**Cybersecurity Incident Handling**

**Organisation: Oil and Gas Free Zones Authority**

**Background**

At about 2.00 PM on October 20, 2021, as the Senior IT Engineer (Cybersecurity/Cloud) in the Oil and Gas Free Zones Authority, during a routine inspection of security reports generated by the Advanced Threat Protection (ATP) systems, one of the security controls implemented as part of the organisation information security management systems (ISMS), spotted a report of suspicious exfiltration of a sensitive financial document. The ATP flagged a particular email with an attachment as being suspicious. The email which was sent from the Authority’s Financial Controller to an external email contained several company’s sensitive documents as attachments.  IT security team quickly reached out to the Financial Controller to inquire if he had sent such a mail. It was discovered he never sent nor authorised such communications. It was therefore established that there was a security breach within the company’s email system.

Based on the background above, a security breach has occurred within the company's email system. As part of the cybersecurity team, we would follow the guidelines provided by the National Institute of Standards and Technology (NIST) to handle this incident.

The NIST Computer Security Incident Handling Guide provides a comprehensive framework for handling computer security incidents. The guide is organised into three phases: preparation, detection and analysis, and containment, eradication, and recovery.

From the background, the suspicious email was detected by the Advanced Threat Protection (ATP) system during a routine inspection of security reports. The email contained several sensitive documents and was sent from the Authority’s Financial Controller to an external email address. Upon investigation, it was discovered that the Financial Controller never sent nor authorized such communications. This indicates that a security breach has occurred within the company's email system.

To manage this incident, The IT security team would follow the NIST incident handling process put in place:

1. Preparation: Establish an incident response team and develop an incident response plan. I led the security team. The incident response plan should outline the procedures to be followed in the event of a security incident.

2. Detection and Analysis: We collected and analysed information related to the incident. This includes identifying the source of the incident, the extent of the damage, and the potential impact on the organisation. In this scenario, the ATP system has already detected the suspicious email. The incident response team analysed the email and its attachments to determine the nature of the breach.

3. Containment, Eradication, and Recovery: Contain the incident to prevent further damage, eradicate the cause of the incident, and recover from the incident. In this scenario, the incident response team isolated the affected systems and devices to prevent further exfiltration of sensitive data. The team also investigated the source of the breach and steps were taken to eradicate it.

By NIST Cybersecurity Framework guidelines, we implemented a set of security controls. These include installing Endpoint Security software to all endpoint devices within the company’s network, a Firewall to prevent suspicious network traffic, web content filtering software installed and configured to regulate access to certain unapproved network resources, Microsoft Office 365 Defender installed and configured to protect the company’s cloud-based emails and all emails account had multifactor authentication activated. Using Microsoft Azure Identity Management, we were able to implement Access control mechanisms on all IT resources within the company and limit access to only authorised users.

Finally, the team developed a plan to recover from the incident and restore normal operations.