Storyboard – FIRST 2025 Example

Exercise Date	6/24/2025
Executive Sponsor	Dave Murray, Vice President of Information Technology
Development Team	Julie O'Conner, Information Security Officer (Facilitator) Michelle Kane, Vice President of Communications
Location	Executive Conference Room, Old Prairie HQ, St. Joseph, Missouri
Goals	Continued adherence to Old Prairie's Cybersecurity Incident Response Plan by performing a biannual tabletop exercise.
Objectives	1. Perform a tabletop exercise focused on the compromise of the organization's social media accounts. 2. Examine the organization's security posture and response to a security incident pertaining to social media accounts. 3. Educate participating business staff on the importance of not reusing passwords.
Scenario	The social media accounts for the organization, which include X, Facebook, and YouTube have all been compromised. The organization was notified at 9:15 AM this morning of malicious posts on all accounts. Logins to all accounts appear to be invalid.
Inject #1 Tuesday, 9:15am	• A call is received to the corporate number asking if the posts on X and Facebook are legitimate. • The call taker views the messages on the public X and Facebook pages. • Both messages are the same and indicate that the Company has been hacked and data exfiltrated.
Inject #1 Key Issues	• Is this an event or incident? • How would reception handle this call? • Are front office staff trained on how to escalate security events and who to escalate them to?
Inject #2 Tuesday, 10:45am	• Investigation into both the corporate X and Facebook accounts determines that existing logins are not working. • Corporate communications is locked out of all social media accounts. • The organization's website is now displaying unauthorized content as well, suggesting a broader incident.
Inject #2 Key Issues	• Does this information change the incident severity? If so, how would it now be classified? • Are the accounts (logins and passwords) the same for both X and Facebook? • Is MFA enabled on the social media accounts?

Inject #3 **Wednesday,** **1:45pm**	• Local news outlets have picked up the story, citing malicious posts and speculating on a data breach. • Stakeholders, including community members, are reaching out for clarification. • Investigation into corporate communication employees' email shows a phishing email that went undetected by the email security tool, resulting in compromised credentials.
Inject #3 **Key Issues**	• Who is responsible for communicating to the public and to the media? • How long would it take to prepare communications and who is responsible for approving external communications? • How do we determine who fell for the phishing email?