Protecting Our Future: Cybersecurity for K-12 Leaders

Cybersecurity Action Plan

Module 1 →

Module 2 →

Module 3 →

Module 4 →

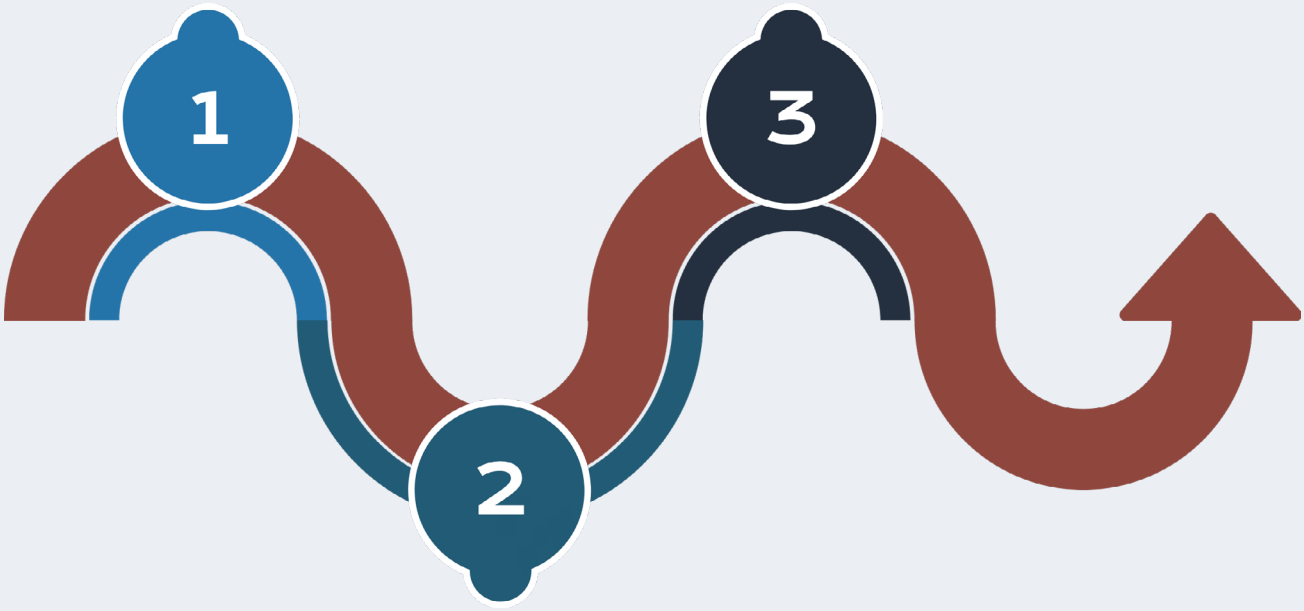
Module 5 →

Module 1

After completing the cybersecurity self-assessment, where along the roadmap do you see your organization?

Where are you starting from, and where do you want to go? What stops will you make along the way?

Use the Draw Tool to chart your intended pathway on the course roadmap below:



Paste screenshots, images, text, or links from Module 1 for each of the following:

	Use the spaces below for text or links	Use the spaces below for screenshots and images
Something that surprised you		
Something that resonated with you		
Something you want to know more about		
Something you want to share with your team		

Module 2

Implementing MFA

After reviewing CISA's MFA Enhancement Guide, identify any resources you need in order to begin the Strategic Planning phase and move into the Tactical Planning and Execution phases.

Next Steps

Record any points of contact you'll need to move forward

Identifying and Prioritizing Known Security Flaws

Prioritize remediation of vulnerabilities listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog, either by signing up for recurring updates or by using a third-party service that automatically identifies the presence of vulnerabilities in the catalog.

Action steps to take if a vulnerability is detected	Team member responsible

Performing and Testing Backups

Identify data that is critical to the continued operations of your school or district.

How is this data currently backed up?

What additional backup solutions could you implement that are separated from the operational network?

What are your next steps? Identify members of your team that can help you move forward.

Minimizing Exposure to Common Attacks

Review the steps outlined by CISA to reduce the likelihood that a malicious actor can identify your organization's assets when scanning the Internet for potential victims.

Steps already taken	Steps to prioritize next

Developing a Cyber Incident Response Plan

Explore the steps outlined in CISA's Incident Response Plan (IRP) Basics document for what to do before, during, and after a cyber event.

Which steps are already included in your IRP? Which ones would you like to add?

Already included	Want to add	
		Before a Cybersecurity Incident
☐	☐	Train the staff
☐	☐	Review your IRP with an attorney
☐	☐	Meet your CISA regional team
☐	☐	Meet your local law enforcement agency (LEA) team
☐	☐	Print IRP documents and associated contacts list
☐	☐	Develop an incident staffing and stakeholder plan
☐	☐	Review the IRP quarterly
☐	☐	Prepare press responses
☐	☐	Select an outside technical resource/investigation firm
☐	☐	Conduct an attack simulation exercise
		During a Cybersecurity Incident
☐	☐	Assign an Incident Manager (IM)
☐	☐	Assign a Tech Manager (TM)
☐	☐	Assign a Communications Manager (CM)
		After a Cybersecurity Incident
☐	☐	Hold a formal retrospective meeting
☐	☐	Review and update policies and procedures
☐	☐	Communicate findings to the staff

Make a list of stakeholders that you'd like to involve in the development of your IR plan.

Creating a Training and Awareness Campaign

Review your employee handbook to ensure it has a section on cybersecurity with information on acceptable use of technology, policies, and escalation procedures.

Is the most important information highlighted in a useful way?

Is there information that's missing? Make a list of any key ideas you'd like to include.

Module 3

Prioritizing CPG Alignment

As you develop your monthly, quarterly, and annual roadmaps, which CPGs would improve your security posture?

Paste screenshots from the CPG Checklist to capture your thinking:

Developing a Long-Term Cybersecurity Plan

After reviewing the NIST Cybersecurity Framework, consider some of the potential benefits from adding the framework to your long-term cybersecurity plan.

Looking ahead, how could the Framework inform your team's thinking about cybersecurity?

Leveraging State and Local Grants

Are state and local grants a viable option for your cybersecurity funding?

If yes, make a list of the next steps you'll need to take to begin the application process.

Record any important points of contact you'll need to get started

Utilizing Free and Low-Cost Services

Evaluate your security program's need for additional services and tools. Which ones are a fit for your needs?

Make a list of the tools you'd like to further explore outside of this course.

Write down your next steps and any points of contact you'll need to move forward.

Asking More of Technology Providers

Work with your team to make a list of the current software systems you have in place, such as a user identification system or mail system.

Record a list of your current software systems.

Return to the list and highlight any systems that require upcharges for basic security features or have unsafe default settings.

Write down your next steps to advocate for better built-in security and any points of contact you'll need to move forward.

Minimizing the Burden of On-Prem Security

Look back on the list of software and IT services you recorded above. Are there any that currently operate in the cloud?

Use the highlighter tool to identify which services from the list above that you would like to migrate.

Write down the next steps you'll need to take for cloud migration and any points of contact you'll need to move forward.

Module 4

Focusing on Collaboration and Information Sharing

Which information sharing groups are best aligned to the cybersecurity needs and goals of your organization?

Mark the organizations you would like to explore further:

- ☐ K12 SIX
- ☐ MS-ISAC
- ☐ SchoolSafety.gov

What information gaps could these organizations potentially fill?

Make a list of next steps you'll take to join a collaboration, and which team members can help.

Partnering to Build a Cybersecurity Network

Think about how your organization has reported cyber incidents, phishing attempts, malware, or vulnerabilities in the past. Where do you think your organization is strong in its cybersecurity network, and where do you see opportunities?

Strengths	Opportunities

Make a list of next steps you'd like to take and identify any team members that can help you get there.

Module 5

Setting Up for Success

After exploring the Needs-Solution Matrix, identify which tools and solutions emerged in perfect balance—aligning with your school's unique needs, CISA key recommendations, and Cybersecurity Performance Goals.

Which of these tools and solutions do you already have in place?

Which ones would you like to explore further?

Course Wrap-Up

Take a few minutes to review the lists of goals, action items, and next steps that you have recorded in your Cybersecurity Action Plan.

Prioritize the action items you want to complete in the near term. Where do you want to be now?

Where do you want to be 6 months from now?

Where do you want to be a year from now?

From this final reflection, write a commitment statement. Include your commitment to what you want to accomplish next, what resources you'll need, and the team members or points of contact to help you get there.

Commitment Statement