UNIT 2: CIA Triad

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 6 Adversarial Thinking 1 Ethics 5 System Security	2.1	- Research history breaches and tie them to confidentiality, integrity, and availability.

Guiding Questions:

- What is the CIA triad, and why is it important?
- Who/what threatens CIA?
- Why do we need CIA?
- How do we protect confidentiality, integrity, and availability?
- What needs integrity?
- What do businesses do when systems go down?
- What is the CIA tradeoff?
- What's legal?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.1 EU Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad).	• Computer, lecture slides, projector, graphic organizers • "Sneakers (4/9) Movie CLIP - No More Secrets (1992) HD." *YouTube*, uploaded by Movieclips, 29 May 2011, https://www.youtube.com/watch?v=F5bAa6gFvLs&feature=emb_logo	• Show movie clip from *Sneakers* linked left. What were the hackers trying to gain access to? What would happen if someone gained control of these things in real life? Point out that the Federal Reserve attack is a loss of confidentiality, the power grid attack is a loss of availability, and the air traffic control attack is a loss of availability. • These three things (confidentiality, integrity, and availability) are what cybersecurity experts try to protect. They compose the CIA triad. • Show the video linked left to introduce the CIA triad.

	• "What is the CIA Triad?" *YouTube*, uploaded by Netwrix, 25 February 2019, https://www.youtube.com/watch?v=xtlFO8Q2GDQ&feature=emb_logo	
6.2.2b: EK The manner in which an adversary carries out their intentions (sometimes called attacks) is related to their capabilities and the resources they can bring to bear. 6.2.2a EK: The intentions of adversaries can be classified as theft, disclosure, disruption, destruction, and/or subversion.	• "CIA Triad." *Quizizz*, created by kimswhite, 2019, https://quizizz.com/admin/quiz/5d6543fd91225c001d7bf45a/cia-triad	• Ask students to list thing that threaten the CIA triad. Be sure to note that these threats include natural disasters, human error, and attackers. • What types of attackers do they know about? Possible answer: nation states, hacktivist, criminals, insider threats, and script kiddies. Review these categories. • Have students list the motivations of these adversaries (see 6.2.2a EK). • Have students play the Quizizz game linked left.
2.1.1a EK: Confidentiality is the protection of information from disclosure to unauthorized parties 2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret	• Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST*, https://nvlpubs.nist.gov/nistpubs/SpecialPublica	• Have students discuss things they want to keep confidential. How do they keep these things confidential? • Discuss prevention, detection/analysis, containment, and post-incident activities. The booklet linked left is an excellent resource for this and could be used for a jigsaw activity or group research project. • Note that controls are ways to secure confidentiality. These include physical, technical, and administrative controls.

2.1.1e EK: Assuring confidentiality includes prevention, detection, containment, and response mechanisms. 2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret 2.1.1b EK: File permissions are a mechanism to control access to only those authorized. 2.1.1c EK: Cryptography is necessary to ensure confidentiality and integrity. 2.1.1d EK: Hiding is another aspect of confidentiality.	tions/NIST.SP.800-61r2.pdf • "Steganography Online." *GitHub*, created by stylesuxx, 2014, http://stylesuxx.github.io/steganography/	• Explain that file permissions are an example of a technical control. Provide examples of this. • Another technical control is cryptography. Explain the definition and purpose of cryptography. • Another way to keep information confidential is data hiding. Steganography is an example of this. There are many online tools available that can be used for steganography. One of those tools is linked left. It is a good idea to create examples of steganography for students to find. These can later be compared to the originals by hashing the files (when integrity is covered).
2.1.2a EK: Integrity is the trustworthiness of data or resources. 2.1.2d EK: Integrity mechanisms include prevention, detection and response mechanisms.		• Ask students if they have ever heard of someone pretending to be someone different online. Is this okay? Why or why not? When a person does this, they lose integrity. Explain the concept of integrity. • What are some other things that we want to be able to trust (files, processes, and systems)?

2.1.2c EK: Data integrity is the information changing in authorized ways by authorized people, often called authentication. 2.1.2 LO: Students will demonstrate that integrity involves trust and credibility. 2.1.2b EK: Assurance is determining how much and in which way to trust a system.		• Discuss ways that files, processes and systems can lose integrity. Cover integrity mechanisms with students (prevention, detection, and response). • A hashing exercise is a good activity here. Discuss ways people authenticate into a system.
2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. 2.1.3aEK: Availability of information refers to ensuring that authorized parties are able to access the information when needed. 2.1.3b EK: Denial of service attacks are attempts to block availability.	• Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST.gov*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf • Schwartz, Samantha Ann. "Black Friday traffic brings down J. Crew, Ulta sites,	• Ask students about a time when they lost Wi-Fi, cell service, or access to a resource (crashed website). How did it impact them? Explain that availability is also important. • Describe a denial of service (DoS) attack. • Have students list ways to defend against a DoS attack. • Using the NIST Computer Security Incident Handling Guide, have students research each stage (as mentioned above). Have students notice that prevention, detection, and response help assure availability. • Have students read the article linked left. How does being down impact online retailers?

2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. 6.2.2d EK: Incident response includes provisioning for the confidentiality, integrity and availability of cyber systems under attack by adversaries. 2.1.3c EK: A disaster recovery plan (DRP) includes backups, redundancies, system dependencies, and alternate sites. 2.1.3d EK: Assuring availability includes prevention, detection, and response mechanisms. 1.2.1b EK: There are trade-offs concerning the harms and benefits of cybersecurity, including the tensions between ensuring privacy and enabling convenience and usability. 6.2.2 LO: Students will know how intentional attacks can adapt to	among other retailers." *CIO Dive*, 26 Nov. 2018, https://www.ciodive.com/news/black-friday-traffic-brings-down-j-crew-ulta-sites-among-other-retailers/542926/ • *Cyberthreat Real-Time Map*. Kaspersky, https://cybermap.kaspersky.com/	• Discuss tradeoffs related to the CIA triad. Have students list examples. • Explore the threat map linked left with students. Explain that systems are constantly under attack and that adversaries are constantly adapting and changing their tactics, making CIA even harder to maintain.

defenses and cause a system to fail.		
1.3.3c: EK Using the anonymity of the internet for behavior that can harm others may not be illegal. 6.2.2c EK: Cyber systems are susceptible to attack from human adversaries. 5.4.1 LO: Students will identify historical consequences of software and hardware vulnerabilities, e.g., power outages, death, theft of trade secrets from other sovereign nations. 5.4.1a EK: Software vulnerability examples that resulted in a loss of confidential data including breaches of credit information (Equifax), healthcare information (Anthem), government records (OPM data breach), home assistants (Amazon Echo hacks), baby monitors (many examples), and fitness tracker data (mapping military bases).		• Another problem impacting CIA is the fact that laws are different all over the world. In some cases, adversaries in other countries are not breaking the law in their home country. • Also, adversaries target more than just desktops and laptops. They target various types of cyber systems. Provide students of examples of this. • Have students research the examples listed in EKs 5.4.1a-5.4.1d, noting how they impacted CIA. This would be a great poster activity.

5.4.1b EK: Software vulnerability examples that resulted in a loss of confidential data and corresponding monetary losses for the victims including intellectual property theft and ability to directly access financial data. 5.4.1c: EK Software vulnerabilities examples that resulted in a loss of integrity such as man in the middle attacks (many examples), compromise industrial control systems (i.e. Stuxnet), vehicle control systems (Jeep Cherokee hack), and medical devices (Medtronic infusion pumps). 5.4.1d EK: Software vulnerability examples that resulted in a loss of availability such as DDoS attacks on websites (Mirai botnet), ransomware that locks outs access to data (WannaCry, Petya, NotPetya), Telephony Denial of Service (attacks on 911).		

8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		• Invite a local cybersecurity professional to showcase their career to your classroom. Hold a Q&A session for the students.