Cyber Questions

Have you noticed any changes to any of your systems since you pulled in today?

How/when do you connect to your corporate network?

What has your company told you about the incident? Any email comms? When was the last time they talked to you? What was it about?

What is your back up communications plan in the event of a Cyber-attack onboard or at a port facility (Incident response)?

How does your company communicate with your vessel? Email, satellite, etc.?

How is your cyber hygiene?

Have you noticed any issues with your computers or systems?

Have you experienced any phishing attempts?

Have you noticed anything out of the ordinary while logged on?

Do you use social media?

Has anyone suspicious reached out to you while online?

How would you rate your computer/software protection?

How do you protect against computer viruses?

How often do you update your systems? Patch?

What systems have a ship to shore interface for monitoring (Engineering)?

How do you update your charts?

Have you noticed any issues with your emergency systems (security and alert)?

Does your computer network interface with K-Line ashore operating systems?

Is there a recreational computer for the crew?

Are your computers on separate networks or are they connected? Separate from safety or ISM reporting systems?

How well do you know your IT infrastructure?

Have you received any suspicious emails or phone calls?

Have you experienced any degrading equipment onboard?

Any ICS/SCADA system diagrams I can see?

Have you ever transited through areas where your electronic equipment experience interference? If so, where?

What specific onboard systems communicate through shore ties? Any issues? If so, what port and when specifically?

Have you noticed any issues with your operational systems (GPS)? Jamming, spoofing, or other anomalies?

How do you connect to the internet?

Do you have Wi-Fi onboard?

Any AIS issues?