurity practices effectively.
    - Challenges:
        - Policy relevance: Ensuring the policy remains relevant amidst evolving threats requires regular updates and reviews.
        - Wide-ranging implementation: Deploying policies across diverse school environments needs strategic planning and support.
2. Conduct leadership training workshops focused on cybersecurity, emphasizing proactive security measures, to equip leaders with the knowledge they need to support and promote cybersecurity initiatives effectively.
    - Challenges:
        - Finding time: Scheduling time for busy leaders to participate in training can be challenging; emphasize the critical nature of their involvement.
        - Engaging content: Creating content that is both informative and engaging for leaders ensures better retention and application.
3. Implement regular security briefings for the superintendent and school board to keep leadership informed and engaged, providing updates on the latest cybersecurity developments and the district's status.
    - Challenges:
        - Information overload: Simplifying complex information into manageable updates is crucial to keep leaders informed without overwhelming them.
        - Actionability of briefings: Ensuring that briefings lead to actionable decisions requires clear, focused presentations.

Resource Allocation

Action Steps:

1. Review and increase the cybersecurity budget to reflect the growing digital threats, ensuring that adequate funding is available to support necessary cybersecurity initiatives and technologies.
    - Challenges:
        - Budget prioritization: Balancing cybersecurity needs with other educational priorities can be difficult; clear communication of cybersecurity risks and potential impacts helps justify the necessary allocations.
        - Forecasting expenses: Accurately predicting the financial resources needed for effective cybersecurity amidst rapidly changing technology landscapes.
2. Prioritize the upgrade of outdated security systems and software to modern standards, ensuring you update and maintain cutting-edge security systems to protect against the latest cyber threats.
    - Challenges:
        - Cost of upgrades: Modernizing IT infrastructure can be expensive; phased upgrades and seeking cost-effective solutions are strategies to manage expenses.
        - Minimizing disruption: Implementing new systems can disrupt school operations; planning upgrades during low-activity periods and ensuring robust training can mitigate this issue.
3. Develop a staffing plan that includes roles specifically focused on monitoring and responding to cybersecurity threats, hiring or training staff to specialize in cybersecurity to ensure constant vigilance and proactive threat management.
    - Challenges:
        - Recruitment difficulties: Finding qualified cybersecurity professionals can be challenging; offering competitive salaries and continuous professional development opportunities can attract the right talent.
        - Integration with existing IT staff: Ensuring new and existing IT staff work cohesively requires clear role definitions and effective team management strategies.

Community Engagement

Action Steps:

1. Launch a cybersecurity awareness campaign that includes regular updates via newsletters and school meetings to educate the community about cybersecurity threats and the district's efforts to combat them.
    - Challenges:
        - Engaging diverse audiences: Crafting messages that resonate with various groups requires understanding their perspectives and communication preferences.
        - Resource allocation: Ensuring there are sufficient resources for regular communication efforts can strain limited budgets.
2. Organize annual cybersecurity fairs that involve students, parents, employees and local IT professionals to promote cybersecurity awareness through interactive and educational events.
    - Challenges:
        - Event organization: Coordinating these events requires significant planning and volunteer management.
        - Participant engagement: Attracting participants and providing valuable and understandable content to diverse audiences.
3. Establish a cybersecurity advisory board that includes local business leaders and law enforcement officials to discuss and plan community-wide cybersecurity initiatives, leveraging local expertise and resources to enhance district-wide cybersecurity strategies.
    - Challenges:
        - Maintaining active participation: Ensuring regular and productive involvement from all board members can be challenging.
        - Aligning goals: Different stakeholders may have different priorities; finding common ground is essential for effective collaboration.

Professional Development

Action Steps:

1. Implement an annual cybersecurity training curriculum for all staff, tailored to different roles within the district, to ensure everyone is up-to-date on the latest cybersecurity practices and protocols.

- Challenges:
    - Curriculum development: Creating a comprehensive, role-specific training program that addresses all relevant cybersecurity aspects.
    - Staff participation: Encouraging busy staff to prioritize and engage fully in training sessions.

2. Sponsor staff to obtain cybersecurity certifications that enhance their capabilities in handling security issues, supporting them in gaining professional certifications to improve their knowledge and skills in cybersecurity.
    - Challenges:
        - Financial investment: Certifications can be costly; securing budget for continuous professional development requires justification of ROI.
        - Time commitment: Balancing time commitments for certification training with staff's regular duties.
3. Conduct bi-annual tabletop exercises to simulate cyber incidents and test the district's incident response and recovery strategies, preparing staff for potential cyber incidents through realistic simulation exercises.
    - Challenges:
        - Realism and relevance: Designing exercises that accurately reflect potential real-world scenarios and are relevant to the participants' roles.
        - Logistics and participation: Organizing comprehensive exercises that involve multiple departments can be logistically complex and ensure full participation.

B. Your **SCHOOL BOARD:** action steps that are within the purview of the School Board's responsibilities. These are organized around their priorities.

Regulatory Compliance and Legal Oversight

Action Steps:

1. Implement a compliance review program to regularly assess the district's adherence to cybersecurity laws.

- Challenges:
    - Keeping up-to-date with changing regulations and ensuring all policies reflect these changes.
    - Ensuring thorough and regular compliance checks without straining district resources.

2. Engage with legal experts to provide ongoing education to the board and administration on regulatory requirements.
    - Challenges:
        - Finding and retaining experts familiar with the specific legal landscape of education and cybersecurity.
        - Integrating legal advice into practical, actionable policies and procedures.
3. Establish a protocol for rapid response to legal advisories or changes in legislation affecting cybersecurity practices.
    - Challenges:
        - Developing a flexible response system that can quickly adapt to new legal requirements.
        - Ensuring that all stakeholders are informed and prepared to implement changes swiftly.

Cybersecurity Governance and Oversight

Action Steps:

1. Establish a cybersecurity oversight committee within the board to focus on policy development, risk assessment, and strategy implementation.
    - Challenges:
        - Assembling a committee with the right expertise and understanding of cybersecurity.
        - Ensuring the committee remains current with the evolving cyber threat landscape and governance best practices.
2. Require regular cybersecurity risk assessments and audits, reporting findings directly to the school board.
    - Challenges:

- Integrating comprehensive, understandable cybersecurity reporting into regular board meetings.
- Acting on audit findings to implement timely and effective mitigations or enhancements.

3. Adopt a board-level cybersecurity framework that aligns with national standards and is tailored to the educational sector.
    - Challenges:
        - Customizing standard frameworks to fit the specific needs and context of the school district.
        - Ensuring continuous improvement and adaptation of the framework in response to new threats.

Strategic Cybersecurity Leadership

Action Steps:

1. Lead by example by participating in regular cybersecurity training and awareness programs.
    - Challenges:
        - Encouraging full board participation and ongoing commitment to cybersecurity education.
        - Tailoring training content to be relevant and engaging for board-level responsibilities.
2. Communicate the importance of cybersecurity investments to stakeholders, highlighting how these investments protect educational and operational capabilities.
    - Challenges:
        - Balancing financial investments in cybersecurity with other educational priorities.
        - Clearly articulating the ROI and benefits of cybersecurity measures in terms stakeholders can appreciate.
3. Develop a crisis management and incident response plan that includes board-level roles and responsibilities.
    - Challenges:

- Ensuring that all board members understand their specific roles during a cybersecurity incident.
- Regularly updating and practicing the response plan to keep it effective and relevant.

Financial Oversight and Cybersecurity Budgeting

Action Steps:

1. Develop a dedicated cybersecurity budget line item that reflects the importance of these initiatives.
    - Challenges:
        - Securing funding within the overall district budget, competing against other critical educational needs.
        - Justifying the cybersecurity spending to stakeholders by demonstrating potential cost savings from avoided breaches.
2. Conduct periodic reviews of cybersecurity expenditures to ensure funds are used effectively.
    - Challenges:
        - Monitoring and assessing the impact of spent funds on improving cybersecurity defenses.
        - Adapting budget allocations based on the evolving nature of cyber threats and district needs.
3. Leverage grants and other funding opportunities to enhance the district's cybersecurity without overextending the budget.
    - Challenges:
        - Identifying and applying for relevant grants that match the district's needs.
        - Managing grant funds according to specific rules and ensuring all grant-funded projects meet their goals.

Community Engagement and Public Communication

Action Steps:

1. Host community forums and workshops on cybersecurity awareness tailored to parents and students.
    - Challenges:
        - Designing engaging and informative events that address community concerns and misinformation.
        - Coordinating these events to reach a wide audience without significant costs.
2. Implement a transparent communication policy regarding cybersecurity practices and incidents.
    - Challenges:
        - Balancing transparency with the need to protect sensitive information about security measures and vulnerabilities.
        - Ensuring consistent, clear messaging that avoids causing unnecessary alarm.
3. Create a feedback loop with the community to gather input on cybersecurity policies and practices.
    - Challenges:
        - Encouraging active participation from a diverse community.
        - Effectively incorporating community feedback into cybersecurity strategies without compromising security standards.

C. Your **COMMUNICATION OFFICER:** action steps that are within the purview of the Communication Officer's responsibilities. These are organized around their priorities.

Crisis Communication and Incident Response

Action Steps:

1. Develop a comprehensive crisis communication plan that includes predefined templates for various cyber incident scenarios.

- Challenges:
    - Creating detailed, scenario-specific templates that are readily adaptable to the specifics of an incident.
    - Regularly updating communication plans to reflect new types of cybersecurity threats.

2. Conduct regular training sessions with communication staff on how to handle cybersecurity incidents, including role-playing exercises.
    - Challenges:
        - Ensuring all communication team members are prepared and understand their roles during different types of cyber incidents.
        - Keeping the team updated with the latest knowledge on cybersecurity and incident management.
3. Establish protocols for rapid response to ensure timely and accurate information dissemination during a cybersecurity event.
    - Challenges:
        - Coordinating effectively with IT and cybersecurity teams to obtain accurate incident details.
        - Managing the timing and content of communications to avoid spreading misinformation.

Public Relations and Media Management

Action Steps:

1. Create a media response team specialized in cybersecurity incidents to engage with journalists and manage media relations.
    - Challenges:
        - Training and maintaining a team with expertise in both media relations and the technical aspects of cybersecurity.
        - Balancing transparency with the need to protect ongoing investigations and sensitive information.
2. Implement a proactive media outreach program to educate journalists about the district's cybersecurity efforts.

- Challenges:
    - Developing relationships with media personnel that can help facilitate more accurate and favorable coverage.
    - Organizing and delivering effective educational sessions for the media without disclosing sensitive operational details.

3. Monitor media coverage continuously to track public sentiment and misinformation, responding swiftly to correct inaccuracies.
    - Challenges:
        - Establishing a comprehensive monitoring system that covers all forms of media.
        - Quickly addressing misinformation while maintaining a positive relationship with the media.

Internal Communications and Employee Awareness

Action Steps:

1. Develop and distribute regular cybersecurity newsletters to keep staff updated on policies, practices, and current cyber threats.
    - Challenges:
        - Ensuring the content is engaging and informative enough to maintain staff interest and compliance.
        - Scheduling regular updates without overwhelming staff with information.
2. Support the organization and implementation of cybersecurity workshops and seminars for staff across all departments in coordination with the IT Department to ensure that the messaging is appropriate for all involved.
    - Challenges:
        - Coordinating with cybersecurity experts to deliver accurate and relevant content.
        - Encouraging participation from all departments, including those who may not typically engage with technical subjects.

3. Provide feedback to the Human Resources and Professional Learning staff on how to effectively communicate cybersecurity topics within new employee onboarding sessions to establish security awareness from the start.
    - Challenges:
        - Integrating comprehensive cybersecurity training into existing onboarding processes without extending their duration significantly.
        - Ensuring new employees absorb and apply cybersecurity best practices effectively.

Strategic Communication Planning

Action Steps:

1. Develop a unified strategic communication plan that includes guidelines for cybersecurity messaging.
    - Challenges:
        - Integrating cybersecurity topics seamlessly into the broader district communications strategy.
        - Ensuring consistency across all communications channels and messages.
2. Coordinate with the superintendent and school board to align communication efforts with executive leadership and policy directions.
    - Challenges:
        - Maintaining regular communication and collaboration with top district officials to ensure alignment.
        - Adapting quickly to changes in leadership or strategic direction that affect communication tactics.
3. Regularly review and update the strategic communication plan to reflect new cybersecurity trends and district policies.
    - Challenges:
        - Keeping the communication strategy current with fast-evolving cybersecurity landscapes and district priorities.
        - Engaging with stakeholders to obtain feedback and make informed updates.

Collaboration with IT and Cybersecurity Teams

Action Steps:

1. Establish regular meetings and communication channels between the Communication and IT departments.
    - Challenges:
        - Coordinating schedules and priorities between departments with different focuses.
        - Developing effective communication protocols that facilitate clear and accurate information exchange.
2. Participate in joint training sessions with IT staff to understand the technical aspects of cybersecurity.
    - Challenges:
        - Bridging the knowledge gap between non-technical communication staff and technical IT personnel.
        - Creating training materials that are accessible and engaging for non-IT staff.
3. Co-develop incident response communication protocols that detail how to communicate internally and externally during IT emergencies including the development of backups and/or redundancy to preferred or typically used communication channels.
    - Challenges:
        - Balancing the need for swift public communication with the accuracy and sensitivity of technical information.
        - Ensuring all communication is vetted through proper channels to maintain security and confidentiality.

Digital Content Security

Action Steps:

1. Implement robust security protocols for all digital communication tools and platforms.
    - Challenges:

- Ensuring all communication tools meet current security standards without compromising usability.
- Regularly updating security measures to counter new vulnerabilities.

2. Train staff on secure practices for creating, storing, and sharing digital content.
    - Challenges:
        - Keeping training up-to-date with the latest security practices and threats.
        - Ensuring all staff consistently apply security practices.
3. Conduct regular audits of digital content access and security measures to prevent unauthorized access.
    - Challenges:
        - Identifying and addressing potential security gaps in digital content management.
        - Balancing thorough auditing with the operational efficiency of the communication processes.

D. Your **CHIEF FINANCIAL OFFICER:** action steps that are within the purview of the Chief Financial Officer's responsibilities. These are organized around their priorities.

Financial Risks and Impacts

Action Steps:

1. Implement advanced security technologies and protocols across all financial systems to guard against unauthorized access and potential financial fraud.
    - Challenges:
        - Balancing the costs of advanced security solutions with budget constraints.
        - Ensuring seamless integration with existing financial management systems.

2. Conduct regular cybersecurity risk assessments to identify and mitigate potential vulnerabilities within financial systems.
    - Challenges:
        - Continuously updating risk assessment strategies to address new and evolving threats.
        - Engaging all relevant stakeholders in the risk assessment process to ensure comprehensive coverage.
3. Establish and maintain a cybersecurity incident response plan specifically tailored for financial systems.
    - Challenges:
        - Developing a response plan that is both rapid and effective in minimizing financial damage during cyber incidents.
        - Training financial staff to respond efficiently and according to the established protocols without exacerbating the situation.

Insurance and Risk Transfer

Action Steps:

1. Evaluate and update cyber insurance policies annually to align with the evolving cyber threat landscape and the district's changing needs.
    - Challenges:
        - Determining the right level of coverage to effectively balance cost against potential cyber risks.
        - Keeping informed of changes in the cyber insurance market to ensure the most effective coverage is obtained.
2. Develop a partnership with cybersecurity legal experts to regularly review insurance policy clauses for compliance with current laws and best practices.
    - Challenges:
        - Finding and maintaining a relationship with legal experts who are up-to-date with the ever-changing landscape of cybersecurity law.
        - Ensuring that legal advice is effectively incorporated into practical insurance strategies without excessive costs.

3. Create an insurance claim management protocol to streamline the process following a cybersecurity incident.
    - Challenges:
        - Developing a protocol that efficiently coordinates all necessary actions from the initial incident detection to the final resolution of claims.
        - Training staff in effective claim management procedures to ensure quick recovery and minimal financial impact.

Cost Management and ROI

Action Steps:

1. Quantify the financial impact of cybersecurity measures by establishing clear metrics for cost savings and risk reduction.
    - Challenges:
        - Developing reliable indicators that measure intangible benefits such as improved security posture or reduced risk exposure.
        - Communicating these benefits effectively to the school board and other stakeholders to secure continued funding.
2. Integrate cybersecurity cost tracking into the district's financial management systems to ensure precise accounting and monitoring of all cybersecurity-related expenditures.
    - Challenges:
        - Implementing comprehensive tracking mechanisms that can accurately differentiate and categorize cybersecurity expenditures from other IT costs.
        - Ensuring that financial reporting systems are updated to reflect these changes without disrupting existing accounting practices.
3. Conduct periodic benchmarking studies to compare the district's cybersecurity spending and ROI with similar educational institutions.
    - Challenges:
        - Gathering relevant data from comparable institutions while maintaining confidentiality and data integrity.
        - Analyzing the benchmarking data to draw actionable insights without oversimplifying the complexities of different cybersecurity environments and threats.

Vendor Management

Action Steps:

1. Strengthen vendor cybersecurity agreements and incorporate regular security audits into contract terms.
    - Challenges:
        - Negotiating contract terms that include stringent security requirements without deterring vendors.
        - Ensuring consistency in enforcement and regular auditing of vendor compliance with cybersecurity standards.
2. Implement a centralized vendor management system to track and manage all vendor-related cybersecurity compliance data.
    - Challenges:
        - Integrating all vendor information into a single system without compromising security or functionality.
        - Ensuring that the system remains up-to-date and can handle the complexity of monitoring various vendors' compliance statuses.
3. Develop and deploy a training program for vendors on the district's cybersecurity policies and expectations.
    - Challenges:
        - Creating a comprehensive training program that is adaptable to a variety of vendors with different levels of cybersecurity expertise and operational scales.
        - Monitoring and ensuring that all vendors complete the training successfully and adhere to the district's cybersecurity standards in their ongoing operations.

Disaster Recovery and Business Continuity

Action Steps:

1. Create and maintain a comprehensive business continuity plan that addresses potential cyber incidents impacting financial operations.

- Challenges:
    - Ensuring the plan is robust and flexible enough to adapt to various types of cyber incidents.

2. Regularly update and test disaster recovery plans to ensure they effectively cover financial systems.
    - Challenges:
        - Coordinating across departments to include all aspects of financial operations in the plans.
        - Managing the logistical and financial aspects of frequent disaster recovery testing.
3. Establish a cross-functional recovery task force that includes members from finance, IT, and other critical departments to oversee disaster recovery operations.
    - Challenges:
        - Assembling a task force with the right mix of skills and ensuring they can effectively collaborate during high-pressure situations.
        - Training the task force to handle specific scenarios related to financial systems, ensuring rapid and coordinated response efforts across various departments.

Governance and Policy Management

Action Steps:

1. Regularly review and update cybersecurity policies to ensure they address current cyber threats and comply with new regulations.
    - Challenges:
        - Keeping policies current with the fast-paced evolution of cybersecurity threats and technologies.
        - Ensuring effective implementation and compliance across all levels of the organization.
2. Develop a framework for assessing the effectiveness of cybersecurity policies in real-time, incorporating feedback mechanisms from all relevant departments.
    - Challenges:

- Designing an assessment framework that is both comprehensive and adaptable to changes in cybersecurity practices and threats.
- Integrating feedback from diverse departments and ensuring it is effectively used to enhance policy effectiveness and compliance.

Employee Training and Awareness

Action Steps:

1. Enhance cybersecurity training programs to include simulations and real-life scenario exercises that focus on the financial sector's specific threats.
    - Challenges:
        - Designing training programs that are both engaging and informative, particularly for non-technical staff.
        - Ensuring ongoing education and updates to training programs to cover new and evolving cyber threats.
2. Implement a recognition and rewards system to encourage staff participation and compliance with cybersecurity protocols.
    - Challenges:
        - Designing a rewards system that effectively motivates employees without leading to complacency or a check-box mentality towards cybersecurity training.
        - Monitoring and evaluating the effectiveness of the rewards system to ensure it genuinely enhances security awareness and compliance.
3. Develop partnerships with external cybersecurity education providers to offer specialized training sessions and certifications for financial department staff.
    - Challenges:
        - Selecting suitable external providers that align with the specific needs of the school district and can adapt their offerings to the evolving landscape of cyber threats.
        - Integrating external training sessions into the regular workflow of employees without disrupting daily operations or financial processes.

E. Your **CHIEF ACADEMIC OFFICER:** action steps that are within the purview of the Chief Academic Officer's responsibilities. These are organized around their priorities.

Educational Continuity and Cybersecurity

Action Steps:

1. Implement cybersecurity best practices in digital learning environments to ensure their resilience against cyber threats.
    - Challenges:
        - Integrating advanced cybersecurity measures without hindering the accessibility or usability of educational technologies.
        - Keeping up with the rapidly evolving cyber threat landscape and updating defenses accordingly.
2. Develop and maintain a comprehensive disaster recovery plan that includes educational technology systems.
    - Challenges:
        - Crafting a recovery plan that minimizes downtime and is tailored to the specific needs of educational platforms.
        - Regular testing and updating of the plan to ensure its effectiveness in various scenarios.
3. Regular training for academic staff on cybersecurity threats and response protocols related to educational technologies.
    - Challenges:
        - Ensuring consistent and comprehensive training across all academic departments.

- Maintaining engagement and retention of cybersecurity knowledge among academic staff.

Crisis Communication Plan

Action Steps:

1. Develop specific communication protocols for different types of cybersecurity incidents.
    - Challenges:
        - Tailoring messages to be appropriate for the age and role of all recipients within the school environment.
        - Training staff to effectively execute these protocols under pressure.
2. Establish a dedicated crisis communication team within the school.
    - Challenges:
        - Assembling a team with the right mix of skills and ensuring they are available during critical incidents.
        - Regularly training the team on updates to crisis management protocols and tools.
3. Regularly review and test the communication plan with simulated scenarios.
    - Challenges:
        - Organizing comprehensive simulations that accurately reflect potential real-world crises.
        - Adjusting the communication plan based on feedback and evolving communication needs.

Cybersecurity in Curriculum Development

Action Steps:

1. Collaborate with curriculum specialists to integrate cybersecurity topics across subject areas.
    - Challenges:

- Aligning cybersecurity integration with existing educational standards and curricula.
- Finding qualified experts to develop age-appropriate cybersecurity content.

2. Establish partnerships with external cybersecurity educational organizations to enhance curriculum resources.
    - Challenges:
        - Identifying and vetting potential partners that align with the district's academic goals and values.
        - Ensuring that external content complements the core curriculum without redundancy.
3. Monitor and evaluate the effectiveness of cybersecurity education within the curriculum.
    - Challenges:
        - Developing metrics and assessment tools to measure student understanding and application of cybersecurity principles.
        - Adapting and refining curriculum content based on feedback and assessment outcomes.

Professional Development in Cybersecurity for Educators

Action Steps:

1. Implement targeted professional development programs focusing on cybersecurity for educators.
    - Challenges:
        - Designing engaging and relevant professional development that addresses the specific cybersecurity needs of educators.
        - Scheduling and funding ongoing training sessions within the constraints of the academic calendar and budget.
2. Create a resource hub for educators with up-to-date information on cybersecurity best practices and teaching resources.
    - Challenges:

- Continuously curating and updating the resource hub to keep it relevant and useful.
- Encouraging regular use and engagement with the hub among educators.

3. Incentivize educators to pursue cybersecurity certifications that enhance their teaching and technical skills.
    - Challenges:
        - Allocating funds to support certification pursuits in a budget-conscious educational environment.
        - Ensuring that the certifications are recognized and valued within the district's professional development framework.

Student Data Protection

Action Steps:

1. Oversee the development and enforcement of robust data protection policies across all academic platforms.
    - Challenges:
        - Updating policies to reflect new technologies and methods of data collection.
        - Ensuring comprehensive staff training on data protection standards.
2. Implement regular audits of data handling and storage practices to ensure compliance with data protection laws.
    - Challenges:
        - Coordinating these audits without disrupting educational activities.
        - Addressing any identified issues promptly to maintain data integrity.
3. Foster a culture of data privacy within the school community by incorporating it into the curriculum and staff training.
    - Challenges:
        - Encouraging a proactive attitude towards data privacy among students and staff.

- Continually reinforcing data protection principles in everyday educational practices.

Community Outreach and Engagement on Cybersecurity

Action Steps:

1. Organize community cybersecurity workshops and informational sessions led by experts.
    - Challenges:
        - Engaging diverse community groups and ensuring high participation rates.
        - Providing content that is accessible and actionable for all attendees.
2. Develop partnerships with local businesses and cybersecurity firms to support community training initiatives.
    - Challenges:
        - Establishing mutually beneficial partnerships that provide real value to the school community.
        - Coordinating schedules and resources with external partners.
3. Launch a cybersecurity awareness campaign using various media platforms to reach all community members.
    - Challenges:
        - Creating compelling and informative campaign materials that resonate with a broad audience.
        - Measuring the impact of the campaign on community cybersecurity practices.

Cybersecurity Integration into Student Support Services

Action Steps:

1. Incorporate cybersecurity education into student counseling and support programs.

- Challenges:
    - Training counselors and support staff to competently advise on cybersecurity issues.
    - Integrating cybersecurity smoothly into existing student support frameworks.

2. Establish a student-led cybersecurity ambassador program to promote peer education.
    - Challenges:
        - Recruiting and training student ambassadors who are both knowledgeable and enthusiastic about cybersecurity.
        - Ensuring the program remains engaging and relevant to students' needs and interests.
3. Create safe and secure online platforms for students to discuss and report cybersecurity concerns.
    - Challenges:
        - Designing platforms that are secure, user-friendly, and accessible to all students.
        - Monitoring these platforms effectively to provide timely support and intervention.

F. Your **RISK MANAGEMENT OFFICE:** action steps that are within the purview of the Risk Management Office responsibilities. These are organized around their priorities.

Cyber Risk Assessment and Mitigation

Action Steps:

1. Conduct comprehensive cybersecurity risk assessments regularly to identify and prioritize risks.
    - Challenges:

- Staying updated with the latest cybersecurity threats and vulnerabilities.
- Integrating diverse inputs from various departments for a holistic risk assessment.

2. Develop and implement risk mitigation strategies that align with the district's overall security posture.
    - Challenges:
        - Balancing resource allocation between immediate threats and long-term security investments.
        - Gaining buy-in from all stakeholders for implementing risk mitigation measures.
3. Monitor and update risk mitigation plans continuously based on new threats and vulnerabilities.
    - Challenges:
        - Keeping risk mitigation strategies adaptive and responsive to the evolving cyber threat landscape.
        - Ensuring ongoing compliance with changing regulations and standards.

Policy Development and Compliance

Action Steps:

1. Craft comprehensive cybersecurity policies that meet all regulatory requirements.
    - Challenges:
        - Continuously monitoring legislative changes and updating policies accordingly.
        - Ensuring policies are both stringent and practical for implementation.
2. Implement regular training programs for compliance across all levels of the district.
    - Challenges:
        - Designing effective training programs that cater to different roles and responsibilities.
        - Measuring and ensuring the effectiveness of training programs in achieving compliance.

3. Establish a compliance monitoring system to track adherence to cybersecurity policies.
    - Challenges:
        - Developing and maintaining a monitoring system that is thorough and unobtrusive.
        - Addressing non-compliance issues swiftly and effectively without disrupting operational workflows.

Cybersecurity Insurance Management

Action Steps:

1. Regularly review and update insurance policies to ensure comprehensive coverage against all forms of cyber threats.
    - Challenges:
        - Keeping abreast of new and emerging cyber risks that need to be covered by insurance.
        - Negotiating favorable terms with insurance providers that adequately cover potential risks.
2. Educate district leadership about the importance of cybersecurity insurance through regular briefings and reports.
    - Challenges:
        - Convincing decision-makers of the necessity for adequate insurance coverage despite budget constraints.
        - Providing clear and concise information on how cybersecurity insurance protects district assets.
3. Conduct simulations of cyber incidents to assess the adequacy of current insurance coverage.
    - Challenges:
        - Designing realistic scenarios that effectively test the district's insurance response.
        - Interpreting simulation results to make informed adjustments to insurance policies.

Incident Response and Crisis Management

Action Steps:

1. Develop a comprehensive incident response plan specific to cybersecurity events.
    - Challenges:
        - Ensuring the plan is comprehensive and covers all types of potential cyber incidents.
        - Regularly updating the plan to reflect new cyber threats and response strategies.
2. Train a dedicated incident response team to handle cybersecurity emergencies.
    - Challenges:
        - Maintaining a skilled response team ready to act at any time.
        - Providing ongoing training and simulations to keep the team prepared and effective.
3. Establish clear communication channels for reporting and managing cybersecurity incidents.
    - Challenges:
        - Ensuring that all staff know how to report incidents promptly and accurately.
        - Maintaining clear and effective communication during a crisis to coordinate response efforts.

Cross-Departmental Collaboration

Action Steps:

1. Create a cybersecurity coordination committee that includes representatives from all key departments.
    - Challenges:
        - Ensuring active and productive participation from all departments.
        - Coordinating the committee's activities without adding significant overhead.
2. Implement integrated cybersecurity training sessions for all departments.
    - Challenges:

- Developing training materials that are relevant and applicable to various departmental functions.
- Scheduling training sessions that accommodate different departmental schedules and responsibilities.

3. Regularly review and assess the integration of cybersecurity practices across the district.
    - Challenges:
        - Collecting and analyzing data from multiple departments to assess cybersecurity integration.
        - Implementing recommendations from assessments without disrupting departmental operations.

G. Your **SCHOOL BUILDING LEADER/PRINCIPAL:** action steps that are within the purview of the School Building Leader/Principal's responsibilities. These are organized around their priorities.

Cybersecurity Awareness and School Culture

Action Steps:

1. Implement a school-wide cybersecurity awareness program that includes regular training sessions for both staff and students.
    - Challenges:
        - Engaging different age groups effectively to ensure the message resonates across all grades.
        - Providing ongoing training within the constraints of the school calendar and academic priorities.
2. Establish clear cybersecurity policies and protocols for all technology use within the school.
    - Challenges:

- Developing policies that are comprehensive yet understandable to all users, including young students.
- Ensuring consistent enforcement of these policies across all levels of the school community.

3. Regularly communicate the importance of cybersecurity through newsletters, assemblies, and parent meetings.
    - Challenges:
        - Crafting messages that are informative but not alarmist, to maintain a positive school environment.
        - Keeping the school community updated with the latest cybersecurity threats and protections.

Security of Educational Technologies

Action Steps:

1. Conduct regular security audits of all educational technologies used in the school.
    - Challenges:
        - Coordinating with IT staff to conduct thorough and regular audits without disrupting educational activities.
        - Addressing identified vulnerabilities promptly to maintain a secure learning environment.
2. Upgrade and maintain IT infrastructure with the latest security patches and updates.
    - Challenges:
        - Balancing budget constraints with the need for up-to-date technology.
        - Planning upgrades in a way that minimizes disruption to teaching and learning.
3. Control and monitor access to educational technologies to ensure only authorized users can access sensitive information.
    - Challenges:
        - Implementing robust access controls that are user-friendly for staff and students.

- Monitoring access logs to detect and respond to unauthorized access attempts promptly.

Training and Development for Staff and Students

Action Steps:

1. Implement targeted cybersecurity training sessions for staff that focus on recognizing phishing attempts, managing passwords, and securing personal and school devices.
    - Challenges:
        - Ensuring all staff members, regardless of technological proficiency, can understand and apply cybersecurity best practices.
        - Providing training that is relevant and can be regularly updated as new threats emerge.
2. Develop an age-appropriate cybersecurity curriculum for students that is integrated into their regular learning activities.
    - Challenges:
        - Creating engaging and educational content that resonates with different age groups.
        - Measuring the effectiveness of the cybersecurity education provided to students.
3. Organize regular cybersecurity drills and simulations to practice responding to cyber incidents.
    - Challenges:
        - Designing realistic scenarios that effectively prepare staff and students for actual cyber events.
        - Coordinating drills that involve the entire school without causing unnecessary alarm or disruption.

Incident Response and Crisis Management

Action Steps:

1. Develop a comprehensive incident response plan tailored to common cybersecurity threats the school might face.
    - Challenges:
        - Ensuring the plan covers all potential incidents and is regularly updated based on emerging threats.
        - Training all staff to be familiar with the plan and know their roles in the event of a cyber incident.
2. Establish a communication strategy that includes notifying affected individuals, parents, and regulatory bodies where necessary.
    - Challenges:
        - Communicating effectively and transparently with stakeholders without causing undue concern or panic.
        - Maintaining compliance with legal requirements for breach notification.
3. Conduct post-incident reviews to learn from the event and improve future responses.
    - Challenges:
        - Collecting accurate information about the incident and response to evaluate what went well and what did not.
        - Implementing changes based on lessons learned without significant disruptions or resistance.

Parent and Community Engagement in Cybersecurity

Action Steps:

1. Host informational cybersecurity workshops for parents and community members.
    - Challenges:
        - Designing workshops that cater to varying levels of technical knowledge.
        - Achieving high attendance rates and ensuring the information presented is actionable and clear.
2. Develop and distribute cybersecurity resource kits to families that include guidelines on safe online practices, recommended security software, and tips for monitoring children's online activities.

- Challenges:
    - Creating resource kits that are comprehensive yet easy to understand for non-technical audiences.
    - Keeping the kits updated with the latest cybersecurity advice and best practices.

3. Establish a regular communication channel (such as a newsletter or a dedicated section on the school website) focused on cybersecurity updates and tips.
    - Challenges:
        - Maintaining consistent and engaging content that encourages regular reading and interaction.
        - Measuring the effectiveness of communications in improving cybersecurity practices among families.
4. Create a feedback mechanism for parents and community members to share their cybersecurity concerns and experiences.
    - Challenges:
        - Encouraging open and honest communication without causing alarm or spreading misinformation.
        - Effectively addressing and responding to feedback in a timely manner to reinforce trust and collaboration.

ABOUT NACC

The K-12 National Advisory Council on Cybersecurity (NACC) is an organization focused on enhancing cybersecurity measures within K-12 school districts. The council aims to address the growing cyber threats facing educational institutions by advocating for a comprehensive districtwide cybersecurity ecosystem. This ecosystem includes developing strategies for protecting technology infrastructure, data assets, and personal records of students and staff. NACC emphasizes the importance of collaboration among district superintendents, IT professionals, and communication leaders to ensure effective cybersecurity practices. The council also advocates for transparent messaging and community trust-building to enhance the overall security posture of school districts.

ABOUT PROJECT TOMORROW

Project Tomorrow's nonprofit mission is to support the effective implementation of research-based learning experiences for students in K-12 schools. Project Tomorrow is particularly interested in the role of digital tools, content, and resources in supporting students' development of college and career-ready skills. The organization's landmark research is the Speak Up Research Project which annually polls K-12 students, parents, educators, and community members about the impact of technology resources on learning experiences both in school and out of school, and represents the largest collection of authentic, unfiltered stakeholder voice on digital learning. Since 2003, over 6.2 million K-12 students, parents, teachers, librarians, principals, technology leaders, district administrators and members of the community have shared their views and ideas through the Speak Up Project. Project Tomorrow is very proud to be part of the collaborative team that developed the 2024 National Educational Technology Plan with the U.S. Department of Education. Learn more about our mission and work at www.tomorrow.org.

ABOUT IBOSS

iboss is a cloud security company that provides organizations and their employees fast and secure access to the Internet on any device, from any location, in the cloud. The iboss cloud platform provides network security as a service, delivered in the cloud, as a complete SaaS offering. Leveraging a purpose-built cloud architecture backed by over 230 issued and pending patents and more than 100 points of presence globally, iboss protects more than 4,000 organizations worldwide. Learn more about the security infrastructure and offerings at **www.iboss.com.**

project tomorrow

NACC

K-12 National Advisory Council on Cybersecurity

iboss®