Question 1: Examine the concept of cybersecurity resilience testing and exercises. Why is it important for organizations to regularly test their cybersecurity resilience plans through tabletop exercises, simulations, and penetration testing?

Answer: Its important because you need to see the varieties of degrees that your systems can be in. Tabletop brings excellent brainstorming without the variables that performing a simulation can bring. Whereas penetration testing brings everything together so that you can test the walkthrough and tabletop in the simulation to see what would happen. Then after you may be able to formulate a response.

Question 2: Examine the role of cybersecurity awareness training and employee education in enhancing cybersecurity resilience. Why is it crucial for organizations to invest in educating their workforce about cybersecurity best practices?

Answer: It is crucial for orgs to invest in educating their workforce on cyber security because people are the most responsible for breaches. This could be in the form of phishing attacks via email, or insider threats. If organizations do no adhere or comply with the laws and regulations, that could mean fines in large amounts for company. If an employee downloads malicious software, it could mean having data lost or exfiltrated. There are too many things that could happen. That's why its important to train your personnel.