Scenario 1 - Ransomware:

Purpose:

- **Technical:**
    - Verify that the procedures for restore are in place
        - Employees know how to switch to backup systems
    - Raise awareness on how to identify malicious content in relevant logs
    - Verify that employees know how to isolate machines
- **Procedure:**
    - Cram on the responsibility areas around notification processes (police, media, the press and others)
    - Cram on the responsibility areas for handling the situation of a ransomware attack

Backdrop:
An employee receives an email, from what seems like one of the coworkers, with an attachment containing relevant information. The employee has high privilege access to important parts of the system. The attachment is opened and looks legit.

Description of scenario:
Part 1: A control room operator is working a night shift in the offshore control room. Suddenly, he discovers a message in one of the text-fields in the alarm lists. The message demands a ransom of 20 million Norwegian kroners. The ransom should be paid to a given Bitcoin address. When the employees in the control room take a closer look at their systems, they observe that everything is encrypted.

Part 2: After three days, the attackers reach out with a new message. This message tells statest they are in control of the main generator of the platform. If the ransom is not paid, they will stop this generator and hence stop the production until they receive the payment.

Justification of the scenario:
Hydro experienced a ransomware attack in 2019 which also makes this type of attack realistic for the petroleum industry. In addition, other huge ransomware attacks have been targeting different sectors over the last years. RYUK (2018), WannaCry (2017) and Petya (2016) are three examples of such ransomware attacks. The economical benefits of performing a ransomware attack can be large if the ransom is paid, and this makes it attractive for potential attackers. If the operators choose not to pay the ransom, the economical consequences for the company might still be large, as the attack most likely causes a stop in production.

A stop in a main generator may also stop the production on other platforms nearby. This can lead to costs up to 100 millions Norwegian kroners a day which is critical for the platforms. This makes such a scenario relevant and it needs to be included in the exercise program.

Exercise plan:

Time duration	Total of 3 hours including introduction and first evaluation.
Prerequisites	- Training of employees on system restore.

	- Training of employees on checking logs.
Participants	- Control room operators - Platform management - The emergency response team (both offshore and onshore) - IT experts - Government authorities - Liaisons from PSA - Employees from SOC
Example questions	*Part 1:* *Technical:* - How can we restore our systems most effectively? - Should components be isolated? - Which components? And why? *Procedure:* - Should emergency preparedness be set? - Who should be involved in this process? - Should external parties be involved? - Should the media be notified? - How can we restore our systems most effectively? *Part 2:* *Technical:* - How to confirm if the attackers actually have control over the main generator? - If they have control over the main generator, how can we manage the situation and take back the control? *Procedure:* - If they have control over the main generator, how can we manage the situation and take back the control? - As the ransom is 20 million Norwegian kroners, and is a relatively small amount compared to the potential loss of this attack, it is expedient to discuss the options around paying the ransom - Consequences where ransom is paid, or not. - Who should be contacted? - Should additional parties be involved and notified? - Who and why? - How to communicate with, and inform, nearby platforms? *Discussion and reflection:* - How can you distinguish the phishing email from a legit email? - What are the routines when suspecting a phishing email?

	- What are the routines if you open content and then get the suspicion? - What kind of security barriers may have been compromised? - What are the benefits of being open about the incident vs. not being open? - Are there any mechanisms for automatically detecting phishing emails? - What is the reason this email got through the filter?
Variations	- If ransom is paid: the threat of shutting down the main generator continues and the attackers request a higher ransom. - The ransomware may be used as a distraction to cover up their initial attack. For example to delete tracks of other attacks. - The ransomware can find its way into the system via a USB stick, a service laptop, being downloaded from the Internet on an IACS-connected engineering workstation or by a zero day attack. - An attacker can gain access to the datacenter onshore and install the ransomware on the backup-servers that they have there.
Suggestions to playbook	