Pre-Tabletop Interview

1. Who will be participating in the TableTop exercise? Legal? HR? Data Owners?
2. Current Size of your IR Team? Dedicated or Surge?
3. In-house Experience?
4. What types of incidents have you all been dealing with over the last few months?
5. How long has the team been in place? Policy, Procedures?
6. Does your policy provide authorization to pull systems offline?
7. (Can you email me your policy, procedures, charter?)
8. Do you have centralized logging/ SIEM in place? how long? how effective?
9. Do you have Network IDS capabilities? Packet Capture?
10. Any Host IDS in place?
11. Any endpoint forensic agent in place? what tools are currently being used for forensics investigations?
12. Response tools? Procedures?
13. Any recent improvements/changes to procedure/tool implementation?
14. Physical locations? Out of what office does everyone work?
15. Sensitive data to protect?
16. Externally facing web servers? Third party service providers? Cloud service providers?
17. Whitelisting, DLP, Detailed Process Logging in place?
18. Wireless components to your network?
19. Do users VPN?
20. Prevalence and Policy concerning Mobile Devices, BYOD?
21. Dual Factor Authentication?