

College Board AP Cybersecurity Course Outline

Effective for the 2026-2027 School Year

AP Cybersecurity is designed as an introductory college-level cybersecurity course. The course emphasizes hands-on cybersecurity skills and real-world scenarios in which students analyze risks, protect systems, and detect cyberattacks.

I. Major Course Skills

College Board organizes AP Cybersecurity around four major skill areas.

Skill 1: Analyze Risk

- Identify organizational assets.
- Identify vulnerabilities and threats.
- Analyze potential cybersecurity attacks.
- Determine the likelihood of an attack.
- Determine the possible impact of an attack.
- Evaluate cybersecurity risks.
- Document risks and findings.

Skill 2: Mitigate Risk

- Recommend security controls.
- Implement protective security controls.
- Implement deterrent security measures.
- Harden devices and systems.
- Configure security settings.
- Evaluate whether security controls are effective.
- Document security changes.

Skill 3: Detect Attacks

- Monitor systems.
- Analyze security logs.
- Identify Indicators of Compromise (IoCs).
- Recognize suspicious activity.
- Identify and classify cyberattacks.
- Analyze digital evidence.
- Evaluate attack-detection methods.

Skill 4: Collaborate

- Work as part of a cybersecurity team.
- Communicate cybersecurity findings.
- Complete assigned cybersecurity tasks.
- Use AI appropriately as a collaborative tool.
- Evaluate information produced with AI.
- Complete cybersecurity activities both with and without AI assistance.

The first three skill categories - Analyze Risk, Mitigate Risk, and Detect Attacks - each account for approximately 25-40% of the skills assessed on the multiple-choice portion of the AP Exam.

Unit 1: Introduction to Security

A. Cybersecurity Fundamentals

- Purpose of cybersecurity
- Confidentiality
- Integrity
- Availability
- Cybersecurity assets
- Vulnerabilities
- Threats
- Risks
- Security controls
- Defense in depth

B. Cyber Adversaries

- Cybercriminals
- Nation-state attackers
- Hacktivists
- Insider threats
- Organized crime
- Competitors
- Script kiddies
- Advanced Persistent Threats
- Adversary motivation, capabilities, resources, and attack objectives

C. Social Engineering

- Phishing
- Spear phishing
- Smishing
- Vishing
- Pretexting
- Impersonation
- Tailgating
- Baiting
- Identification of social-engineering techniques and appropriate mitigations

D. Authentication

- Usernames and passwords
- Strong passwords
- Password managers
- Multifactor authentication
- Something you know
- Something you have
- Something you are

E. Artificial Intelligence and Cybersecurity

- AI as a cybersecurity tool
- AI-assisted threat detection
- AI-assisted analysis
- Risks associated with AI
- AI-generated misinformation

- AI-enabled attacks
- Appropriate use of AI in cybersecurity work

Unit 2: Securing Physical Spaces

A. Physical Security

- Buildings
- Server rooms
- Network closets
- Computers
- Storage devices
- Workstations
- Mobile devices

B. Physical Vulnerabilities

- Unlocked doors
- Unsecured network equipment
- Unattended computers
- Poor visitor controls
- Improper equipment disposal
- Exposed network cables
- Lack of surveillance

C. Physical Attacks

- Equipment theft
- Device theft
- Unauthorized building access
- Tailgating
- Dumpster diving
- Hardware tampering
- Malicious USB devices

D. Physical Security Controls

- Locks
- Badge systems
- Security guards
- Cameras
- Motion detectors
- Fences
- Lighting
- Biometric access
- Visitor logs

E. Detecting Physical Attacks

- Camera records
- Badge logs
- Visitor logs
- Access logs
- Security alerts

Unit 3: Securing Networks

A. Networking Fundamentals

- Local Area Networks
- Wide Area Networks
- IP addresses
- MAC addresses
- Routers
- Switches
- Wireless access points
- Servers
- Clients

B. Network Vulnerabilities

- Unsecured services
- Open ports
- Weak network configurations
- Unencrypted communication
- Poor segmentation
- Insecure wireless networks
- Misconfigured firewalls

C. Network Attacks

- Denial-of-Service attacks
- Distributed Denial-of-Service attacks
- Man-in-the-Middle attacks
- Spoofing
- Packet sniffing
- Wireless attacks
- Unauthorized network access

D. Managerial Controls

- Acceptable-use policies
- Security policies
- Password policies
- Incident-response procedures
- Access policies

E. Wireless Security

- Wi-Fi vulnerabilities
- Wireless authentication
- Secure wireless configurations
- Rogue access points
- Wireless encryption

F. Network Segmentation

- Why networks are segmented
- How segmentation limits attacks
- Network zones
- Separation of sensitive systems
- Containment of compromised devices

G. Firewalls

- Purpose of a firewall
- Allow rules
- Deny rules
- Source addresses
- Destination addresses
- Ports
- Protocols
- Inbound traffic
- Outbound traffic
- Interpret and modify firewall rules

H. Network Logs

- Failed connections
- Suspicious IP addresses
- Unusual ports
- Repeated authentication attempts
- Abnormal traffic
- Indicators of Compromise

Unit 4: Securing Devices

A. Device Security

- Desktop computers
- Laptops
- Servers
- Smartphones
- Tablets
- Internet of Things devices

B. Device Vulnerabilities

- Unpatched operating systems
- Outdated applications
- Weak passwords
- Excessive permissions
- Unnecessary services
- Malware
- Misconfiguration

C. Malware

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware
- Keyloggers
- Rootkits
- Botnets

D. Authentication

- Password security
- Multifactor authentication
- User accounts
- Account privileges
- Authentication policies

E. Anti-Malware

- Antivirus software
- Endpoint protection
- Malware signatures
- Behavioral detection
- Quarantine
- Updates

F. Operating-System Security

- User accounts
- Administrator privileges
- Software updates
- File permissions
- Services
- Security configuration

G. File Permissions

- Read
- Write
- Execute
- Who can access a file
- What actions a user can perform
- Whether permissions create a security vulnerability
- How permissions should be changed

H. Detecting Device Attacks

- System logs
- Authentication logs
- Application logs
- Malware alerts
- Failed login attempts
- Account activity

Unit 5: Securing Applications and Data

A. Application Security

- Web applications
- Software
- Databases
- Online services

B. Application Attacks

- Injection attacks

- SQL injection
- Directory traversal
- Session attacks
- Authentication attacks
- Unauthorized access

C. Data Security

- Data at rest: files, databases, hard drives, USB drives, cloud storage
- Data in transit: networks, websites, email, wireless connections

D. Access Control

- Authentication
- Authorization
- Permissions
- Least privilege
- User roles
- Administrative privileges

E. Cryptography

- Encryption
- Decryption
- Keys
- Symmetric encryption
- Asymmetric encryption
- Hashing
- Digital certificates
- How cryptography protects confidentiality and integrity

F. Application and Data Logs

- Web server logs
- Authentication logs
- Application logs
- Database activity
- Failed login attempts
- Suspicious requests

G. Detecting Application Attacks

- Repeated login failures
- Suspicious URLs
- Abnormal database queries
- Unauthorized access
- Unexpected file activity
- Strange user behavior

Concepts That Should Appear Throughout All Five Units

Risk

Asset -> Vulnerability -> Threat -> Risk -> Mitigation

1. What are we protecting?
2. What vulnerabilities exist?

3. Who or what could exploit them?
4. What would happen if the attack succeeded?
5. How likely is the attack?
6. What security control could reduce the risk?
7. How would we detect the attack?

Defense in Depth

- Physical security
- Authentication
- Firewalls
- Network segmentation
- Endpoint protection
- Encryption
- Logging
- Monitoring
- Security policies

Indicators of Compromise

- Network logs
- Authentication logs
- Application logs
- Operating-system logs
- Firewall logs

Policies

Students need practice interpreting cybersecurity policies and deciding whether actual device or user behavior complies with those policies.

Hands-On Skills Students Should Practice

- Reading firewall rules
- Creating firewall rules
- Analyzing network logs
- Analyzing system logs
- Analyzing application logs
- Identifying Indicators of Compromise
- Configuring file permissions
- Evaluating passwords
- Evaluating authentication systems
- Identifying malware
- Identifying network attacks
- Identifying application attacks
- Performing vulnerability assessments
- Recommending security controls
- Hardening devices
- Evaluating security policies
- Documenting findings
- Explaining cybersecurity decisions using evidence

The course should include hands-on, career-relevant work such as scenarios, case studies, cyber-range activities, and cybersecurity competitions.

AP Cybersecurity Exam

Section I - Multiple Choice

- 60 questions
- 80 minutes
- 70% of AP Exam score
- Includes individual questions and question sets based on cybersecurity scenarios
- Students analyze scenarios and digital evidence, identify vulnerabilities and attacks, recommend mitigations, recognize IoCs, and explain cybersecurity concepts.

Section II - Free Response

- 1 free-response question
- 50 minutes
- 30% of AP Exam score
- Device Security Analysis
- Sources may include security policies, firewall rules, system logs, application logs, and file-system permissions.
- Students identify security problems, detect evidence of attacks, interpret policies, configure or recommend file permissions and firewall rules, explain impacts, recommend improvements, and cite evidence.

The first regular AP Cybersecurity exam for the 2026-27 school year is scheduled for May 5, 2027 and is fully digital through Bluebook.

Recommended Yearlong Teaching Sequence

Weeks	Focus	Topics
Weeks 1-4	Unit 1 - Introduction to Security	Cybersecurity fundamentals, threats, adversaries, social engineering, authentication, AI, and risk.
Weeks 5-8	Unit 2 - Securing Physical Spaces	Physical vulnerabilities, physical attacks, controls, policies, and detection.
Weeks 9-17	Unit 3 - Securing Networks	Networking fundamentals, wireless security, network attacks, segmentation, firewalls, and log analysis.
Weeks 18-26	Unit 4 - Securing Devices	Operating-system security, malware, authentication, permissions, endpoint security, and device logs.
Weeks 27-33	Unit 5 - Securing Applications and Data	Application attacks, access controls, encryption, data protection, and application logs.
Weeks 34-35	Integrated Security Analysis	Combine network logs, device logs, application logs, firewall rules, file permissions, and security policies.
Weeks 36-37	AP Exam Review	Emphasize risk analysis, attack identification, IoCs, firewall rules, file permissions, log analysis, evidence-based explanations, and Device Security Analysis FRQs.

Simplified AP Cybersecurity Framework

8. Identify what needs to be protected.
9. Identify the vulnerability.
10. Identify the threat or attacker.
11. Determine the risk.
12. Select a mitigation.
13. Implement the security control.
14. Monitor the system.
15. Detect evidence of an attack.
16. Analyze the evidence.
17. Harden the system and document the solution.

This sequence reflects the College Board emphasis on Analyze Risk -> Mitigate Risk -> Detect Attacks while applying those skills across physical spaces, networks, devices, applications, and data.

Sources

College Board AP Central - AP Cybersecurity: <https://apcentral.collegeboard.org/courses/ap-cybersecurity>

College Board AP Students - AP Cybersecurity: <https://apstudents.collegeboard.org/courses/ap-cybersecurity>

College Board AP Central - AP Cybersecurity Exam:
<https://apcentral.collegeboard.org/courses/ap-cybersecurity/exam>

College Board AP Central - AP Cybersecurity Course Audit: <https://apcentral.collegeboard.org/courses/ap-cybersecurity/course-audit>