Tutorial 4 – Colonial Pipeline exercise

Due date: 25 August 11.59pm

Weighting: 3%

1. https://www.immersivelabs.com/resources/webinars/take-a-walk-on-the-darkside-a-pipeline-cyber-crisis-simulation/.

For each of the 8 injects, state which answer your group originally chose, and briefly explain the reason why. Then also state the answer chosen on the video.

GR: Answered in group in tutorial. IN: Answered by myself outside tutorial

Inject	Your group's answer	Why did you choose this option?	Answer chosen on video
1 - GR	**Option 3**	If the attack goes into the operations network, then technicians could be locked out of key system controls, this is in line with what the company did.	Option 3
2 - GR	Option 2	There is no guarantee that files will be decrypted even if you pay. Additionally, it is not ethical to pay money to a criminal organisation. Additionally have one-day old backups, so can rebuild from there.	Option 2
3 - GR	Option 4	Process of elimination: Thought was that this was a publicly discussed issue. Option 1 seemed a bit vague, in option 2, an apology seems like the company admitting fault where they shouldn't (out of their control). Option 3 would be a lie as we don't know when the company would be running, we can't say its soon.	Option 1
4 - GR	Option 4	Option 1 is the morally right thing to do to protect employees and put staff first. Option 2 is more focused on protecting the company image. Option 4 would be preferred by an economic and business standpoint so companies can follow compliance and make profit.	Option 4
5 - IN	Option 2	At this point, option 2 is the correct option, due to reputation management being crucial at this stage in the crisis. External help from the government has led to media attention. Communication of the crisis at hand to the press is the correct option, as this could damage the company's reputation if left too long, and can also control the narrative to avoid damage to company image if false information is spread.	Option 2
6 - IN	Option 4	Option 2 is not valid due to the company being a distributor across all areas so publicly this wouldn't be a good look. Option 3 would not work due to the demand that is met by all customers and supply shouldn't be conformed to one area. Option 1 and 4 are valid options however option 4 is a better strategic approach in the long run as it addresses larger paying and contracted customers as well as supplying to the public in the long run. Option 1 is valid purely however based on a business standpoint delivering to higher paying customers should be present.	Option 3
7 - IN	Option 3	Option 1 is not valid due to if it was from initial compromise this would've happened already. Option 4 is not valid as this would have been disclosed to SOC that this is happening. New attacks do happen although it is unlikely. Option 3 is valid due to the company trying to rebuild and taking systems offline. This may have affected the company website when taking some systems offline resulting in the HTTP error message.	Option 3
8 - IN	Option 1	Due to ransomware attacks being such a prevalent issue for US business and infrastructural sectors from 2020 onwards, complete transparency is a better option. By enabling other organizations and the public in general, knowledge of the lessons learnt and the actions taken, will address the importance of cybersecurity in these sectors, and how to handle ransomware attacks.	Option 2