PIPELINE CYBERSECURITY

ENHANCING THE RELIABILITY OF AMERICA'S LIQUID AND GAS DELIVERY SYSTEMS

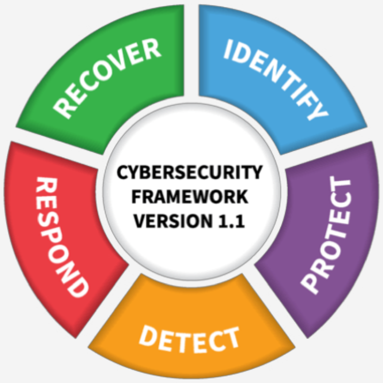
Liquid and natural gas pipeline operators take the cybersecurity of their assets and operations very seriously. The evolving threats targeting America's critical infrastructure cannot be ignored, and energy companies are keenly aware of the threats. Through their own security experts, security vendors, and relationships with the intelligence community, pipeline companies are getting the information they need to protect and defend their systems. Pipeline companies are participating in the Downstream Natural Gas and Oil and Natural Gas Information Sharing and Analysis Centers (ISACs) as another vector to receive and share threats to the industry.

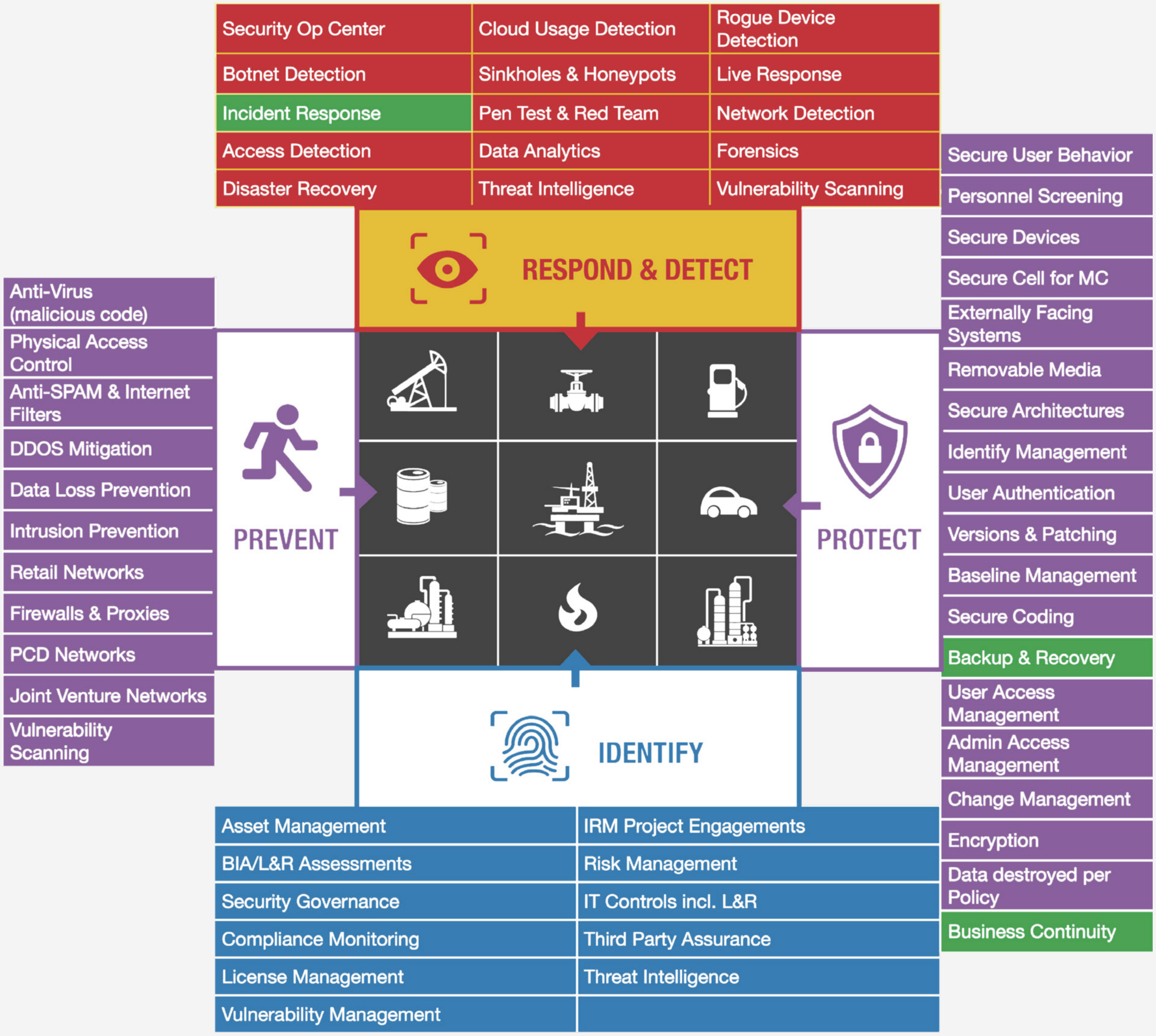
While there are an increasing number and severity of cyber threats to pipelines, that does not equate to higher vulnerability. Companies operating pipelines are continuously responding to threats and increasing the sophistication of their defenses. Most, if not all, of the largest industry companies – including natural gas pipeline operators – manage cybersecurity as an enterprise risk – the highest designation – with oversight from Boards of Directors and Senior Executives.

The reliance upon proven risk management-based frameworks and public-private collaboration, rather than prescriptive regulation, is the best way to bolster the cybersecurity of the natural gas and oil pipeline industry. With the increasing sophistication and adaptiveness of cyber adversaries, it is essential that industry be afforded the necessary flexibility and agility to respond to a constantly-changing threat landscape, and that government and industry continue to partner to share cyber threat intelligence and strengthen cyber defenses.

In recognition of the sophistication and dedication of cyber attackers, and the enterprise risk presented by cyberattacks, natural gas and oil pipeline companies have developed comprehensive risk-based "defense-in-depth" approaches to cybersecurity similar to industry's approach to managing the other enterprise risks: robust governance, systematic risk-based management, and multi-dimensional programs based on best-in-class standards and proven frameworks.

A layered defense approach provides optimal protection in the rapidly evolving cyber threat landscape, as no one layer of defense or technology will ever be completely effective. This approach creates a landscape that is much more challenging for an attacker to fully penetrate – providing necessary time to implement defensive response measures.





Security Op Center	Cloud Usage Detection	Rogue Device Detection
Botnet Detection	Sinkholes & Honeypots	Live Response
Incident Response	Pen Test & Red Team	Network Detection
Access Detection	Data Analytics	Forensics
Disaster Recovery	Threat Intelligence	Vulnerability Scanning

RESPOND & DETECT

PREVENT

- Anti-Virus (malicious code)
- Physical Access Control
- Anti-SPAM & Internet Filters
- DDOS Mitigation
- Data Loss Prevention
- Intrusion Prevention
- Retail Networks
- Firewalls & Proxies
- PCD Networks
- Joint Venture Networks
- Vulnerability Scanning

PROTECT

- Secure User Behavior
- Personnel Screening
- Secure Devices
- Secure Cell for MC
- Externally Facing Systems
- Removable Media
- Secure Architectures
- Identify Management
- User Authentication
- Versions & Patching
- Baseline Management
- Secure Coding
- Backup & Recovery
- User Access Management
- Admin Access Management
- Change Management
- Encryption
- Data destroyed per Policy
- Business Continuity

IDENTIFY

Asset Management	IRM Project Engagements
BIA/L&R Assessments	Risk Management
Security Governance	IT Controls incl. L&R
Compliance Monitoring	Third Party Assurance
License Management	Threat Intelligence
Vulnerability Management	

Example of cybersecurity programs deployed across one company

Natural gas and oil pipeline companies implement cybersecurity programs that comprise many components. Companies often frame these components through the lens of the National Institutes of Standards and Technology's (NIST) Cyber Security Framework (CSF), a voluntary framework intended to provide a common language organizations can use to assess and manage cybersecurity risk.

The CSF is designed to complement, and not replace or limit, an organization's risk management process and cybersecurity program. Each individual organization can use the CSF in a tailored manner to address its cybersecurity objectives. Operators can use the CSF, as well as the Transportation Security Administration's (TSA) Pipeline Security Guidelines, to ensure they are appropriately assessing and responding to risks in an ever changing threat landscape.

Most natural gas and oil pipeline companies operate in a cybersecurity landscape consisting of three critical areas: the industrial control systems (ICS), internet-facing components and internal networks. Natural gas and liquid pipeline companies account for and manage cybersecurity to protect the use of automated digital controls, or ICS, are not unique or new to pipelines; they are prevalent across the entire energy landscape, including at coal and nuclear power generation facilities.

Today's ICS environments in the natural gas and oil industry rely on computing technologies for advanced control of unit processes, such as adjusting valves to regulate pressure or controlling pumps to regulate product flow, located in refineries, petrochemical plants and pipeline/terminal distribution sites. These technologies in turn make operations vulnerable to cyber threats. For this reason, it is a widely accepted practice to ensure ICS remain logically isolated from systems providing control of the unit.

Organizations mitigate the risk of a cyber threat to internal networks from exposure to the public internet by creating a security zone between the ICS and business network that is frequently referred to as the DMZ. Firewalls within the DMZ serve as "data diodes" allowing specific information to travel from ICS to IT environments while limiting or eliminating information flow from IT environments to ICS.

A company's business network or enterprise zone is the environment where users perform functions such as email, collaboration and analytics. It is here that companies hold most intellectual property assets and conduct other internal business transactions. For the natural gas and oil pipeline industry, the most valuable intellectual property includes information regarding proprietary technology, breakthrough research, bid proposals and acquisitions and mergers. Industry's cybersecurity focus in this area relies on early detection and a layered approach to defenses. User awareness training is also a critical focus area as it is highly recognized that no amount of technology will protect against every threat – the end-user plays a large role as a layer in defense.

The natural gas and oil pipeline industry relies on internet-facing components such as e-commerce for product purchases along with areas that allow collaboration with business partners. These components are contained within an area of a company network that is outwardly facing to the public and separated from the internal business network by another DMZ.

The reliance upon voluntary mechanisms including the aforementioned use of proven frameworks and public-private collaboration, rather than compulsory standards or regulations, is the best way to bolster the cybersecurity of industry companies and the critical infrastructure they operate. The pipeline industry is already deeply engaged on the issue of cybersecurity and working to stay informed and ahead of our adversaries. With the increasing sophistication

Pipeline Companies Operate to Leading Cybersecurity Standards and Frameworks

API Standard 1164

Content unique to pipelines not covered by NIST CSF and IEC 62443; Currently being updated with expected completion in 2019.

NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)

Pre-eminent Framework adopted by companies in all industry sectors; Natural gas and oil companies increasingly orient enterprise-wide programs around NIST CSF.

International Electrotechnical Commission's IEC 62443

Pre-eminent family of standards for industrial control systems (ICS) security; Widely-adopted by natural gas and oil industry; applicable to any type of natural gas and oil ICS.

International Organization for Standardization ISO 27000

Best-known standard in the family providing requirements for an information security management system (ISMS).

and adaptiveness of cyber adversaries, and it is essential that industry be afforded the necessary flexibility and agility to respond to a constantly-changing threat landscape and the continuous innovation by cyber criminals.

Government efforts related to pipeline security are covered by the TSA's Office of Security Policy and Industry Engagement's Surface Division. With the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties, TSA developed the Pipeline Security Guidelines. Utilizing a similar industry and government collaborative approach, these guidelines are regularly updated to reflect the advancement of security practices to meet the ever-changing threat environment in both the physical and cybersecurity realms[i].

Natural gas and oil companies provided input to TSA as it developed and updated the Pipeline Security Guidelines. Pipeline operators also partner with TSA through its Pipeline Corporate Security Review program as TSA has completed reviews of all the nation's top 100 pipeline systems, which transport 84 percent of the nation's energy[ii]. Recently, DHS announced they will provide more support to TSA's efforts to enhance pipeline security through the newly formed National Risk Management Center. The industry is ready to engage with this effort as it begins to take shape.

Pipeline companies agree with policymakers and others that cybersecurity of the nation's critical infrastructure is a priority. The industry takes seriously the responsibility to protect the infrastructure in order to provide reliable energy for society and to safeguard the public and the environment. The industry faces an increasing number of cyberattacks and evolving, sophisticated cyber threats from a variety of malicious actors including nation states, criminal organizations and others. These threats are not unique or new to pipelines; they are prevalent across the energy system, and the pipeline industry to taking the needed steps protect their personnel, systems, and operations.

[i] Transportation Security Administration Office of Security Policy and Industry Engagement's Surface Division, Pipeline Security Guidelines, March 2018, https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

[ii] Transportation Security Administration, "Securing and Protecting Our Nation's Pipelines," 2016, https://www.tsa.gov/news/releases/2016/07/11/securing-and-protecting-our-nations-pipelines

energy API | AMERICAN PETROLEUM INSTITUTE