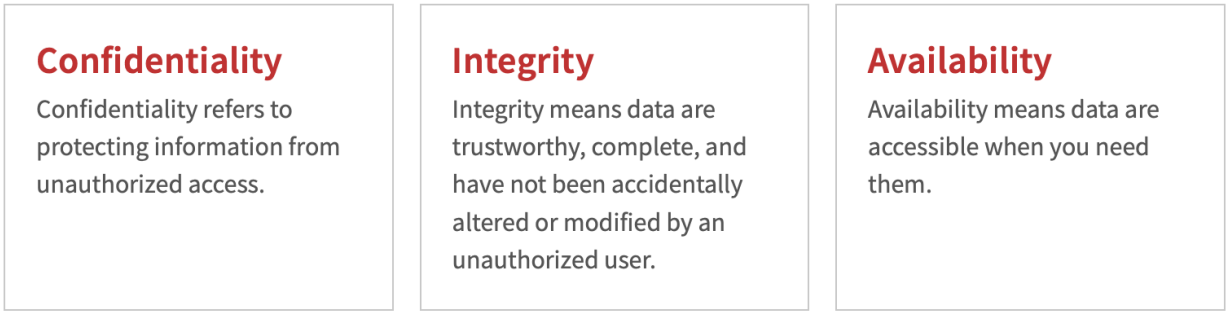
AP cybersecurity intro: CIA triad

Notes:

- intro-who
- intro-why cybersec: real people losing things that matter
- interest? code? infrastructure? policy?
- articles and notes by email: bill@hpa.edu
- HCRW text
- "Writing code itself is useless, but learning system architecture will turn you into a genius"
- FedEx sign-you will not see things the same way after this course
- First year of AP cyber (APCS)-we get to design the course-no comparison
- inventory machines-mac? M class?
- metaphors:
  - highway metaphor-car is your computer, road is the internet
  - house metaphor-burglars casing your neighborhood then your home
- cyberthreat game:

(syllabus is at the bottom)

Cybersecurity is about real people and the things they value, threatened by other real people
CIA Triad:



Screenshot 2026-08-07 at 5.35.11 AM.png

- **Confidentiality**-is my stuff secret? from whom?
- **Integrity**-is my information intact? has it been changed?
- **Availability/Access**-can I access my information, my devices, my systems? Ransomware?

HPA, myHPA

- grades changed
- 24x7 operation (boarders)
- needs food and water for all
- billing locked by ransomware
- student records released

Queens Hospital

- 24 hour operation
- critical life and death consequences
- patient records are private
- surgeries cannot be delayed
- ambulances may be diverted
- many devices are internet connected (drug drips, X-rays, CT)
- patient information needs to be accessed 24x7
- patient portal needs to be accurate and open (appointments)
- older systems not hardened, little tech support

Hawaiian Airlines

- 24 hour operation (planes in the air, planes on the ground)
- ticketing, reservations must be operational
- fuel, logistics, personnel need to be in the right places
- flights delayed, customers stranded
- financial data must be confidential (competition, labor)
- tech support mainly works on web front end, not cybersec
- inbound freight and mail are delayed

Local Law firm

- sensitive information needs to be confidential (from opponents)
- financial settlements need to be private
- access to records is critical
- integrity of documents is critical (cases, agreements)
- paid tech support, maybe not on site

Kamuela Board of water supply

- 24x7 operation of water treatment and pumping

- remote control of valves, pumps and storage tanks
- regulation of critical systems (pipe pressures)
- billing needs to be private and reliable
- data on use needs to be accurate
- older remote systems (SCADA) with little tech support

Small Doctor’s office

- daily use
- HIPAA regulations (fines for each record released)
- drug prescriptions must be private and accessible
- usually little or no technical background

Personal savings account

- many home users have no tech support
- savings accounts can be emptied
- identity fraud if records are accessed
- remote control of computer can gather all passwords

Smart home

- security cameras viewed remotely
- critical devices inoperative (hot water, lighting, cooking)
- access to personal data (banking)
- little or no tech support

Young brothers barge service

- navigation disrupted-groundings
- fuel and consumables miscalculated-stranded
- scheduling and personnel disrupted
- access to financial records blocked
- access to communications blocked
- could cause disruption in life on our island (fuel, water, electricity)

Case Studies:

Hospital Ransomware

Industry: Healthcare
Observed Symptoms
• Doctors cannot access patient records.
• Surgeries are delayed.
• Ambulances are diverted.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Availability

Screenshot 2026-08-07 at 5.27.44 AM.png

Airline Reservation System

Industry: Transportation
Observed Symptoms
• Reservation system unavailable.
• Thousands of flights delayed.
• Passengers stranded.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Availability

Screenshot 2026-08-07 at 5.27.55 AM.png

Personal Savings Account

Industry: Finance
Observed Symptoms
• Savings account emptied.
• Fraudulent transfers detected.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Confidentiality

Screenshot 2026-08-07 at 5.28.05 AM.png

High School Grades

Industry: Education
Observed Symptoms
• Grades unexpectedly changed.
• Students dispute records.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Integrity

Screenshot 2026-08-07 at 5.28.15 AM.png

Water Treatment Plant

Industry: Critical Infrastructure
Observed Symptoms
• Chemical settings changed.
• Public safety concern.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Integrity

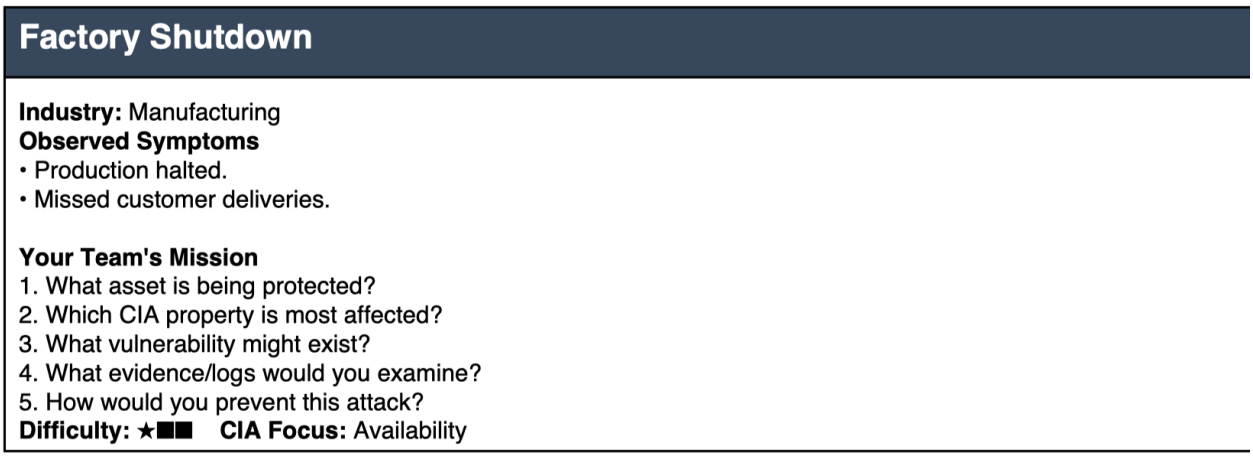
Screenshot 2026-08-07 at 5.28.25 AM.png

Smart Home

Industry: Consumer IoT
Observed Symptoms
• Security cameras viewed remotely.
• Family privacy lost.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Confidentiality

Screenshot 2026-08-07 at 5.28.47 AM.png



Screenshot 2026-08-07 at 5.28.56 AM.png

Download AP_Cybersecurity_Investigation_Cards_v2.pdf (application/pdf, 16.5 KB)

Download AP_Cybersecurity_Breach_Cards.pdf (application/pdf, 8.2 KB)

Syllabus==========

Welcome to AP Cybersecurity!

As this is the first year we are offering this course, it will expand on our previous semester courses of Computer Engineering and Cybersecurity.

This is a fast moving topic, and I'll be sharing articles and videos to help you keep up.

As an AP course, you know there is a GPA bump for this class, and I think we can boil down our work into three buckets:

- Homework: turned in on time for credit, half points if turned in before our next class.
- Labs: most of our work will be hands-on labs, to how we weight this may change
- Quizzes: I like to check in at the beginning of each class with a quiz, but I'm flexible on how we do this. I don't prefer humongous tests, but as this is an AP course, we'll be doing some evaluations from the college board to see how we are progressing.

Goals:

Our goal is safety in a digital world.

Cybersecurity is about protecting real people from other real people who want to do them harm.

Some of these “black hats” are now using AI, giving them superpowers that we will learn about.

Your superpower is the 20Watt computer you have between your ears: you are a creative, curious human, and that combination always wins out.

Much of what we will do together might seem like a detective mystery.

To use a highway metaphor-your car is your computer, your road is the internet.

Another way to look at security is protecting your house from a burglar.

To learn how to defend yourself and others in this changing landscape, we will be learning about common threats (the CIA model), and how best to protect yourself from these threats.

We’ll also create mock-attacks using “blue team vs. red team” games, which are loads of fun.

Cybersecurity exists on several levels:

- **Physical**: wired and wireless networks, fiber networks-how do they work, how are they vulnerable
- **Logical**: How does information pass through these networks: protocols, transport, machine to machine communications, hacking, code, operating systems, firewalls, Ddos, encryption, passwords, malware, clam AV,
- **Social/Human:** vulnerabilities, social engineering, spoofing, digital forensics, phishing, AI aided phishing, ransomware

Tools:

We will be using several levels of tools to research these, including your laptop, so we will discuss what laptop you have, and what tools you can load onto it.

Know that we will never use your laptop in an attack-defend role: your laptop is your private property, we have other machines in the elab for that.

Resources:

Along with shared articles and videos, we have several texts on pdf we will use. These can be found on the cybersecurity pages at elab.hpa.edu, login will be shared in class.

Me:

My email is the shortest in the world: bill@hpa.edu (when you run the network, you get to pick your address, one good reason to get into cybersec).

If you can email your homework before 7 PM, I can read it and give you suggestions and comments to get more points and better understand the material.

You:

How to succeed?

- Take notes in class-we may make this a graded exercise, points for notes, let's discuss in class
- Reach out when you are stuck: you are busy, with other class loads, sports, and a vibrant social life (we hope). Let me know how I can help, that's why I'm here.
- Collaborate: this will be your secret weapon in college, but be careful: college computer courses will fail you and send a letter to the dean if you copy work, including code. I know this first-hand. (ask).
- AI: you would not send a robot to the gym to do your workout, but it might make a helpful workout partner. Know that I use AI a great deal with my programming, but my ideas are mine. Anything you submit with your name for credit must be your thinking, not the collective slop of the silicon intelligence.

Course description: from the course catalog…

This course introduces students to the fundamentals of cybersecurity through interactive activities, real-world case studies, and hands-on labs. Students will learn how to stay safe online, understand how cyberattacks work, and explore careers in cybersecurity. The course builds critical thinking, ethical awareness, and technical confidence using both unplugged and online tools.

Course Objectives:

- Understand the core principles of cybersecurity (confidentiality, integrity, availability)

- Identify different types of cyber threats and attacks

- Practice safe online behaviors and password hygiene

- Explore ethical hacking and digital forensics

- Learn about network security, cryptography, and firewalls

- Investigate career paths in cybersecurity

As always, reach out to me if you have any questions.

aloha

b

Migrated from Apple Server Wiki. Original page ID: e703f1P7

Revision #3
Created 2026-09-29 16:00:08 UTC by Admin
Updated 2026-09-29 16:49:32 UTC by Admin