Bastian | Planning & Pacing Guide

UNIT 7: HISTORY & ECONOMICS OF CYBER   **Estimated Time in Hours: 6-8**

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 6 Adversarial Thinking 8 Implications	5.2, 5.4, 6.1, 8.1, 8.2, 8.3	- Information Campaign Presentation - Phishing Simulation - Supply Chain Case Write-up - Targeted Attack Simulation

Guiding Questions:
- How have historical cybersecurity ideas and events impacted society?
- How has the expansion of the threat environment been addressed in society?
- How do risk management and economic trade-offs impact cybersecurity decisions?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design. EK: 6.1.4a,b 8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field. EK: 8.1.1a,b,d 8.2.1 LO: Students will describe how political ideologies, economic structures, social	- Notebook "How the Kim Dynasty Took Over North Korea | History." *YouTube*, uploaded by HISTORY, 27 Apr 2018, https://www.youtube.com/watch?v=56c6W8EGfcA&feature=youtu.be - Galante, Laura. "How (and why) Russia hacked the US election." *YouTube*, uploaded by TED, 25 May 2017,	**Information Campaigns: (1 - 2-day lesson)** In this lesson students learn how information campaigns were used and considered vital throughout history impacting the ruling family in a country and creating chaos in a US election. The lesson begins with students brainstorming in their notebook, writing what they know about information campaigns and any campaigns they know about. Students then watch the video on the Kim Dynasty. There is then a class discussion about how the Kim Dynasty was put in place and has maintained power through an information campaign. Students go back to their notebook and reflect on what they have learned. Students then watch the video on How (and why) Russia Hacked the US election. The class discusses the video. After watching the video, students listen to the Influence Operation Kill Chain Podcast (stop at 17 min 40 sec). Students then discuss what they learned from the How

organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1a,b	https://www.youtube.com/watch?v=TO-_kVIkY6A&feature=youtu.be • Operation Kill Chain Podcast (stop at 17 min 40 sec): Schneier, Bruce and Henage, Dan. "Crypto-Gram September 15, 2019." *The Crypto-Gram Security Podcast*, Libsyn, 15 Sep 2019, https://hwcdn.libsyn.com/p/5/f/a/5fad7065005f08b5/crypto-gram-2019-09.mp3?c_id=54940355&cs_id=54940355&destination_id=19374&expiration=1595269974&hwt=2283dfea4d63724de9cc5d77c5aa8c06	(and why) Russia Hacked the US election and the Influence Operation Kill Chain Podcast. Students then research information campaigns throughout history. They select a campaign and create a brief presentation on the campaign.
6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design. EK: 6.1.4a,b	• Notebook • Lord, Nate. "What is Social Engineering? Defining and Avoiding Common Social	**Social Engineering: (1-day lesson)** In this lesson students will learn how social engineering works and how it is used to design effective phishing attacks. • The lesson begins with the phishing video to introduce the topic. After the video the students reflect in their notebook about the strategy of social engineering used.

	Engineering Threats." Data Insider Blog, *DigitalGuardian.com*, 11 Sep 2018, https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats#:~:text=Social%20engineering%20is%20a%20non,into%20breaking%20standard%20security%20practices.&text=When%20successful%2C%20many%20social%20engineering,authorized%20access%20to%20confidential%20information. • Phishing Video: "It Wasn't Me - #SecureYourAccount." *YouTube*, uploaded by Dubai Police, 27 June 2019, https://www.youtube.com/watch?v=HTkdw	Students then read about social engineering. After reading about social engineering students watch a 3-minute video on a form of social engineering. The class then discusses social engineering. The lesson is wrapped up with students completing a phishing simulation.

	[nwAqlg&feature=youtu.be](#) • Social Engineering Video: "This is how hackers hack you using simple social engineering." *YouTube*, uploaded by oracle mind, 1 May 2016, [https://www.youtube.com/watch?v=lc7scxvKQOo&feature=youtu.be](#) • Phishing Simulation: "What is phishing?" Living Security, [https://phishing.livingsecurity.com/](#)	
8.3.3 LO: Students will describe how economics shape the decisions of consumers. EK: 8.3.3b,c	• "CS Principles 2017 | Unit 4 | Ch. 1 | Lesson 4: The Cost of Free." *Code.org*, [https://curriculum.code.org/csp-1718/unit4/4/](#)	**Consumers: (1-day lesson)** In the first day of the lesson students learn about how they have to give away their data in order to fully participate in today's economy. • Day 1 - Follow the Code.org "The Cost of Free" lesson.
5.2.2 LO: Students will know some common hardware-related vulnerabilities EK: 5.2.2a,b	• Notebook • Supply Chain Security & Trust Podcast:	**Supply Chain: (1-day lesson)** In this lesson students learn what a supply chain is, what the risks are and best practices to minimize the risks.

5.2.3 LO: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle. EK: 5.2.3a,b,c	Schneier, Bruce and Henage, Dan. "Crypto-Gram October 15, 2019." *The Crypto-Gram Security Podcast*, Libsyn, 15 Oct 2019, https://hwcdn.libsyn.com/p/1/4/1/141a42757fb7e7a1/crypto-gram-2019-10.mp3?c_id=56423036&cs_id=56423036&destination_id=19374&expiration=1595268544&hwt=a330ee278baf60848a9ff35ed7bb5bab • Soare, Bianca. "Supply Chain Cybersecurity: What Are the Risks?" Heimdal Security, 21 Jan 2020, https://heimdalsecurity.com/blog/supply-chain-cyber-security/ • Duca, Sean. "Supply chain remains the weakest link in cybersecurity." Supply	• The lesson begins with students listening to a podcast about supply chain security. Students then read about supply chains and take notes in their notebook. The class discusses the supply chain. Students then research and find a supply chain issue. Students complete a 1 page write up on the issue. They identify the issue, explain what happened, how it happened, and how it could be prevented in the future or ways to minimize the issue.

	Chain, *SupplyChainDigital.com*, https://www.supplychaindigital.com/technology/supply-chain-remains-weakest-link-cybersecurity • "Best Practices in Cyber Supply Chain Risk Management." National Institute of Standards and Technology Computer Security Resource Center, *CSRC.NIST.gov*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf	
8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.	• Notebook • "'WEB WARRIORS' Documentary over cyber warfare." *YouTube*, uploaded by	**Cyber Warfare: (1-day lesson)** In this lesson students learn about cyber warfare and the impacts cyber warfare has on business and society. • The lesson begins with students completing a quick write in their notebook answering the following question:

EK: 8.1.1c,f,h 8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1a,b	Techofriendly, 18 Nov 2016, https://www.youtube.com/watch?v=0IY7DL0ihYI&feature=youtu.be	"What is cyber warfare?" Students then watch the "Web Warriors" video. Students take notes on the video. The lesson wraps up with a class discussion about cyber warfare.
8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1d,e 8.3.1 LO: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity. EK: 8.3.1a,b,c,d 8.3.2 LO: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers. EK: 8.3.2a,b,c,d	• "Targeted Attack: The Game." Trend Micro, http://targetedattacks.trendmicro.com/ • Notebook	**Business Experience Simulation: (1-2-day lesson)** In this lesson students walk through a business simulation where they will have to make the proper choices based on the information given in order to avoid a successful cyber attack against the company. • The lesson begins with students being introduced to the Targeted Attack simulation. Students work through the simulation, making decisions about how to address cyber issues while maintaining the budget and keeping the project on target. Once students complete the simulation they reflect in their notebook what went right or wrong. If they failed the simulation, they can go back through it to see where they made mistakes. The class is wrapped up with a discussion about the standards addressed in this lesson.

8.3.3 LO: Students will describe how economics shape the decisions of consumers. EK: 8.3.3a,d		