



CYBER RESILIENCE AND BEYOND: A ROADMAP TO BUILDING INCIDENT RESPONSE SUCCESS



Cybersecurity incidents in the oil and gas sector present unique challenges that differ greatly from natural disasters or physical attacks. With the average downtime from a cyberattack estimated at 24 days, the potential financial and reputational damages are significant. This roadmap outlines strategic steps to enhance your preparedness and response capabilities to these threats.

Phase I



PREPARE FOR THE INEVITABLE



Imagine 150,000 people checking your windows and doors every hour to see if they are unlocked. That is what it's like to operate in today's digital environment. The question isn't if a cyberattack will happen to your company, but when. Threat intelligence and data replication are two critical components of preparing for the inevitable attack.

Threat Intelligence

Monitoring and analyzing cyber threats allow you to identify and predict adversaries' tactics, techniques, and procedures (TTP). Employing the concept of the cybersecurity "kill chain" helps in understanding how attackers escalate privileges and move laterally within the network. Recognizing the indicators of compromise (IoC) early in the kill chain can be crucial for a timely response.



Kill Chain: The steps an attacker takes to identify and exploit vulnerabilities to extract data or deploy malicious payloads, often starting with reconnaissance and culminating in data exfiltration.

Data Replication

Cyberattacks may necessitate the complete shutdown of Industrial Control Systems (ICS). Therefore, robust data replication strategies are vital for ensuring data availability during and after an incident. Aligning Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) with business continuity plans ensures minimal operational downtime.



RTO: The maximum duration your business operations can withstand being offline after an incident.



RPO: The maximum tolerable data loss measured in time.

Phase II

COUNTER AND CONTAIN

Effective utilization of threat intelligence enables real-time monitoring and predictive analytics of ongoing cyber threats, which can enhance decision-making capabilities once a breach occurs. Implementing robust segmentation, isolation, and virtualization controls can significantly limit damage.

Segmentation and Isolation

Dividing a network into smaller, manageable segments and isolating compromised systems to prevent the spread of an attack is a cornerstone of network security. This strategy limits access to critical resources and contains the attack to controlled zones.

Virtualization

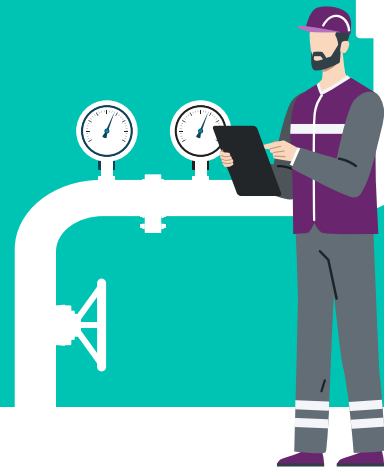
Leveraging virtual machines (VMs) to run applications or processes ensures they can be compartmentalized, isolated, and managed independently. In the event of a compromise, affected virtual instances can be replaced with minimal impact on other operational areas paramount to critical business functions.



Phase III

RECOVER AND RESTORE

Post-incident recovery begins with thoroughly assessing the damage and identifying compromised systems. This assessment helps prioritize recovery efforts and resource allocation.



Post-Incident Analysis

It is crucial to evaluate the efficacy of your threat intelligence system and understand the specific vulnerabilities exploited during the attack. This evaluation should inform the continuous improvement of security measures and incident response strategies.

Continuous Improvement

An incident response plan is not static; it requires ongoing evaluation and updating to adapt to the evolving cyber threat landscape and ensure preparedness for future incidents.

CTG offers tailored solutions to level up your current security posture. Connect with one of our experts today: solutions@ctg.com | www.ctg.com