INTRODUCTION
Our increasing dependence on technology and web-based communication has opened the door for cybersecurity threat, particularly in the oil and gas industry. Petroleum companies face significant threats, such as hydrocarbon installation terrorism, which can cause plant shutdowns resulting from sabotage and interruption of utilities. With the oil and gas sector fueling every aspect of our daily life, the protection of this particular critical infrastructure has never been more crucial. We cannot afford to underestimate the consequences of attacks on the operations and systems that power our lifestyle.

WHAT ARE THE CONSEQUENCES?
- Plant Sabotage/Shutdown
- Utilities Interruption
- Production Disruption
- Hydrocarbon Installation Terrorism
- Facility Terrorism
- Undetected Spills

WHAT THREATS DO YOU FACE?

96% of all security incidents fall into nine basic patterns:
1. Point-of-Sale Intrusions
2. Crimeware
3. Cyber Espionage
4. Insider Misuse
5. Web App Attacks
6. Miscellaneous Errors
7. Physical Theft/Loss
8. Payment Card Skimmers
9. Denial of Service

HOW HAS THE THREAT EVOLVED?
In 2010, STUXNET shocked the industry as the first computer worm to attack SCADA systems. A year later, a derivative—DUQU—was specialized for cyber espionage. Today, oil and gas stakeholders face more advanced threats, such as DUQU 2.0 and Flame. As cybersecurity threats grow in scope, owners and operators must proactively secure critical industrial controls and systems.

WHAT'S REQUIRED?
- HSPD-7 requires the strengthening of the security and resilience of critical infrastructure against cyber threats that could have a debilitating impact on national security, economic stability, or public health and safety, including acts of terrorism.
- CFATS identifies and regulates high-risk chemical facilities to ensure that they have the necessary security measures to avoid attack or exploitation.
- NERC CIP defines industrial cybersecurity standards, focusing on system reliability and customer information security.

GUIDELINES
- American Petroleum Institute (API) 1164
- API – Recommended Practice 780, Risk Assessment Methodology
- ISA/IEC-62443
- Interstate Natural Gas Association of America (INGAA) – Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry

WHAT SHOULD YOU PROTECT?

- PIPELINES
- EXPLORATION & PRODUCTION
- TANK FARMS
- UTILITIES/ OFF-SITES
- CONFIDENTIAL DATA
- BUILDINGS
- REFINERIES
- TELECOM
WHY PARSONS FOR CYBERSECURITY?

Parsons has worked behind the scenes for 30+ years to deliver cybersecurity services that have protected our nation’s most sensitive information and critical infrastructure to federal customers. This experience is enhanced by 70+ years of experience designing, building, and managing these assets around the globe. Parsons has combined its in-depth knowledge of cybersecurity with its expertise in the sustainment of critical assets to offer PARSecure®, a secure suite of services that includes both cyber and physical security. This offering allows us to leverage our experience and become a trusted cybersecurity partner for customers in federal, state, and local government, and the commercial marketplace. Using PARSecure® and our team of cybersecurity experts, we can ensure that cutting-edge cybersecurity people, processes, and technologies are in place—addressing the full spectrum of risks to your business and protecting your most valuable assets. Setting us apart is our state-of-the-art Cyber Solutions Center, located in Centreville, VA. This hands-on laboratory enables the Parsons team to demonstrate and analyze operational networks, supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICS) that control all critical infrastructure, building systems, manufacturing systems, medical treatment facilities, water and wastewater, transportation, and more. We can then custom design, test, and implement the technical options needed to protect the security of client networks and infrastructure, in addition to providing training to those entrusted to maintain the security of these systems. Parsons is a leader in technical solutions, continuity of operations, critical infrastructure, and classified facility protection. Together, we create a safer, more secure world.