UNIT 6: Data Security Concerns

Estimated Time in Hours: 6

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 1 Ethics 8 Implications	4.1, 4.2	- Research common password recovery questions and determine how users can be tricked into supplying the information. - Research cyber warfare. - Research security clearances and the actions that can prohibit a person from qualifying for one. - Research what to do in the instance of identity theft. Using a VM, have students set up role-based and rule-based access controls. - Complete a hashing lab.

Guiding Questions:

- What is data confidentiality?
- What can be learned from someone's data, and how could a hacker use this information?
- What are the harms and benefits of data protection?
- What is cyber warfare?
- How is data managed and protected?
- How can people harm data?
- What is data security?
- What are different types of access control?
- What is origin integrity, and how do you prove it?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Ask students if they have ever experienced or known someone who experienced identity theft, an online account takeover, a direct cyber attack, or a breach. Have them compare their experience with the 2018 national

4.1.1g EK: Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.	• "ITRC Surveys, Studies and Whitepapers." Identity Theft Resource Center, *IDTheftCenter.org*, https://www.idtheftcenter.org/surveys-studys/ • "2018 End-of-Year Data Breach Report." Identity Theft Resource Center, *IDTheftCenter.org*, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf	results (identity theft = 15.23%, online account takeover = 22.84%, direct attack = 38.41%, and breach = 43.32%). Explain to students that every time that happens you are suffering an attack on confidentiality. • The site linked on the left has a lot of information for students to explore regarding identity theft. It also has an infographic (linked left) with fast facts you can discuss with the class. The PDF also highlights breaches by type, industry, and types of information exposed. • Have students look at the definition of data confidentiality and explain why it is important. • Discuss data types (regulated, PII, business/commercial, and collaborative data). Have students provide examples of each type.
4.1.1a EK: Data can reveal much about people, their thoughts, and lives; which makes personally identifiable information highly sensitive.	• Collins, J. Carlton. "Online security: The password-recovery questions you should be answering." Journal of Accountancy, *JournalOfAccountancy.com*, 1 Mar 2018, https://www.journalofaccountancy.com/issues/2018/mar/password-recovery-questions.html	• Ask students things an attacker can learn from someone's social media account, buying history, medical records, or browser history. • Tell students they have to come up with their own hacker names based on their favorite food and their mother's maiden name. Before they reveal their answers, ask them why this a bad idea. Ask if they have seen similar "games" on social media.

	• "Social Media Habits & You: Trend Analysis 2018." Identity Theft Resource Center, *IDTheftCenter.org*, https://www.idtheftcenter.org/wp-content/uploads/2018/10/ITRC_CyberScout_Social-Media-Habits-and-You-Survey_Trend-Analysis_2018_Web.pdf	• Have students research common password recovery questions (see link to left). How could attackers find this information? How could they leverage this knowledge? • How could attackers leverage social against a target? • Why would attackers target the social media accounts of people who work for organizations?
8.1.1c EK: Events in cyber warfare and cybercrime escalated the need for increased cybersecurity efforts 1.2.1 LO: Students will discuss how cybersecurity can significantly impact the quality of people's lives both positively and negatively. 1.2.1a EK: Examples in history demonstrate the harms and benefits of cybersecurity from multiple perspectives.	• Garrie, Daniel. "Defining cyberwarfare…in hopes of preventing it." *YouTube*, uploaded by TED-Ed, 20 Aug 2013, https://www.youtube.com/watch?v=ZVoDwtyvDJc&feature=emb_logo • *U.S. Army Cyber Command*. United States Army, https://www.arcyber.army.mil/ • "Fact Sheets." *U.S. Army Cyber Command*,	• Ask students if there is a "downside to cybersecurity." Possible answers are it being user centered (users are a weak link), it makes access slower, it can be expensive and become outdated quickly, the solutions can be used by criminals to hide from law enforcement. • Discuss the definition of cyber warfare. The video linked on the left may help with this. Have students research the role of the U.S. in cyberwarfare. Using the fact sheets linked on the left, ask students to create a presentation or poster on a cybersecurity-related topic.

	https://www.arcyber.army.mil/Info/Fact-Sheets/	
4.1.1b EK: Data can be used to help individuals, but it can also be exploited to harm individuals. 4.1.1c EK: Data must be protected in processing, transmitting and storage 4.2 EU: Data Security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted and stored.	• "Developing and Using Security Classification Guides." Published by the Information Security Oversight Office (ISOO), updated Oct 2018, accessed via the National Archives, *archives.gov*, https://www.archives.gov/files/isoo/training/scg-handbook.pdf • Christensen, Michelle D. "Security Clearance Process: Answers to Frequently Asked Questions." Published by the Congressional Research Service, 7 Oct 2016, accessed via Federation of American Scientists, *fas.org*, https://fas.org/sgp/crs/secrecy/R43216.pdf	• Of course, the main weapon in cyberwarfare is data. Remind students of the three states of data (at rest, in motion, and in use). Point out to students that data must be protected in all three states. Have students map possible attack to the three data states. For example, Ransomware targets data at rest. • Discuss how data security utilizes technical and non-technical controls. One of these is through data classifications. Discuss data classifications used by businesses and government. How are they alike? How do they differ? • Using the document linked on the left, have students read about classification requirements and do the Three Little Pigs activity in the booklet. Next, have them research eligibility requirements for a security clearance and the investigation process.
4.1 EU: Data security deals with the integrity of the data, i.e., the protection from corruption or errors; the privacy of data; and	• Boadu, Edwin Okoampa and Armah, Gabriel Kofi. "Figure 1.1: Relationship Between Hospital	• Discuss access management with students (identification, authentication, authorization, and accounting). Provide the definition and examples.

data confidentiality, i.e., it being accessible to only those who have access privilege to it. 4.1.1d EK: The purpose of personal data protection is not to merely protect a person's data, but to protect the fundamental rights, freedoms, and welfare of persons who are related to that data 4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns.	Workers and Privilege." Role-Based Access Control (Rbac) Based in Hospital Management, *International Refereed Journal of Engineering and Science*, Vol. 3, Issue 9, Sept 2014, http://www.irjes.com/Papers/vol3-issue9/H395367.pdf	• Explain the purposes of data protections. Have students consider the emotional ramifications to users and the time lost in addition to the loss of privacy and financial impact. • Discuss data security strategies (physical, technical, and administrative). Provide examples of each. • Give students different scenarios and have them list physical, technical, and administrative controls to use in each scenario. • Discuss various access control models (MAC, DAC, RBAC, and RuBAC). Have students pick one and create a slideshow or poster with the characteristics and use case for each model. Figure 1.1 in the report linked to the left is an example of what the students could create. In a VM, have students set up a role-based and rule-based access control Example: Windows Live Family Safety
4.1.1f EK: Origin integrity means the original data is trustworthy, and its source is trusted to produce trustworthy data. 4.1.1e EK: Data integrity means only authorized changes are made only by authorized people. 8.1.1h EK: Cybersecurity events have led to the development of		• Ask students if they would like a $100 bill. What about a fake $100? Which is more valuable? Why? • Tie this to original integrity. It is important that we are able to trust data. Have students brainstorm examples where origin integrity would be important. Discuss how hashing helps prove origin integrity and how the access control models help create origin integrity. • Tie this unit to a cybersecurity career like cybersecurity architect.

various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		