

Securing Our Schools: Cybersecurity for K-12 IT Professionals

Course Syllabus

This course is designed to equip school IT professionals with a comprehensive understanding of the current K-12 cybersecurity landscape and the activities that increase security and protection in their computing environment. While evaluating their school's current systems and procedures, IT teams will learn about industry best practices to protect networks, student data, and overall IT infrastructure.

Learning Objectives

This course is designed for K-12 Information Technology Directors, Network and Systems Administrators, Technicians, and IT Specialists.

In this course, participants will:

- Review the threat landscape in K-12 education and understand federal recommendations for strengthening school cybersecurity
- Develop a comprehensive risk assessment for infrastructure and data systems
- Learn about control, authentication, and backup measures that protect networks and increase data security
- Create an incident response plan to handle cybersecurity issues that arise
- Explore security awareness and training programs for leaders, educators, families, and students
- See how other schools implement cybersecurity initiatives



Course Format

This self-paced course consists of five modules. It is designed to take approximately 90-120 minutes to complete, with additional time allotted for completing a personalized Action Plan.

Course Overview

Module 1: Introduction

In this module, IT professionals immerse themselves in visual data and narrative scenarios to better understand the current landscape of school cybersecurity. They explore federal cybersecurity recommendations for schools and reflect on the important role they play as the front line of cybersecurity inside their schools. By the end of the module, they'll understand the course structure and resources that will guide their learning.

Lesson 1: School Threats and Vulnerabilities

Lesson 2: IT Cybersecurity Responsibilities

Lesson 3: Course Overview

Module 2: Cybersecurity Frameworks and Threat Management

In this module, IT professionals dive deeper into cybersecurity measures designed to identify inherent risks and vulnerabilities in their school's digital learning environment. As they learn about each key practice, they'll identify actionable steps they can take to manage cybersecurity risk to systems, devices, and student data. They'll also discover Microsoft solutions and other resources that can support their goals along the way.

Lesson 1: Cyberthreats in Education and Zero Trust

Lesson 2: Vulnerability and Risk Assessments

Lesson 3: Threat Management

Module 3: School Network and Data Security

This module introduces IT professionals to key actionable steps that strengthen the security and safety of school networks and technology systems. They'll discover steps they can take to control access while securing their school's network against unauthorized users. They'll also take time to evaluate their current protection level against data loss and identify potential gaps where student data is most vulnerable.

Lesson 1: Access Control and Authentication Models

Lesson 2: Data Loss Prevention

Lesson 3: Secure Network Design



Module 4: Incident Response and Recovery

In this module, IT professionals develop a response plan for cybersecurity incidents. Using well-established incident response models, they'll learn how to monitor, classify, and report cyber incidents within their school. They'll also evaluate their school's current incident response plan and identify any areas for improvement.

Lesson 1: Incident Response Plans

Lesson 2: Investigation, Management, and Response

Lesson 3: Disaster Recovery Planning

Module 5: Planning for Progress

This final module brings everything together and focuses on guiding IT pros to make their own actionable plan for addressing cybersecurity threats and securing networks and systems within their schools. They'll identify tools they can leverage to meet their goals and discover solutions to support the personal goals they established at the start of the course.

Lesson 1: Security Awareness and Training

Lesson 2: Collaboration and Information Sharing

Lesson 3: Partnering to Build a Cybersecurity Network

Lesson 4: Course Wrap-Up