WHITE PAPER

INDUSTRIAL CYBERSECURITY RISKS - OIL AND GAS OPERATIONS

"Challenges and roadmap for a secure ecosystem"

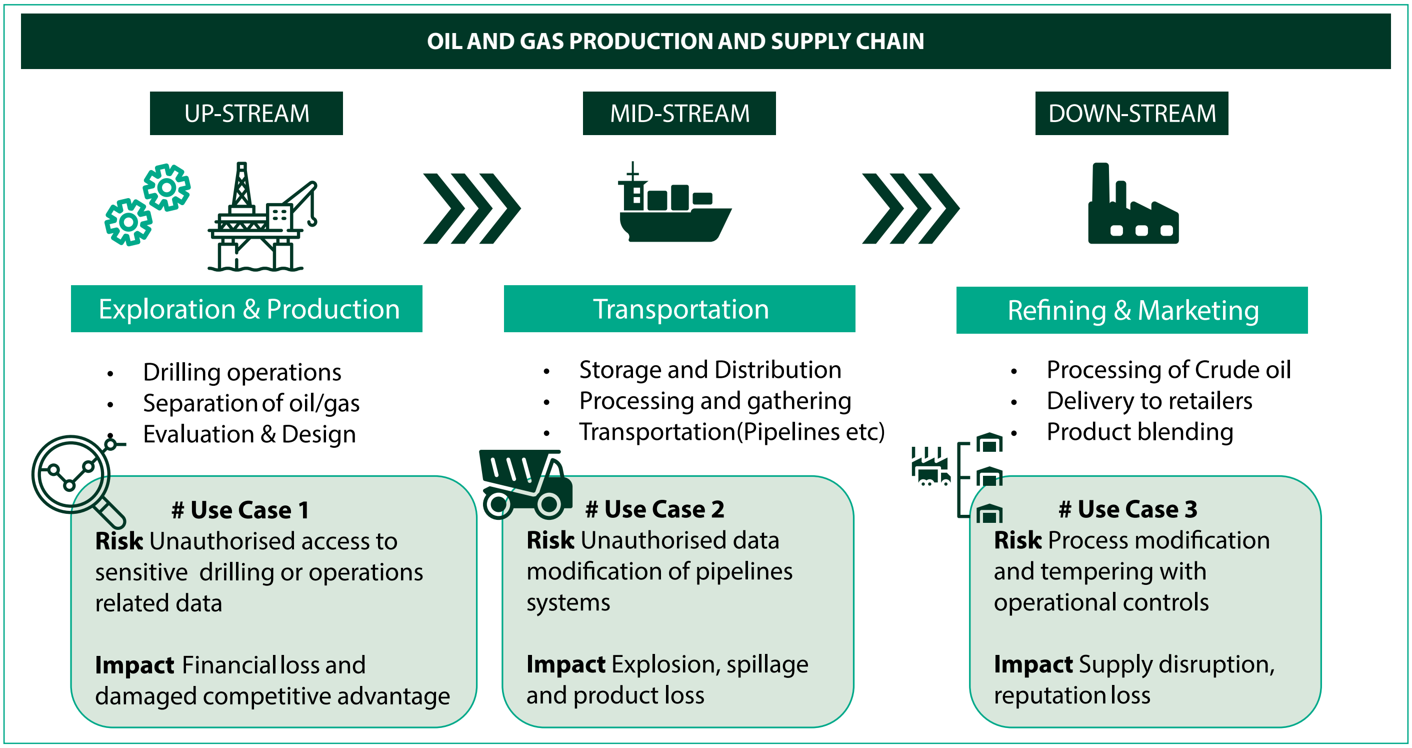
Abstract

From military aggression to cyber threats, the oil & gas sector has always been a high-profile target for adversaries. Originally, the probability of a major failure due to a cyberattack was highly minimal as organizations usually adopted a production-oriented approach wherein operational systems were isolated and never integrated into enterprise systems. In the current scenario though, the emergence of the Internet of Things (IoT) has nullified the most basic assumptions about operational technology. All sorts of industrial facilities, like oil fields, pipelines and refineries, are vulnerable to cyber-attacks. The major security-related concerns in the oil and gas industry range from lack of asset visibility in a distributed environment; to setting operational, technological, and environmental specific policies and procedures, defining roles, responsibilities and accountability and implementing technical controls for assessing real-time security incidents for a dynamic production environment. In this paper, inherent limitations & security challenges the oil & gas organizations face have been discussed in detail along with the approaches that define the way forward for addressing these concerns. Key factors that need to be considered for defining and designing right security roadmaps for sustainable cybersecurity programs have been discussed in detail.

Infosys®
Navigate your next

Overview – The oil & gas industry

The oil & gas industry happens to be a complex industry having multiple, cumbersome and complicated processes involved. At a high level, all the processes in this industry can be sub-divided into three i.e., Upstream, Midstream, and Downstream. The processes in the oil & gas sector include exploration, gathering, production, processing, refining, storage, and transportation of petroleum liquids and natural gas. ICS (Industrial Control System) and OT (Operational Technology) are used to manage the industrial operations and enable monitoring & controlling of these operations across the value chain.



OIL AND GAS PRODUCTION AND SUPPLY CHAIN

UP-STREAM

Exploration & Production

- Drilling operations
- Separation of oil/gas
- Evaluation & Design

# Use Case 1

Risk Unauthorised access to sensitive drilling or operations related data

Impact Financial loss and damaged competitive advantage

MID-STREAM

Transportation

- Storage and Distribution
- Processing and gathering
- Transportation(Pipelines etc)

# Use Case 2

Risk Unauthorised data modification of pipelines systems

Impact Explosion, spillage and product loss

DOWN-STREAM

Refining & Marketing

- Processing of Crude oil
- Delivery to retailers
- Product blending

# Use Case 3

Risk Process modification and tempering with operational controls

Impact Supply disruption, reputation loss

Figure 1: Oil and Gas production and supply chain risk

Automation and digitization of the oil and gas lifecycle process have led to growth driven performance such as increased production rates, downtime and cost reduction. However, these processes are also posing the following obstacles in this sector:

- The insecure communication between OT and corporate network that supports critical decision making can be misused to gain access and execute production loss
- Unsecured remote access can allow a malicious user to take control of the process systems and adversely affect the production
- Poor security governance allowing vendors to introduce new security threats via unmanaged devices
- Inadequate security testing of the operational assets allow systems in production to be deployed unpatched; this creates security loophole for hackers to exploit
- Isolated assets are deployed on a network without adequate communication. Improper visibility and control on the assets can expose an operational network for exploitation

The transformation of many oil & gas companies from the state of isolated operational systems & environments to fully integrated businesses has resulted in many challenges. For instance, the current IT security measures and existing products are not apt to prevent cyber-attacks in an operational production environment. This renders the domain vulnerable to various cyber threats and high impact consequences like:

- Plant shutdown or an explosion
- Leakage of commercially sensitive information
- Modification of pipeline parameters
- Utilities interruptions & supply disruptions
- Tempering with operation controls
- Production circle shutdown
- Health and safety hazards

Operational assets and systems are usually not designed with security as the backdrop and therefore are vulnerable to manipulation and disruptions

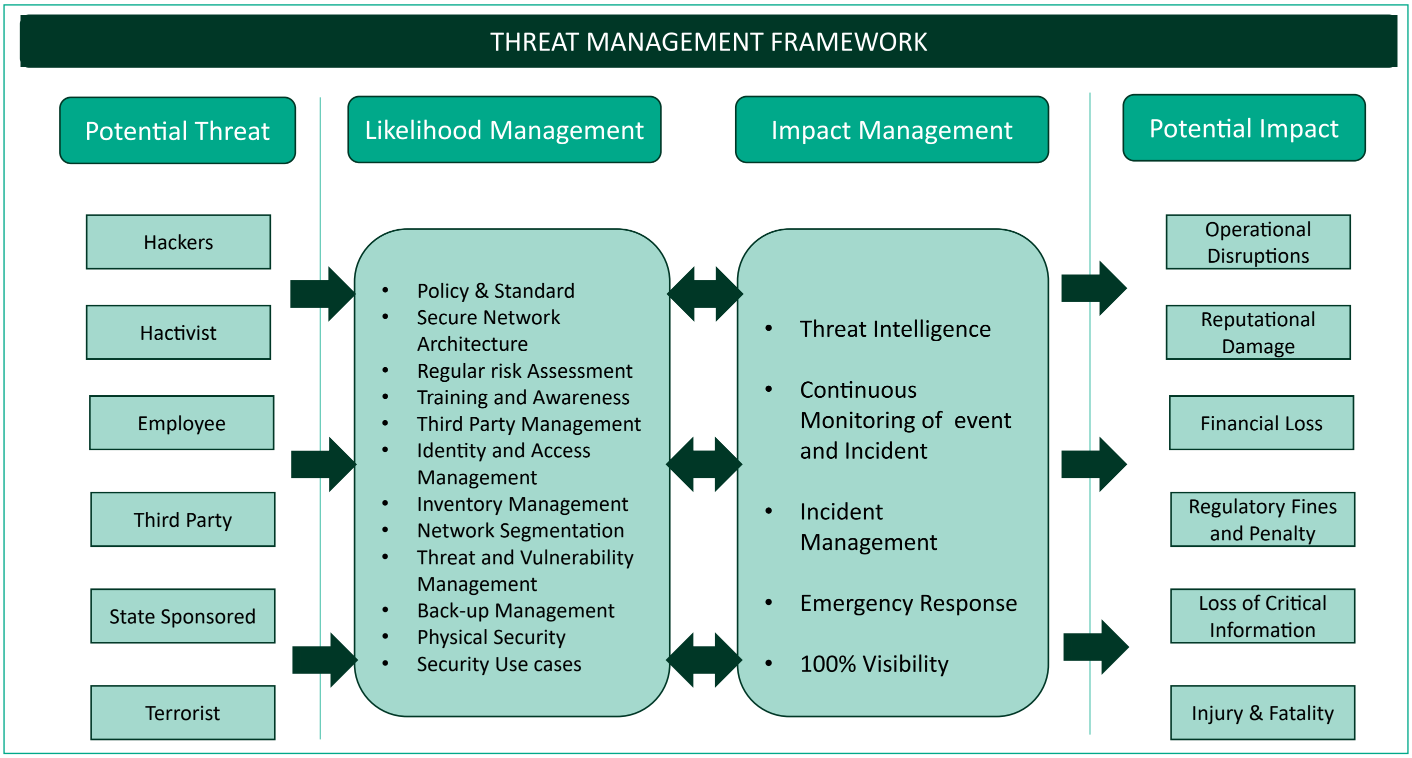


Figure 2: Threat Management framework for oil and gas industry

A comprehensive approach that can bring IT and OT security together is a must for addressing the new age security challenges.

Identifying potential threats and their consequences should be considered while creating an end-to-end management framework that can assess and reduce the likelihood of an impact, thus significantly minimizing the overall risk posture of an organisation.

It's critical to build a sustainable, robust and integrated cybersecurity framework to avoid serious cyber threats and achieve a risk free, incident free organization.

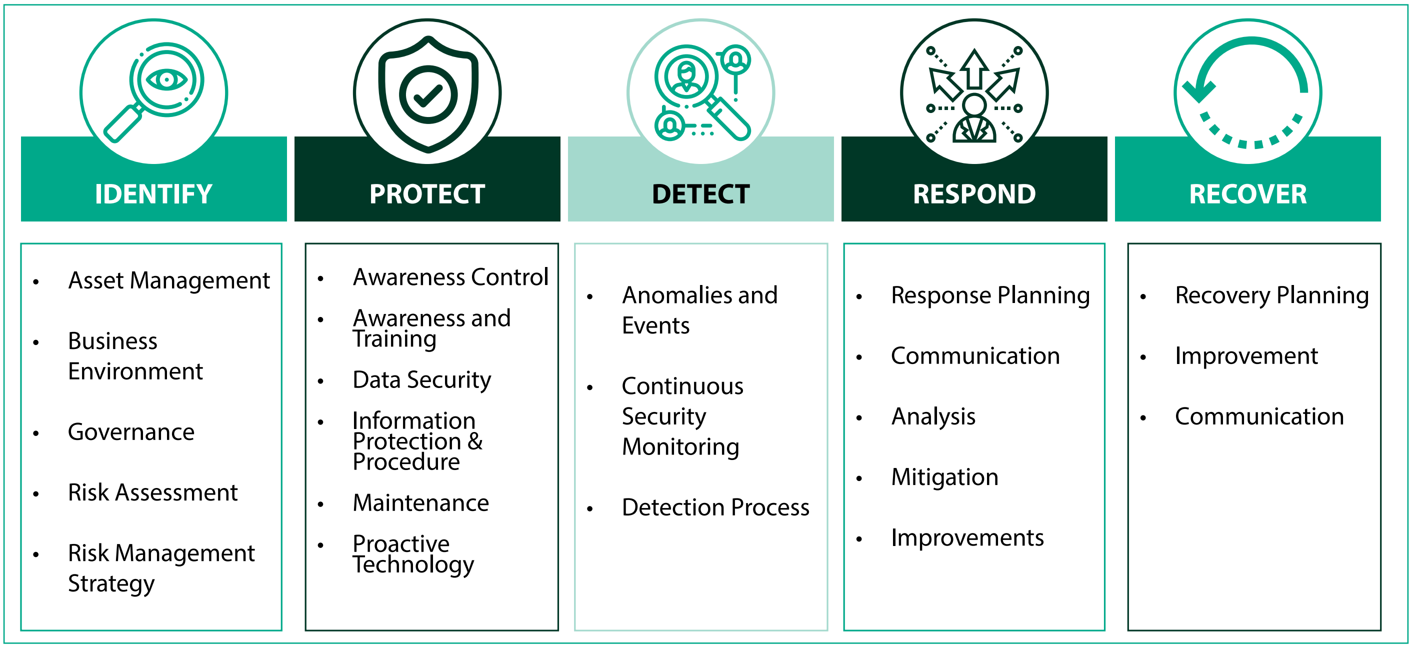
Building blocks for addressing OT security

Traditionally, safety had been a top priority when it came to designing, defining and deploying processes and systems in an operational environment. Although even today, it's a major driving force, the indulgence of digital connectivity in the cyber domain has brought about an enhanced threat landscape for the sector.

As the industry currently faces these new challenges, it has to revamp its cybersecurity approach to be more standardized and integrated with the corporate and operational environment.

Therefore, organizations need to adopt new and advanced technologies involving in depth defense strategies. These should be a combination of practices, processes and technologies designed to defend process control networks, systems, computers, programs and data from attacks, damage, disruption, unauthorized access or misuse.

Defining and implementing a program to achieve security maturity at each stage needs to be aligned with goals of improving the cybersecurity posture and creating an operational environment that can identify, protect, detect, respond and recover.



IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Awareness Control
- Awareness and Training
- Data Security
- Information Protection & Procedure
- Maintenance
- Proactive Technology

DETECT

- Anomalies and Events
- Continuous Security Monitoring
- Detection Process

RESPOND

- Response Planning
- Communication
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvement
- Communication

Figure 3: Reference - Cyber Security Framework NIST

Identify: Understanding the organizational goal and business requirements. Gathering the current landscape information to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the identify function are vital for planning a secured environment. They help an organization to identify its current security posture and steps needed to improve as per the security requirements. They provide visibility of the current threat landscape, next steps & actions needed to improve the security posture.

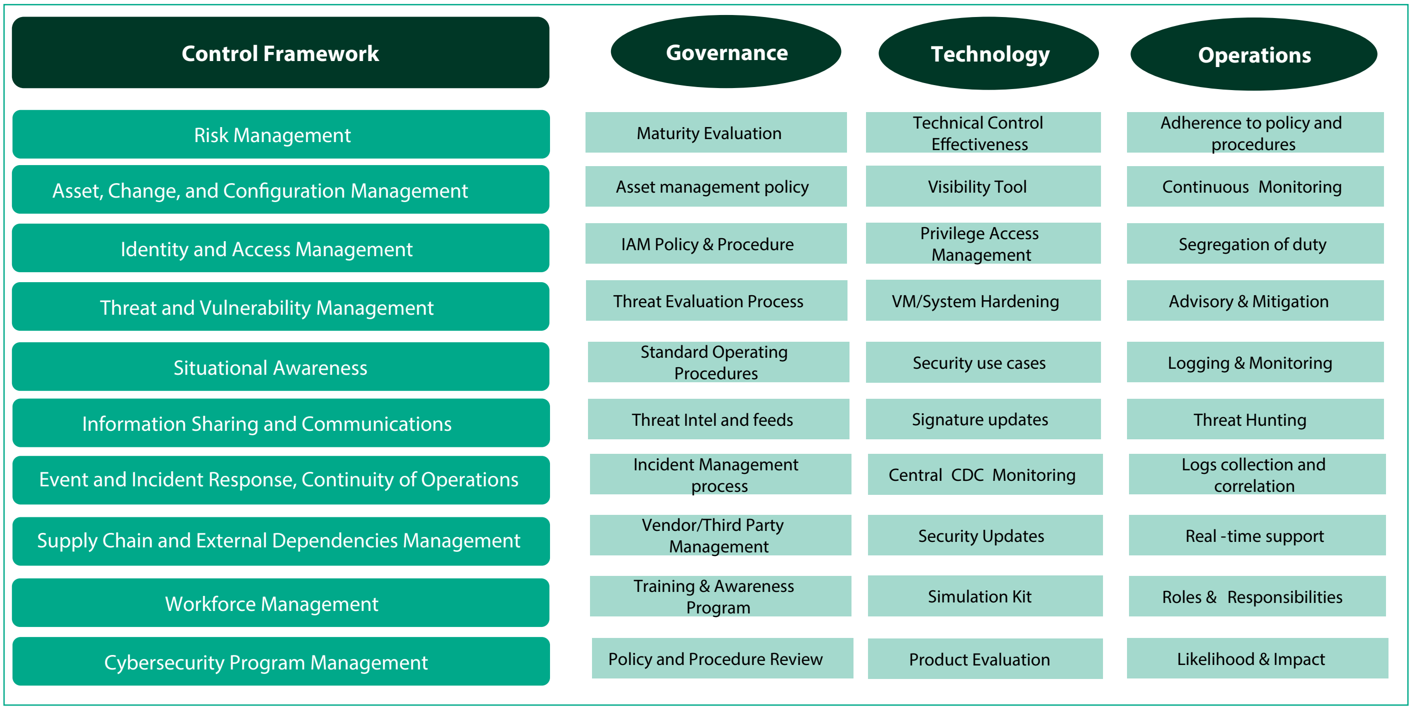
Protect: Developing and implementing security controls to ensure continuity and availability of critical infrastructure services. Protect activities help an organization to deter cyber intrusion and malicious activities. Based on the initial understanding of the requirements, security controls are identified to protect the systems. Controls have to be derived from people, processes, technology or combined.

Detect: There are chances that intrusions still happen even after implementing multiple controls and technology solutions. A system with no openings to intrusions is almost impossible to achieve. Organizations should have a system that can detect and deter any intrusions. Early detection of intrusion helps to reduce the spread of the attack and thereby the impact to the organization.

Respond: This is a key step in which processes and activities are clearly identified, planned and communicated within the team and organization. These processes and procedures are created and implemented to respond to all cyber incidents. This enables an organization to restrict the impact of a cyber-security incident to a minimum level.

Recover: This step involves creating and implementing processes and procedures for recovering from the cyber incident. This enables organizations to recover fast from the impact and come to normalcy in minimum time. Creating and maintaining business continuity procedures is a must for any organisation.

Stated below is the Infosys cyber control framework for addressing the above security concerns and implementing the controls in order to build cybersecurity capabilities with regards to all three aspects -governance, technology and operations. Infosys helps in defining, implementing and integrating required security measures in each area based on the current maturity level and recommends a roadmap to the organisation.



Control Framework	Governance	Technology	Operations
Risk Management	Maturity Evaluation	Technical Control Effectiveness	Adherence to policy and procedures
Asset, Change, and Configuration Management	Asset management policy	Visibility Tool	Continuous Monitoring
Identity and Access Management	IAM Policy & Procedure	Privilege Access Management	Segregation of duty
Threat and Vulnerability Management	Threat Evaluation Process	VM/System Hardening	Advisory & Mitigation
Situational Awareness	Standard Operating Procedures	Security use cases	Logging & Monitoring
Information Sharing and Communications	Threat Intel and feeds	Signature updates	Threat Hunting
Event and Incident Response, Continuity of Operations	Incident Management process	Central CDC Monitoring	Logs collection and correlation
Supply Chain and External Dependencies Management	Vendor/Third Party Management	Security Updates	Real -time support
Workforce Management	Training & Awareness Program	Simulation Kit	Roles & Responsibilities
Cybersecurity Program Management	Policy and Procedure Review	Product Evaluation	Likelihood & Impact

Figure 4: Infosys Cybersecurity control framework for oil and gas industry

Governance: This is a key area in which processes and activities are clearly identified, planned and communicated within the team and organization. Processes and procedures are created and implemented for the effective handling of security-related issues across the organisation. Governance is to secure the environment and help organizations to assess their current security state and the steps needed to improve it as per the requirements. It provides an overview of the current threat landscape, corrective steps & actions needed to improve the security posture.

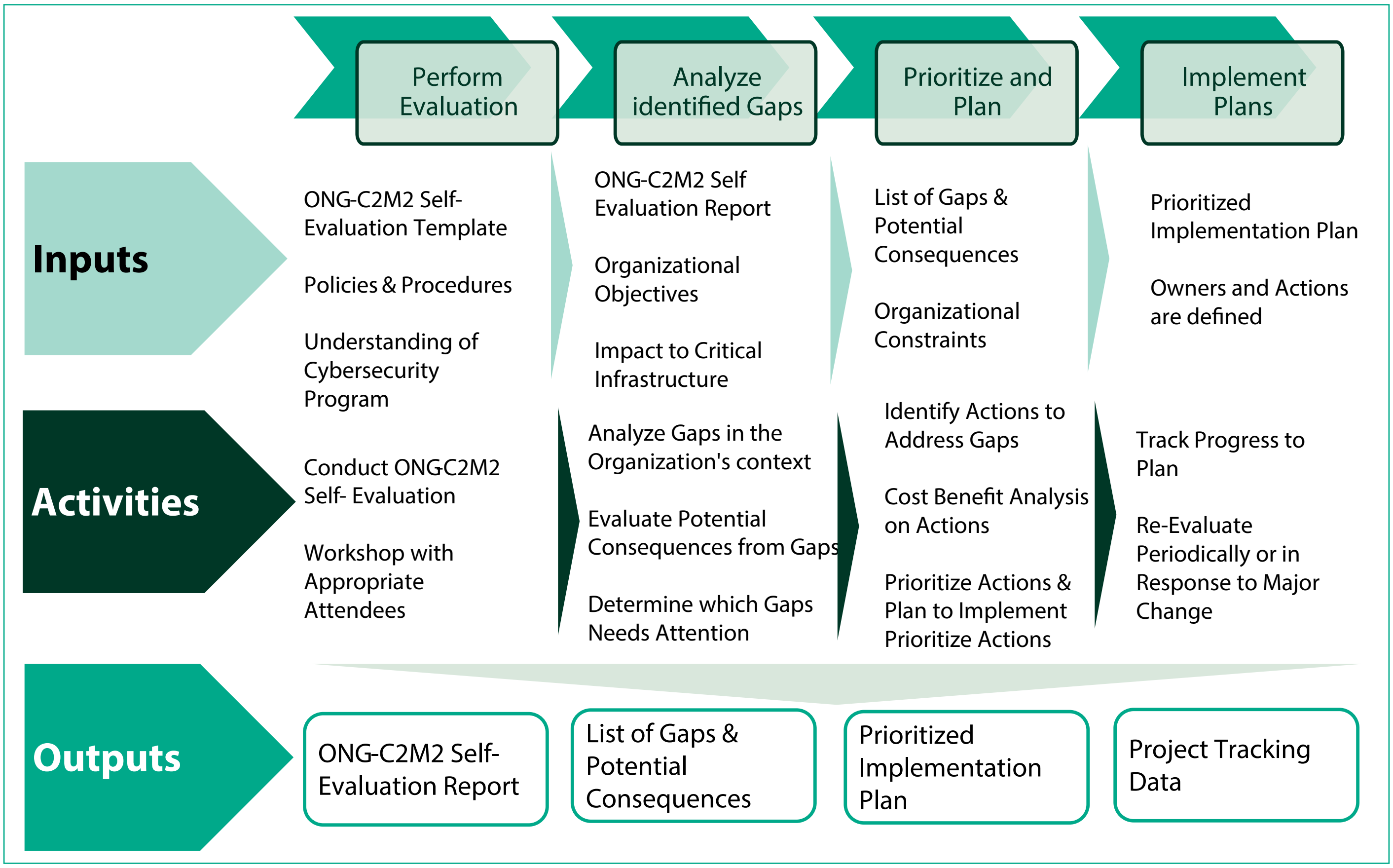
Technology: Technology helps organizations to deter cyber intrusion and malicious activities more effectively and in real-time. Based on the initial understanding of the requirements, technology-based security controls are identified to protect the systems. However, there are chances that intrusions still happen even though multiple controls and technology solutions have been implemented. Technology based controls help in effectively dealing with the spread of sophisticated attacks and impacts on an organization.

Operations: The most important function of operations is to have the right processes and procedures for responding against cyber incidents. This enables organization to restrict the impact from a cyber-security incident to a minimum level. Organisations must have continuous monitoring capabilities to ensure real-time detections. They can then trigger immediate application of correction measures in case of a breach. Centralized systems must be in place to run integrated security operations for both corporate and operational environments with clearly defined roles and responsibilities for each and every stakeholder involved. Apart from this, creating and maintaining business continuity and timely recovery procedures is again a must for the organisations and undoubtedly for the oil & gas production value chain.

Assessing and improving security posture using the security maturity model for the oil & gas industry

The first step of the OT security improvement program is to conduct risk and maturity assessment to identify the risks & its impact on the organization and understand the maturity of its security controls in the ICS environment. With the continuous changing face of the threat landscape, organizations need to identify opportunities to strengthen and determine their current security posture and measure target desired state in operational environments continuously.

Cybersecurity maturity model for the oil & gas (ONG-C2M2) subsector helps to evaluate, prioritize and improve organizational cybersecurity capabilities consistently, and communicate critical cybersecurity investment requirements to the leadership. The ONG-C2M2 model enables organizations to effectively evaluate and benchmark security requirements and capabilities.

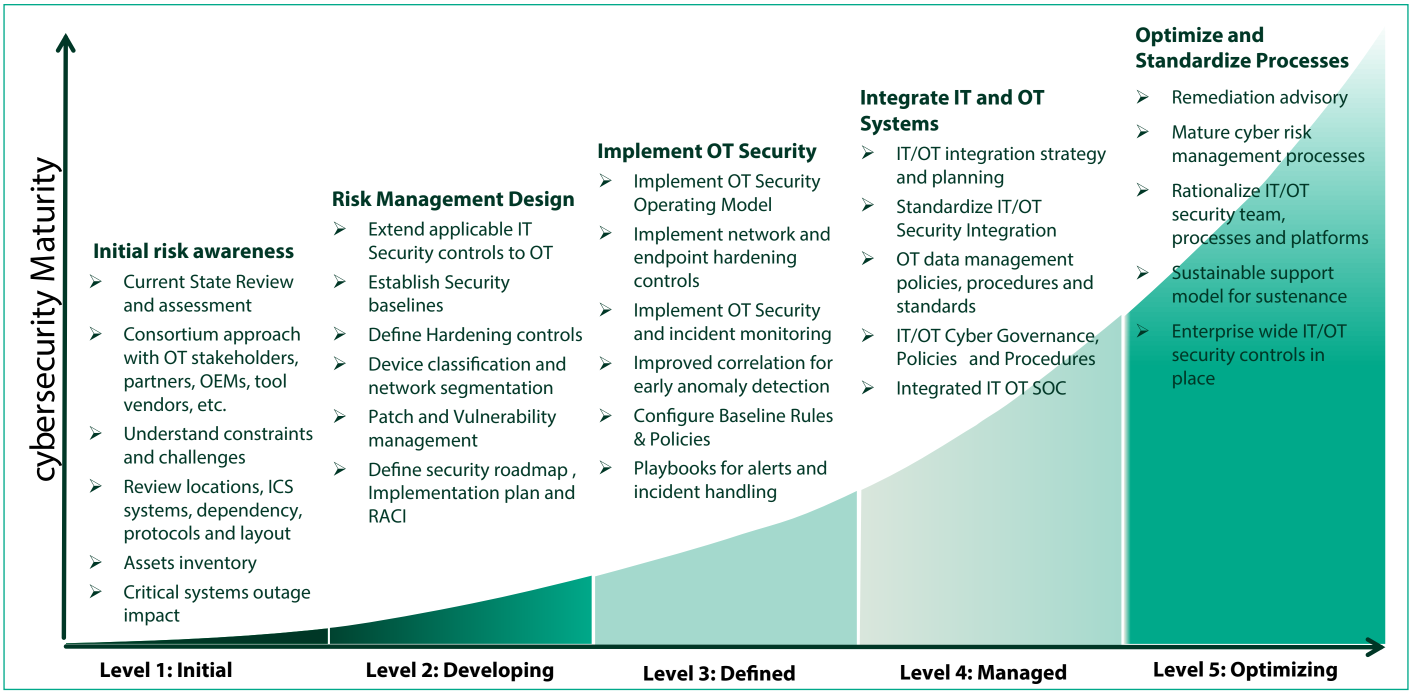


	Perform Evaluation	Analyze identified Gaps	Prioritize and Plan	Implement Plans
Inputs	ONG-C2M2 Self-Evaluation Template Policies & Procedures Understanding of Cybersecurity Program	ONG-C2M2 Self Evaluation Report Organizational Objectives Impact to Critical Infrastructure	List of Gaps & Potential Consequences Organizational Constraints	Prioritized Implementation Plan Owners and Actions are defined
Activities	Conduct ONGC2M2 Self- Evaluation Workshop with Appropriate Attendees	Analyze Gaps in the Organization's context Evaluate Potential Consequences from Gaps Determine which Gaps Needs Attention	Identify Actions to Address Gaps Cost Benefit Analysis on Actions Prioritize Actions & Plan to Implement Prioritize Actions	Track Progress to Plan Re-Evaluate Periodically or in Response to Major Change
Outputs	ONG-C2M2 Self-Evaluation Report	List of Gaps & Potential Consequences	Prioritized Implementation Plan	Project Tracking Data

Figure 5: ONG-C2M2 process

Reference : Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model

The Infosys maturity roadmap stated below, helps oil & gas organizations in their maturity improvement journey by enabling them to identify their current maturity levels across their OT environment. It helps them identify the maturity target and activities needed for achieving the desired target. The maturity level moves from an isolated & insecure OT environment to an integrated enterprise ecosystem with shared utilization of resources at Level 5. It defines the actions that are needed for their IT OT convergence program. The initial key activities include assessment of the maturity level & risk from the OT systems to their business, preparing propositions in terms of business outcomes, reviewing the effectiveness of existing governance for IT/OT alignment and identifying how the digital journey will impact the organization from a cybersecurity perspective. It is important that the organization identify its desired maturity level based on the business value and then set the target maturity level goal along with planned activities and timelines for achieving it.



Initial risk awareness

- Current State Review and assessment
- Consortium approach with OT stakeholders, partners, OEMs, tool vendors, etc.
- Understand constraints and challenges
- Review locations, ICS systems, dependency, protocols and layout
- Assets inventory
- Critical systems outage impact

Risk Management Design

- Extend applicable IT Security controls to OT
- Establish Security baselines
- Define Hardening controls
- Device classification and network segmentation
- Patch and Vulnerability management
- Define security roadmap , Implementation plan and RACI

Implement OT Security

- Implement OT Security Operating Model
- Implement network and endpoint hardening controls
- Implement OT Security and incident monitoring
- Improved correlation for early anomaly detection
- Configure Baseline Rules & Policies
- Playbooks for alerts and incident handling

Integrate IT and OT Systems

- IT/OT integration strategy and planning
- Standardize IT/OT Security Integration
- OT data management policies, procedures and standards
- IT/OT Cyber Governance, Policies and Procedures
- Integrated IT OT SOC

Optimize and Standardize Processes

- Remediation advisory
- Mature cyber risk management processes
- Rationalize IT/OT security team, processes and platforms
- Sustainable support model for sustenance
- Enterprise wide IT/OT security controls in place

Figure 6: Cybersecurity maturity roadmap

Although the risk level and current maturity may vary for different organisations there are few controls for industrial security transformation which every oil and gas organisation should have in place. Deploying these controls can be an effective initiation point for a comprehensive integrated cybersecurity program aimed at achieving the identify, protect, detect, respond and recover capabilities.

Security policy & guidelines: Defining and establishing security policies, procedures and guidelines for the ICS environment. It should cover the control areas such as asset inventory, access control, patch management, network security, workforce development, portable media usage, security incident management, backup and restore, etc.

Assets visibility: Maintaining complete asset inventory detailing the total assets, attributes, types and locations. Performing periodical reconciliation and reviews. Providing complete visibility of OT assets including the SCADA systems and field devices and network visibility using passive monitoring of the OT network. This monitoring has Zero impact on existing systems and processes. It provides automated asset discovery, classification and management along with real-time monitoring of asset configuration and changes in the network. It gathers extended information and details of all PLC/ RTU/DCS/SCADA devices including OS & firmware versions, associated vulnerabilities with mitigation recommendations.

Network security: Communication and access to the ICS environment must be defined & aligned with the business needs. Network segmentation, segregation and secure baselines should be implemented as per the best practices. We help organizations to design and implement security architecture using zones and conduits incorporating DMZ's as per IEC 62443. The conduits have appropriate security controls and technologies like firewalls and VPN. Blocking all communication from IT to OT or else having a minimal connection (single if possible) through a Firewall and DMZ. Reviewing the firewall rules regularly to make sure adequate protection is provided in light of the ever- changing security threats.

Continuous monitoring: Implementing passive security platforms for ensuring 24/7 centralized monitoring for all the incidents and events performed in an operational environment. Conducting real time monitoring of OT security activities. Integrating the alerts from OT security platform and leveraging the existing IT CDC infrastructure and team for monitoring the security events and carrying out the handling of incidents from OT environment.

Security governance: Ownership, roles and responsibilities must be developed, defined and implemented. The secure governance framework is the foundation for building a resilient security framework. It is highly recommended to focus on identifying the gaps and mitigating the governance in areas of access management, roles and responsibilities, third-party management, incident management, patch and vulnerability management, policy and configuration management and back-up policy

Removable media: The use of removal media must be restricted and should be scanned for malware and virus. A dedicated and approved set of portable media should be maintained that can be used in an OT environment. Its access should be restricted.

Access control: Assets within the ICS environment be it physical or logical should be accessed only with proper authentication and authorization. Implementation of digital identity, privileged access mechanism, secure remote access and centralised password management tools can be leveraged to address major security concerns in the area of access management.

Training and Awareness: Regular training and awareness programs must be in place for professionals at each level to ensure that systems and environments are being used in a secure and responsible manner. Continuous interactive evaluation and improvement programs based on the best security practices and simulation-based training demonstrating the potential impact of security breaches in the real-world scenario should be implemented.

Incident management: Incident management and response processes should be developed and tested periodically. Integrating security platforms to existing centralised SIEM solutions for developing test cases and event correlation of security incident and alerting must be carried out.

Patch & vulnerability management: Defining and implementing a systematic, accountable, and documented patch and vulnerability management process for managing exposure to vulnerabilities. Defining governance framework for identifying and evaluating the severity of new or existing vulnerabilities and mitigating them in a timely and effective manner. Periodical review of patches and vulnerabilities must be performed to keep track of the security status in the environment.

Brief Summary

In this new age of connectivity, the past practices of isolation between the corporate and operations environment for oil and gas sectors have pretty much disappeared. As digitization continues to grow in the operational environment and the risk of sophisticated cyber-attacks looms large, the preparedness of industries is still in the initial phase.

With this connected world and sophisticated cyber-attacks scenario, the need for closing the security gaps in an operational environment cannot be ignored. Any further delay could lead to a potentially disastrous impact on the sector.

Never in the past, the need for strengthening the security and resilience of operational infrastructures against cyber threats has risen to this scale. The starting point for the industry is to initiate cyber maturity assessment, analysing the current state of the environment and preparing a roadmap for addressing the security challenges by defining the short term, medium term and long term goals. A secured IT OT integration helps oil & gas companies to transform from disconnected networks to integrated businesses thus fast-tracking their digitization journey.

Authors

Suhas Desai, Industry Principal, Infosys

Nilby Jose, Principal Consultant, Infosys

Saurabh Srivastava, Consultant, Infosys

Yogesh Shelke, Associate Consultant, Infosys

For more details, please contact: CyberSecurity@infosys.com

Infosys®
Navigate your next

For more information, contact askus@infosys.com