AP Cybersecurity Course Syllabus

Course Overview

AP Cybersecurity introduces students to the fundamental principles used to secure computer systems, networks, devices, and data in modern digital environments. Students will learn to identify vulnerabilities, understand cyber threats, and design strategies to defend against attacks using a defense-in-depth approach.

Throughout the course, students examine how cybersecurity affects individuals, organizations, governments, and societies. Students analyze real-world cyber incidents and develop technical and analytical skills necessary to detect, prevent, and mitigate cyber threats.

By the end of the course, students will understand how cybersecurity principles apply across physical systems, networks, devices, and software applications, and how responsible security practices contribute to a safer digital world.

Prerequisites

This course is designed for students with little to moderate prior technical experience.

Recommended preparation includes:

- Basic computer literacy
- Introductory knowledge of computer systems or networking (helpful but not required)
- Strong analytical and problem-solving skills

Required Resources

Online resources and labs provided by the instructor

- Online Text: JuiceMind.com
- Exam Registration: apclassroom.collegeboard.org

Course Goals

Students will:

- Develop an understanding of cybersecurity principles and defense strategies.
- Identify common vulnerabilities and cyber attack methods.
- Learn to apply defense-in-depth strategies across systems and networks.
- Evaluate risks and threats in modern digital environments.
- Analyze the societal, ethical, and economic impacts of cybersecurity.
- Develop problem-solving skills related to protecting digital systems and information.

Learning Environment

The course combines lectures, discussions, case studies, simulations, and hands-on activities. Students will analyze real cybersecurity incidents, perform threat modeling exercises, and develop strategies for protecting systems and networks.

Learning activities may include:

- Interactive cybersecurity simulations
- Threat analysis exercises
- Case studies of real-world cyber attacks
- Collaborative investigations
- Security strategy design activities

The AP Exam

The AP Cybersecurity end-of-course exam has consistent question types and weighting every year, so you and your students know what to expect on exam day.

Section I: End-of-Course Multiple-Choice Exam

60 multiple-choice questions | 80 minutes | 70% of score | 4 answer options

Questions assess students' understanding of cybersecurity concepts and their ability to analyze risks, identify vulnerabilities, evaluate security controls, and detect cyber attacks across multiple domains.

Topics assessed may include:

- Social engineering and cyber threats
- Physical security vulnerabilities and protections
- Network security and defenses
- Device authentication and protection
- Application and data security
- Cryptography and encryption
- Cyberattack detection methods

Section II: Free-Response Question

1 free-response question | 50 minutes end-of-course exam | 30% of score

The free-response question requires students to analyze a cybersecurity scenario and apply course concepts to evaluate risks, identify vulnerabilities, and propose appropriate security measures.

Students may be asked to:

- Identify potential threats or vulnerabilities in a system
- Explain how an attacker could exploit a weakness
- Recommend security controls to mitigate risks
- Describe methods for detecting cyber attacks
- Evaluate the effectiveness of cybersecurity defenses

The second section of the AP Cybersecurity Exam consists of a written response where students demonstrate their understanding of cybersecurity principles by analyzing a scenario and explaining how risks can be mitigated, attacks detected, and systems protected using appropriate security strategies.

Recommended Grading Scheme

Category	Weight
Assignments and Activities	25%
Quizzes	20%
Unit Exams	25%
Projects and Case Studies	20%
Final Exam	10%

Pacing

Lesson plans are structured around a 45-minute class period, and lesson folders should take 45 minutes to complete, unless otherwise stated. The instructional content of a lesson should never take more than this long to teach, but exercises and review may spill over into homework based on student ability.

In total, JuiceMind's AP Cybersecurity is designed to take 110 days to complete using only material included within this course. This is shorter than a typical school year to allow for additional review and supplemental content, and to accommodate the AP Exam (typically around May 15), which occur before the end of the school year.

Course Breakdown

Unit 1: Introduction to Security (~10 class periods)

Students explore the foundations of cybersecurity and learn how attackers exploit human behavior and technological vulnerabilities.

Topics Covered:

1.1 Understanding Social Engineering
1.2 Suspicious Website Logins
1.3 Best Practices for Public Networks
1.4 AI-Based Cybersecurity Attacks
1.5 Leveraging AI in Cyber Defense

Students examine common cyber threats and learn how individuals and organizations can reduce risk through safer digital practices.

Unit 2: Securing Spaces (~21 class periods)

Students learn how cybersecurity extends beyond digital systems into physical environments. They explore how physical access and environmental vulnerabilities can compromise computer systems.

Topics Covered:

2.1 Cyber Foundations
2.2 Physical Vulnerabilities and Attacks
2.3 Protecting Physical Spaces
2.4 Detecting Physical Attacks

Students analyze real-world examples of physical breaches and design strategies for securing facilities and equipment.

Unit 3: Securing Networks (~26 class periods)

This unit focuses on protecting computer networks from unauthorized access and cyber attacks.

Topics Covered:

3.1 Network Vulnerabilities and Attacks
3.2 Protecting Networks: Managerial Controls and Wireless Security
3.3 Protecting Networks: Segmentation
3.4 Protecting Networks: Firewalls
3.5 Detecting Network Attacks

Students learn how network defenses work and explore techniques used to detect malicious activity.

Unit 4: Securing Devices (~23 class periods)

Students examine vulnerabilities in computing devices and the techniques used to protect them.

Topics Covered:

4.1 Device Vulnerabilities and Attacks
4.2 Authentication
4.3 Protecting Devices
4.4 Detecting Attacks on Devices

Students investigate authentication systems, device hardening, and strategies used to identify compromised devices.

Unit 5: Securing Applications and Data (~30 class periods)

Students learn how software and stored data are protected against cyber threats. They explore cryptography, access controls, and application security.

Topics Covered:

5.1 Application and Data Vulnerabilities and Attacks
5.2 Protecting Applications and Data: Managerial Controls and Access Controls
5.3 Protecting Stored Data with Cryptography
5.4 Asymmetric Cryptography
5.5 Protecting Applications
5.6 Detecting Attacks on Data and Applications

Students analyze how encryption and security practices help protect sensitive information in modern digital systems.