Data Protection and Cyber Security

Producer: Pre-work	• There is a AhaSlides poll activity at the beginning of this session (page 4 of this guide). Talk to the facilitator to get the information and the link to the poll. • There is a Miro sticky note activity in this session (page 7 of this guide). Talk to the facilitator to get the information and the link to the virtual sticky note website. • There is a breakout room activity scheduled for this session on Slide 16 (page 9 of this guide). Collaborate with the Facilitator to decide if participants should be put into specific groups or if the groups can be chosen at random. There will be 3 groups of participants placed into 3 different rooms. • There is a Kahoot quiz game on slide 19 (page 10 of this guide). Talk to the facilitator to get the information and the link to the quiz.
	• Note that depending on the audience, the facilitator may be presenting the content for more than one phase during this session. Confer with the facilitator to ensure you know which phases will be covered.

Facilitator Pre-Work:	• This guide was developed for the purposes of delivering this course via Microsoft Teams, but it can also be used for classroom training with the following considerations: ○ AhaSlides poll on slide 6 (page 4 of this guide), and Miro sticky note activity on slide 12 (page 7 of this guide), a Breakout room activity on slide 16 (page 9 of this guide), and a Kahoot quiz game on slide 19 (page 10 of this guide) will need to be adapted to fit the classroom environment.
	• There is a AhaSlides poll activity at the beginning of this session on slide 6 (page 4 of this guide). Talk to the facilitator to get the information and the link to the poll.
	• There is a Miro sticky note activity in this session on slide 12 (page 7 of this guide). Talk to the facilitator to get the information and the link to the virtual sticky note website.
	• This session contains a breakout room activity on slide 16 (page 9 of this guide), where participants will need to be divided into 3 groups. Collaborate with the Producer about whether you feel those groups should be formed a certain way or if the Producer can make them at random.
	• There is a Kahoot quiz game on slide 19 (page 10 of this guide). Talk to the facilitator to get the information and the link to the quiz.

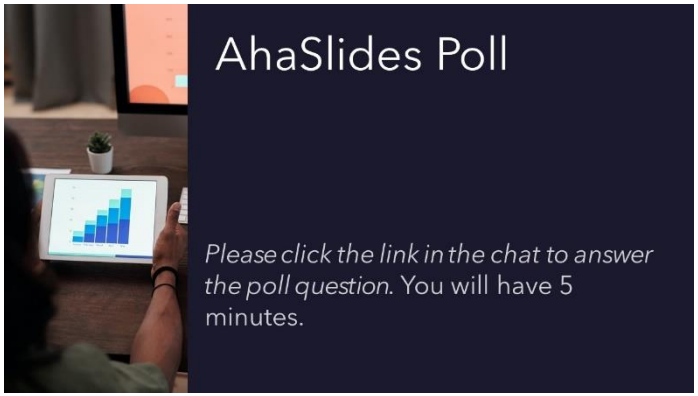
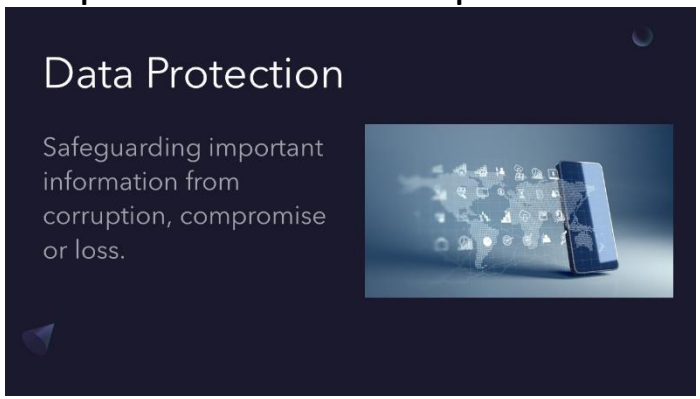
	• Open the PowerPoint file associated with this guide
	• Share the PowerPoint application and ensure that the Microsoft Teams *Attendees* and *Chat* panels are visible
	• Some key talking points and questions are included in this guide but be prepared to add your own commentary and questions as well.
	• Aim towards generating a response from the learner(s) at least once every five minutes; this will keep learners engaged and will encourage them to follow along closely. Examples of these types of responses have been noted using **ASK**

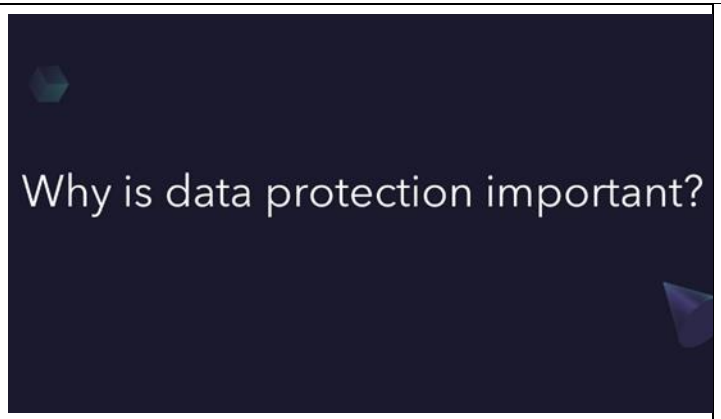
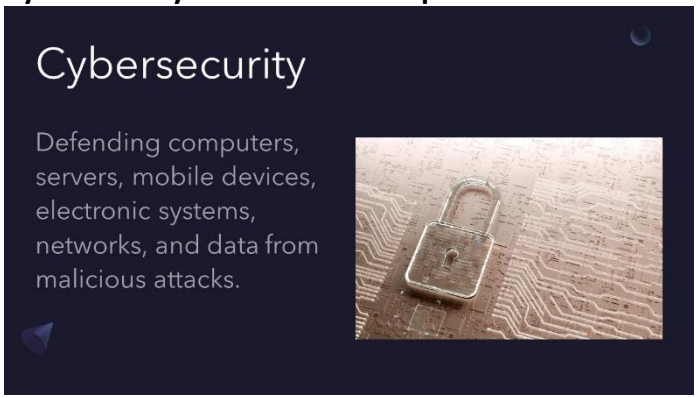
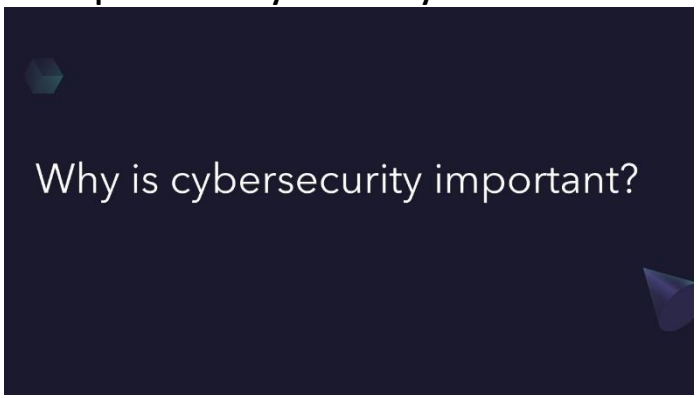
Session # 1		
Slides	**Approximate Timing**	**Topic**
1-3	5 minutes	Introduction
4-12	20 minutes	Introduction to Data Protection and Cybersecurity
13-16	13 minutes	Identifying and Protecting sensitive information
17-18	5 minutes	Securing Digital Assets and Infrastructure
19-21	12 minutes	Quiz and Closing
Total:	50- 55 minutes	

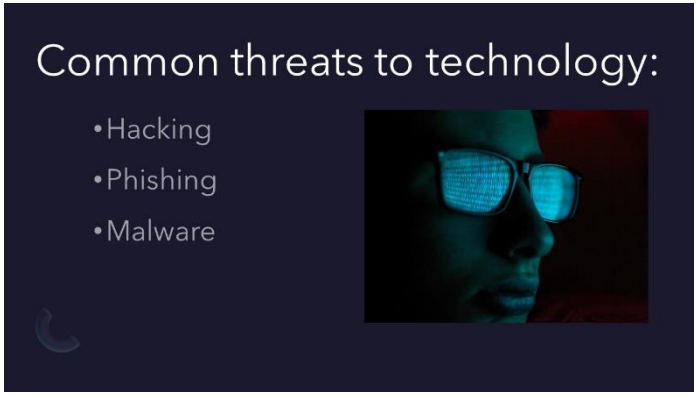
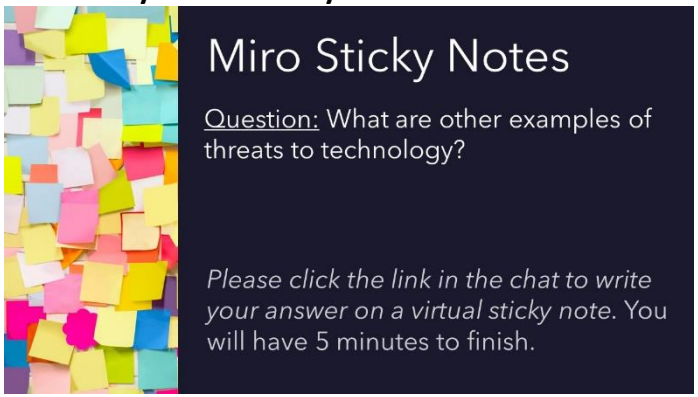
Slide#) Duration	**Slide**	**Facilitator Notes**	**Producer Notes**
1) Less than 2 minutes	**Title**	**Do**: − Welcome learners − Introduce yourself Remind learners that that the session will be recorded and will be available for their review.	**Do:** − Check for facilitator readiness **Say**: − Greet early learners as needed, letting them

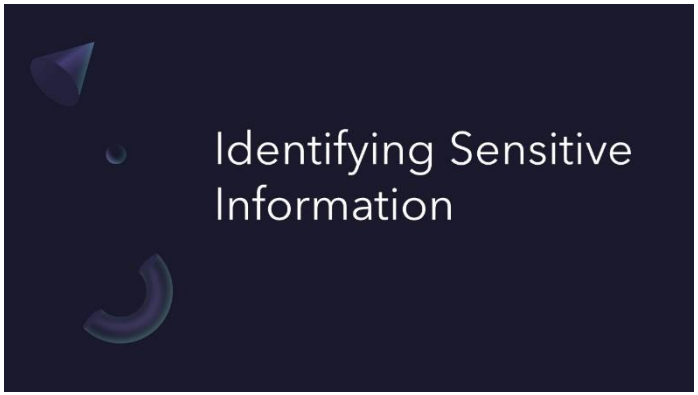
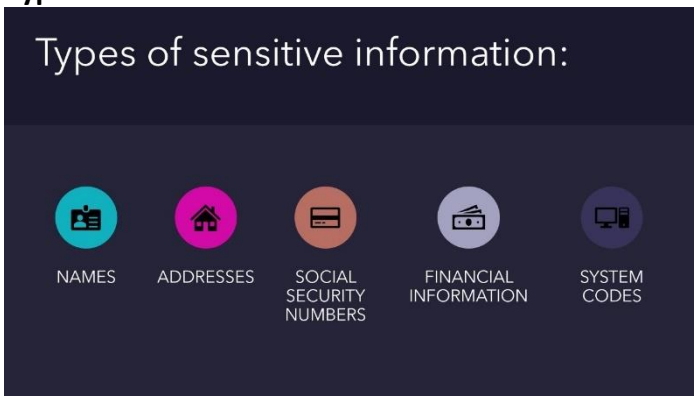
			know the session will begin shortly – Please remind everyone that they should remain muted unless called upon Also, to use the raise hand icon if they have questions
2) Less than 2 minutes	**Introductions** 	Say: Please introduce yourselves one at a time. Say your name and your department.	–
3) 1 minute	**Learning Objectives** 	Do: List objectives.	–

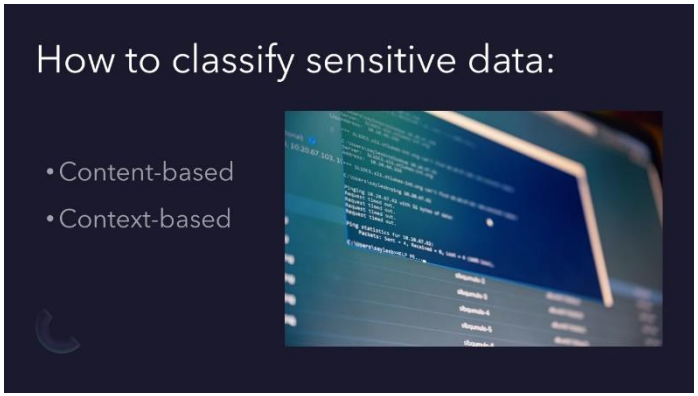
4) Less than 1 minute	**Subtopic title slide: Introduction to Data Protection and Cybersecurity** 	**Say: Introduction to data protection and cybersecurity**	
5) 1 minute	**Real life example** 	**Say: A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.** **Some businesses are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.**	
6) 5 minutes	**AhaSlides Poll**	**Say: Before we start I would like everyone to take a short poll. You will have 5 minutes.** **Do:**	**-Do:** **- Put the link and information to the AhaSlides poll in the group chat.**

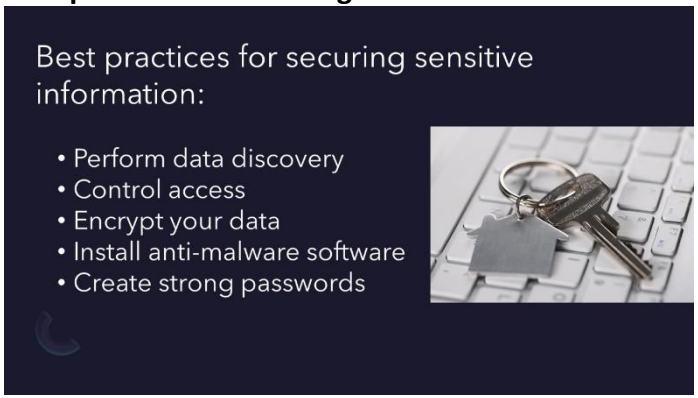
		**– Instruct participants to click the link to the AhaSlides poll in the chat.** **– Review submissions and talk about the results.** **- See page 12 for poll question and possible responses**	**-Collect the results and share the screen with everyone after 5 minutes.**
7) 1 minute	**Data protection definition and importance.** 	**Say: Data protection is the process of safeguarding important information from corruption, compromise or loss.**	
8) 2 minutes	**The importance of data protection**	**Ask: Why is data protection important?** **Do:** **– Instruct participants to type the answer into the chat.** **– Review submissions and provide correct answer if no one provides it.** **Explain: The importance of data protection increases as the amount of**	

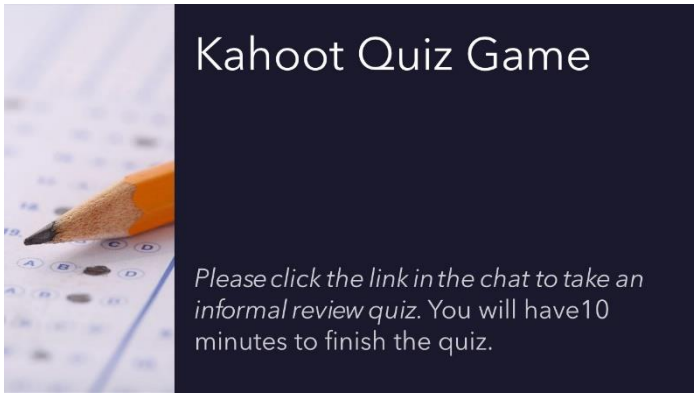
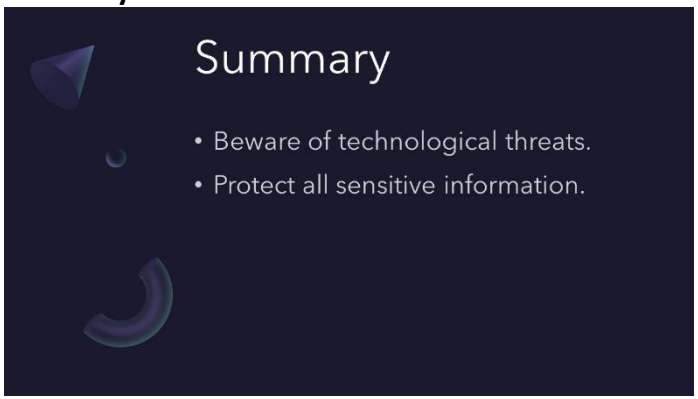
		**data created and stored continues to grow.**	
9) 1 minute	**Cybersecurity definition and importance.** 	**Say: Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.**	
10) 2 minutes	**The importance of cybersecurity** 	**Ask: Why is cybersecurity important?** **Do:** **– Instruct participants to type the answer into the chat.** **– Review submissions and provide correct answer if no one provides it.** **Explain: Cybersecurity is important because there are dangers such as malware that could erase the company's**	

		entire system, an attacker breaking into the system and altering files, an attacker using your computer to attack others, or an attacker stealing secret information.	
11) 2 minutes	**Common threats** 	**Say: Hacking refers to the unauthorized access to computer systems or networks with the intent of stealing data or causing damage. Phishing is a type of social engineering attack in which scammers use fraudulent emails, text messages, or other communication methods to trick users into revealing sensitive information, such as passwords or private keys. Malware is malicious software designed to harm computer systems or networks. Malware can include viruses, worms, Trojans, and other types of malicious software.**	
12) 5 minutes	**Miro sticky notes activity** 	**Say: The next activity uses Miro sticky notes. Miro uses virtual sticky notes to gather ideas from everyone in this training. The question is: What are other examples of threats to technology?** **Do:** **– Instruct participants to click on the link to the Miro sticky notes in the chat.** **– Review submissions and provide correct answers if no one provides it.** **Explain: Other examples include viruses, spyware, and adware.**	**-Do:** **- Put the link and information to the Miro sticky notes in the group chat.** **-Collect the results and share the screen with everyone after 5 minutes.**

13) Less than 1 minute	**Subtopic title: Identifying and Protecting sensitive information** 	**Say: Identifying sensitive information**	
14) 1 minute	**Types of sensitive information** 	**Say: Privacy regulations describe sensitive information as any personal data or information that could potentially cause harm, damage, embarrassment, or discrimination to an individual if it is disclosed, accessed, or used without authorization.** **Sensitive information typically includes personal identifying information such as names, addresses, Social Security numbers, financial information and system codes.**	
15) 1 minute	**How to classify sensitive data**	**Say: You can inspect data based on its content files or databases to determine the information's sensitivity.** **You can also use context such as using metadata about a file as indicators of its particular characteristics. This metadata includes who created the file or database,**	

		**the application, its use, or the location in which it was created/ modified.**	
16) 10 minutes	**Discussion Activity** 	**Say: Now we will break into small groups to discuss this question: Which types of sensitive information are the most vulnerable to threats? Why? You have 10 minutes.** **Do:** **– Instruct participants to accept their request to join their breakout rooms.** **– Review each group's answers.** **Explain: Out of the examples that we discussed, financial and government related information such as social security numbers and financial information is most likely to be stolen.**	**-Do:** **- Create breakout rooms with 3 to 4 people in each room.** **-Close the breakout rooms after 10 minutes.**
17) Less than 1 minute	**Subtopic title: Securing Digital Assets and Infrastructure**	**Say: Securing digital assets and infrastructure**	

			
18) 4 minutes	**Best practices for securing sensitive information** 	**Say: Perform data discovery by looking at how much data is sensitive or critical to the company and what needs to be compliant with security regulations. Control access to information because the more people who have access to sensitive information, the more room there is for internal breaches, data theft and/or loss. Encrypting your data can make it difficult for unauthorized users to access data because it's encoded. Install anti-malware software because if your computer is infected with malware confidential data can be stolen by hackers. Create strong passwords, so they are not easy for other users to guess.**	
19) 10 minutes	**Kahoot Quiz Game**	**Say: Now there will be an informal review quiz hosted on Kahoot. You have 10 minutes.**	**-Do:** **- Put the link and information to the Kahoot quiz in the group chat.**

		**Do:** **– Instruct participants to click the link to the Kahoot quiz in the chat** **- See page 12 for poll questions and correct answers**	**-Collect the results and share them with the facilitator only.**
20) 1 minute	**Summary** 	**Say: To wrap up today's training it's important to protect yourself and the company against technological threats such as malware and phishing. It's also important to protect sensitive information such as social security numbers and financial information. There are several different ways to do this such as controlling access to your information and installing anti-malware on your computer. I hope you take what you learned today to further protect sensitive information.**	
21) 1 minute	**Conclusion**	**Say: Thank you everyone for joining us today. If you have any further questions please let me know.**	

Addendum

- Slide 6 (page 4): AhaSlides Poll
  - Question: Have your online accounts (Facebook, bank accounts, etc.) ever been hacked?
  - Possible Answers: Yes or No (There is no correct answer.)
- Slide 19 (page 10): Kahoot Quiz Game
  - Question 1: Which one of these threats uses social engineering to attack and steal data?
    - Correct Answer: Phishing
  - Question 2: Which one of these is not considered sensitive information?
    - Correct Answer: Relationship status
  - Question 3: What is the difference between content-based and context-based sensitive data?
    - Correct Answer: Context-based classification uses metadata about a file as indicators of its particular characteristics.
  - Question 4: Which practices are best for securing sensitive information?
    - Correct Answer: Control access, encrypt your data, and perform data discovery
  - Question 5: What are examples of malware?
    - Correct Answer: Malware can include viruses, worms, and Trojans.