

UNIT 8: Cybersecurity Business Economics

Estimated Time in Hours: 8

<p><u>Big Idea(s)</u> 8 Implications 1 Ethics</p>	<p><u>Enduring Understandings</u> 8.3, 1.3</p>	<p><u>Projects & Major Assignments</u> - Examine terms of service agreements for various companies to create a wall of fame and wall of shame. - Research the reactions of businesses after breaches to determine the level of transparency.</p>
<p>Guiding Questions:</p> <ul style="list-style-type: none"> • If you are buying a piece of technology, how do you decide what to purchase? What factors do you consider? • Do consumers view security as a selling feature? • Why do companies struggle with cybersecurity? • How should companies address cybersecurity? • What happens if a company does not invest in cybersecurity? • Why do businesses get cybersecurity wrong? • Are businesses prepared for cyber attacks? • What do businesses stand to lose for being unprepared? • How does supply chain impact cybersecurity? • What do consumers need from businesses regarding cybersecurity? 		
<p>Learning Objectives & Respective Essential Knowledge Statements</p>	<p>Materials</p>	<p>Instructional Activities and Classroom Assessments</p>
<p>8.3.3 LO: Students will describe how economics shape the decisions of consumers.</p> <p>8.3.3a EK: Consumers are often driven by new functionality which is tangible while the security features of the product</p>	<ul style="list-style-type: none"> • Computer, lecture slides, projector, graphic organizers, access to Internet "Intro to Economics: Crash Course Econ #1." <i>YouTube</i>, uploaded by CrashCourse, 8 July 2015, 	<ul style="list-style-type: none"> • Ask students what factors into their decisions when making a technology-related purchase. What features are important to them? You might need to use a specific piece of technology as an example to narrow the scope (television, cell phone, tablet, etc.). Is security ever a consideration? What about for the average consumers; do they consider security?

Hairston_Williams | Planning & Pacing Guide

<p>may only be understood or appreciated when the security fails.</p> <p>8.3.1a EK: Economic value typically measures gains achieved, not losses avoided.</p>	<p>https://www.youtube.com/watch?time_continue=110&v=3ez10ADRgM&feature=emb_logo</p>	<ul style="list-style-type: none"> Depending on the students' background, they may need the video linked to the left to better understand economics. Why is economic value typically measured in gain achieved instead of losses avoided? Ask students for examples.
<p>8.3 EU: Measuring the economic value of cybersecurity is often an indirect process that relies on risk management trade-offs rather than direct benefits.</p>	<ul style="list-style-type: none"> Mňuková, Kateřina. "The Boat Game. Fun way how to teach your team start caring about the risks." <i>Medium, Medium.com</i>, 27 Mar 2018, https://medium.com/@katerina_mnuk/boat-game-62916dad70 Whiting, Jim. "Titanic–Not Enough Lifeboats." <i>iNK Think Tank, NonfictionMinute.org</i>, 2 May 2020, https://www.nonfictionminute.org/the-nonfiction-minute/titanic-not-enough-lifeboats Javaherdashti, Reza and Akvan, Farzaneh. "Figure 3: Risk Assessment Matrix." <i>On the Link Between Future Studies and Necessity of</i> 	<ul style="list-style-type: none"> Ask students how much a company should spend on cybersecurity? How much is enough? Use the game linked on the left to introduce the idea of risk managements. This game could be adjusted to fit the scenario of the Titanic using the information linked on the left.

Hairston_Williams | Planning & Pacing Guide

	<p>Including Corrosion in a 'Desired Future' Scenario: Presenting a Model, <i>International Journal of Engineering Technologies and Management Research</i>,. 24. 1-8., 2015, accessed via Research Gate, <i>researchgate.net</i>, https://www.researchgate.net/figure/An-example-of-a-Risk-Assessment-Matrix_fig3_283150764</p>	
<p>8.3.3d EK: Ill-informed consumers and businesses are prone to underinvest or invest in wrong solutions if they do not possess an accurate understanding of threats and defenses.</p> <p>8.3.1 LO: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity.</p>		<ul style="list-style-type: none"> • Ask students what happens if companies do not invest in cybersecurity? Have students investigate examples of this. • Explain to students that, for businesses, cyber attacks are difficult to predict, limited by bureaucracy, difficult to implement, and difficult to evaluate. Attacks are hard to investigate and prosecute. However, for the attacker, attacks are easy to produce, cheap to launch, easy to adapt, hard to investigate, and hard to prosecute.
<p>8.3.2 LO: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers.</p>	<ul style="list-style-type: none"> • Carfagno, Don. "How Much Should Your Company Invest in Cybersecurity?" CyberShark, 	<ul style="list-style-type: none"> • Have students research the impact of a cyberattack on small businesses. Suggest examples similar to the ones on the left.

Hairston_Williams | Planning & Pacing Guide

<p>8.3.1b EK: The lack of cybersecurity can cause substantial economic losses; including the compromise of sensitive data, the modification of critical data, the improper behavior of a system, or the unavailability of a system.</p> <p>8.3.1d EK: When misaligned incentives arise the party making the security–efficiency trade-off is not the one who loses out when attacks occur.</p> <p>8.3.1c EK: The lack of cybersecurity can result in major financial and reputational loss, but this loss only occurs after a successful attack.</p> <p>8.3.1d EK: Even in the event of a successful attack, the loss may or may not have lasting direct economic impact on the provider of the service.</p>	<p><i>BlackStratus.com</i>, 4 Nov 2018, https://www.blackstratus.com/how-much-should-your-company-invest-in-cybersecurity/</p> <ul style="list-style-type: none"> • Miller, Gary. “60% of small companies that suffer a cyber attack are out of business within six months.” <i>The Denver Post</i>. <i>DenverPost.com</i>, updated 24 March 2017, https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/ • “Cyber attacks – impacts and risk management for organisations.” <i>YouTube</i>, uploaded by Dentons, 26 Sept 2017, https://www.youtube.com/watch?v=gySzp3RrXjo&feature=emb_logo 	<ul style="list-style-type: none"> • Ask students what business have to lose if they do not invest in cybersecurity. The video linked on the left can help with this. • Discuss who else suffers when businesses are not prepared for an attack.
<p>8.3.2c EK: Cybersecurity risks occur when outsourcing the production or maintenance of</p>	<ul style="list-style-type: none"> • Wouk, Kris. “Where are iPhones Made?” 	<ul style="list-style-type: none"> • Explain to students that businesses also have to consider their supply chain. Have students research all the

Hairston_Williams | Planning & Pacing Guide

<p>technology to third party sources that may have different security practices.</p>	<p>MakeUseOf, <i>MakeUseOf.com</i>, 28 May 2019, https://www.makeuseof.com/tag/where-are-iphones-made/</p> <ul style="list-style-type: none"> Greenberg, Andy. "Supply Chain Hackers Snuck Malware Into Videogams." <i>Wired Magazine</i>, <i>Wired.com</i>, 23 Apr 2019, https://www.wired.com/story/supply-chain-hackers-videogames-asus-ccleaner/ 	<p>different countries where iPhones are made. Are all these countries trusted by the U.S.? Why would this be a concern for the U.S. military? Let students know that supply chain is not just a military concern. Have them read about the Asus supply chain breach linked to the left.</p>
<p>8.3.2d EK: Whenever security depends on the weakest link in the global supply chain, firms do not prioritize in investing in security when they know that other players will not invest, leaving them vulnerable in any case.</p>	<ul style="list-style-type: none"> "Software supply chain attacks explained." <i>YouTube</i>, uploaded by Windows, 10 Sept 2018, https://www.youtube.com/watch?v=uXm2XNSavwo 	<ul style="list-style-type: none"> Have students watch the video link on the left. How is supply chain security dependent on the weakest link?
<p>8.3.3b EK: In order to fully participate in today's economy, consumers must give away their data and agree to a company's terms that may conflict with their values.</p>	<ul style="list-style-type: none"> <i>Terms of Service; Didn't Read</i>, https://tosdr.org/ "How to Monetize Your Data." Lotame, <i>lotame.com</i>, 13 Jan 2020, 	<ul style="list-style-type: none"> Since not all companies have a consumer's best interest in mind, consumers need to consider how a company will use their information. This is often spelled out in a terms of service agreement. Have students pick a product or application they use and find the terms of service agreement. They should read the agreement, making

Hairston_Williams | Planning & Pacing Guide

<p>8.3.3c EK: Consumers are often unaware of the value of their information that they exchange for an incentive from a company that uses their data for monetary purposes.</p>	<p>https://www.lotame.com/how-to-monetize-your-data/</p>	<p>note of how the company handles their privacy. Next, students should visit the site on the left and see how the site rates companies (just scroll down upon getting to the site). Based on these criteria, what score would their choice have.</p> <ul style="list-style-type: none"> Ask students if it is okay for a free service (like Google for Facebook) to sell your browsing history to advertisers. Have students look at it from a business’s perspective by reading the article linked to the left.
<p>1.3.1 LO: Students will explore the tensions that exist between transparency, autonomy, resilience and security.</p> <p>1.3.1a EK: Transparency in cybersecurity is important for trustworthiness but can come at a risk to security.</p> <p>1.3.1b EK: Autonomy is the idea that every entity is in control of their own thoughts and actions.</p> <p>1.3.1c: EK Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.</p>	<ul style="list-style-type: none"> “Timehop Security Incident, July 4th, 2018.” <i>Timehop.com</i>, updated 11 July 2018, https://www.timehop.com/security/ “Four 9s vs Five 9s: What’s the Real Cost of the Difference?” Intelligent Fiber Network, <i>IntelligentFiber.com</i>, https://www.intelligentfiber.com/four-9s-vs-five-9s-whats-the-real-cost-of-the-difference/ 	<ul style="list-style-type: none"> Have students define the terms <i>transparency</i>, <i>autonomy</i>, <i>resilience</i> and <i>security</i>. How do these terms compete? Why are they important to consumers? Have students go to the linked information on the left and discuss this press release with students. How does it demonstrate transparency? Discuss autonomy and resilience with students. Ask students what percentage of the time they expect a service (like Google) to be up and running? How long can a service be down before it is considered unreliable? Discuss the 5 nines of uptime. The site linked to the left can help with this concept.

Hairston_Williams | Planning & Pacing Guide

<p>1.3.1d EK: Security is freedom from potential harm or other unwanted coercive change caused by others.</p> <p>1.3 EU: Cybersecurity practices are highly complex and variable causing tensions between what the ethical duties are, to whom the ethical concern should be considered, and whose interests should be invested in protecting.</p> <p>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.</p>		<ul style="list-style-type: none">• Discuss the meaning of “security is freedom.” What is the difference between security and privacy?• Have students debate why cybersecurity issues are complex and why tensions exist. See example below. <p>Example: Let’s say there is a small business suffers a data breach. It is small, and only a few people were impacted. Should the company make the breach public?</p> <ul style="list-style-type: none">- If they do, the company could go out of business and employees would lose their jobs.- If they don’t similar businesses might suffer a similar breach. <ul style="list-style-type: none">• Have students explore a career, such as executive cyber leadership.
---	--	---