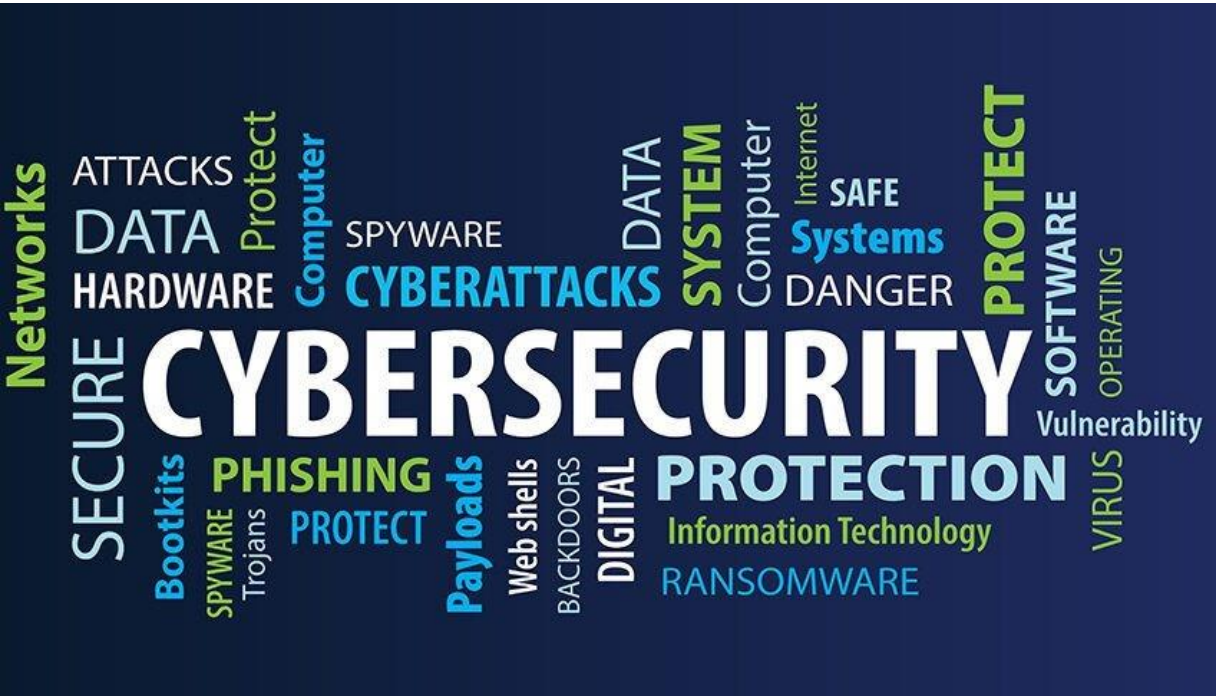
Cyber security Management in Oil and Gas

Manage and Awareness

Dashti Khudhur
Manager, Risk Management

Objectives



-What's Cybersecurity
-Why in Oil & Gas
-Cyber security Types
- Risks to present and future engergy

What's Cyber Security

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks.It aims to reduce the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks and technologies.

Why in Oil and Gas

Domain area:

1-Risk Management

2-Asset, Change and Configuration Management

3-Identify and Access Management

4- Threat and Vulnerability

5- Situational Awareness

6- Information Sharing and Communication

7- Even and Incident response,

8-Supply Changing and External Dependencies Management

9-Workforce Management

10-CyberSecurity Program Management

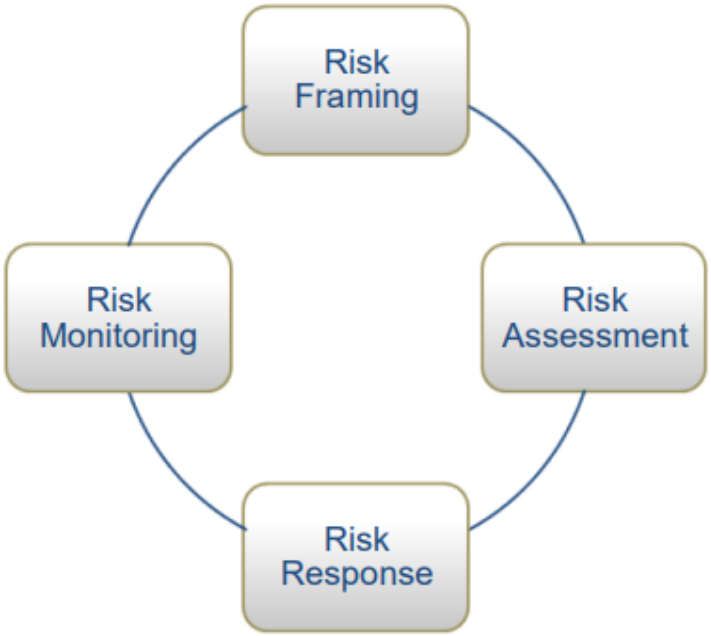
Why in Oil and Gas

1-Risk Management

Establish, operate, and maintain an enterprise cyber security risk management program to identify, analyze, and mitigate cyber security risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Why in Oil and Gas

1-Risk Management cont..



Why in Oil and Gas

2-Asset, Change and Configuration Management

Manage the organization’s operations and IT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

Why in Oil and Gas

3-Identify and Access Management

Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

Why in Oil and Gas

4-Threat and Vulnerability

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization’s infrastructure (e.g., critical, IT, operational) and organizational objectives.

Why in Oil and Gas

5- Situational Awareness

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).

Why in Oil and Gas

6- Information Sharing and Communication

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

Why in Oil and Gas

7-Supply Changing and External Dependencies Management

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

Why in Oil and Gas

8-Workforce Management

Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives

Why in Oil and Gas

9-CyberSecurity Program Management

Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure

Cybersecurity Types

- Critical infrastructure security.
- Application security.
- Network security.
- Cloud security.
- Internet of Things (IoT) security.

Any Question