network perception

# Understanding Risk-Based Compliance Verification

*The May 7, 2021 ransomware attack on Georgia's Colonial Pipeline Co. may prove a watershed moment for the way energy companies tackle escalating and increasingly complex cybersecurity challenges. Building IT and OT partnership through a focused risk-based compliance verification strategy can help your organization stay ahead of evolving threats and a fast-changing regulatory landscape. Here's how.* **| by Lisa Holton**

## Executive Summary

Energy is one of 16 industries defined by the Department of Homeland Security (DHS) as critical to the nation's economic security, national public health and safety. Yet rapid digitization, amplified by workplace and facility disruptions during the COVID-19 pandemic, has exposed industrial control systems to important cybersecurity vulnerabilities.

Energy firms typically operate with geographically dispersed legacy communication systems tied to strict availability requirements that don't work well with traditional IT-centric cybersecurity solutions. In this Network Perception White Paper, we'll explore how a risk-based, compliance verification-first focus can help stakeholders validate the correct segmentation of their network and improve their cybersecurity and resilience strategies as new threats emerge.

## Introduction

In May 2021, hackers broke into the network of Colonial Pipeline Co. with nothing more than a phishing email —triggering the shutdown of the largest fuel pipeline in the United States. The next day, Georgia-based Colonial paid a $5 million bitcoin ransom to DarkSide, a cybercriminal group believed to operate out of Russia.

The breach revealed how vulnerable even the most critical national energy infrastructures are to the rapidly evolving world of cybercrime. As early as 2018, one estimate showed that nearly 60% of energy companies had experienced a breach in their industrial control (ICS), supervisory control and data-acquisition (SCADA) systems.

Regulatory response to the Colonial Pipeline attack was swift. Between May-July 2021, DHS's Transportation Security Administration (TSA) would issue two security directives to owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas. The first focused on incident reporting and emergency response; the second focused on threat mitigation and long-term contingency and recovery planning.

We anticipate even stricter regulation in the future. And with that rising regulatory agenda come significant time, training and cost concerns related to compliance issues. In June 2021, the annual Cost of a Data Breach Report from IBM and the Ponemon Institute reported that out of 25 factors that either amplify or mitigate breach costs, regulatory compliance ranked No. 1.

It's a particularly urgent message for professionals in the merging world of information technology (IT) and operational technology (OT). Developing a focused and independent approach to risk-based compliance verification can help set realistic resiliency targets as cybersecurity and regulatory agendas accelerate.

We believe that most energy organizations will learn — if they haven't already — that their legacy and often geographically dispersed OT systems are vulnerable to both high- and low-tech attacks that can weaken power grids anywhere in the world.

For example, the 2013 sniper attack on a Pacific Gas and Electric substation just south of San Jose was accomplished by gunmen with apparently unfettered physical access to the facility. No software required.

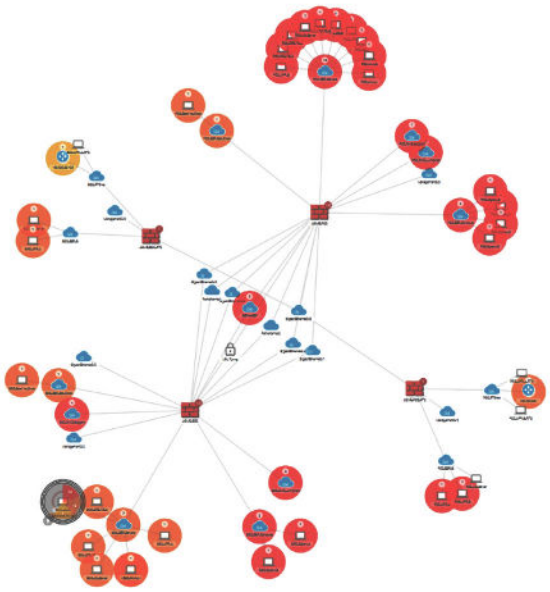
Enter COVID-19. Cybercrime has continued to escalate exponentially during the pandemic and to a wider range of utilities. By summer 2020, worldwide denial-of-service cyberattacks on utilities rocketed almost 600% from the previous year, and an October 2021 alert from the Cybersecurity & Infrastructure Security Agency (CISA) pointed to escalating ransomware attacks on both OT and IT assets throughout U.S. water and wastewater systems, citing: "the increased use of remote operations due to the COVID-19 pandemic has likely increased the prevalence of weaknesses associated with remote access."

As these threats evolve, decision-makers need more holistic compliance structures to keep their organizations safe. This paper will focus on what risk-based compliance verification means, how important network segmentation is for the energy industry and why investing in it today will be essential for enterprise safety, growth, and success.

## Assessing the Industrial Threat Landscape

In April 2021, President Joe Biden launched a U.S. Department of Energy (DOE) initiative to protect the energy sector supply chain from cybersecurity risks. It calls for:

- Implementation of measures or technology to enhance cyber risk detection, mitigation, and forensic capabilities;
- Setting concrete milestones for owners and operators to identify and deploy technologies and systems that enable near-real-time situational awareness and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks;
- Reinforcing and enhancing the cybersecurity posture of critical infrastructure information technology (IT) networks; and
- Including a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.



The administration's emphasis on ICS and OT networks is significant. As many organizations weigh cybersecurity investments in their legacy technology, they also must weigh potential risks from industrial internet of things (IIoT) technologies that will play a larger part in their future operations.

Already, many operational technologies are supported by vendors in the cloud — a source of greater efficiency but a significant new third-party security risk with potentially dramatic consequences. In July 2021, Gartner reported that by 2025, cyber attackers will have weaponized OT environments to "successfully harm or kill humans," adding that "organizations in asset-intensive industries like manufacturing, resources and utilities struggle to define appropriate control frameworks."

Organizations must balance these accelerating risks with a regulatory schedule that's now continual due to digitalization. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) now requires year-round audits with a calendar that announces upcoming additions or changes to standards.

Keeping ahead of threats and regulatory requirements will require organizations to develop a more holistic and hierarchical approach to industrial control systems that may be beyond current standards like the Purdue Model of Computer Integrated Manufacturing.

Adopting risk-based compliance verification practices will help guide that evolution.

## A Look at Today's Key Threats

As many industries have digitized processes over the years, some have not planned for security risks associated with the aggressive digitalization that has accelerated during the pandemic. It's left organizations open to widening threats including:

- **Supply Chain Vendor Risk Management:** When cyber criminals distribute a type of malware disguised as legitimate software that allows cybercriminals to breach and take control of a company's computer system, as happened at network software company SolarWinds in December 2020.
- **Ransomware:** Fueled by human error and security breaches related to remote work, ransomware is invasive software unleashed in an otherwise ordinary email or similar communication that when opened can lock up a network until a ransom is paid, as happened in the Colonial Pipeline attack.
- **Insider Involvement:** Employees and deeply embedded vendors and suppliers can have the closest proximity—and sometimes the most sophisticated knowledge of your facilities, equipment and electronic systems. They are uniquely qualified to launch attacks or enable attacks with no awareness they're involved at all. For example, in July 2021, the Kaseya malware cyberattack disrupted some 1,000 businesses along the Dublin company's supply chain through weak points in the firm's network.

### What is a mission-critical asset?

Any device, software application or digital database essential to the daily operation of your business. If removed, stolen or destroyed, your business could not run.

## Why OT Attacks Are Becoming More Significant

In many cases, the tactics used in cyberattacks are starting to blur — but they're also becoming more sophisticated as cybercriminals develop greater awareness of how physical and electronic assets work together within the organizations they're targeting. In energy, the potential consequences of weaknesses within physical and electronic systems are potentially vast.

Consider a transmission line that's intentionally damaged by criminals on the ground, similar to the PG&E attack mentioned above. Typically, utilities have software to detect and re-route service when any disruption occurs, no matter what the cause.

However, consider a coordinated physical and cyberattack on the same transmission line where a hacker successfully disarms the electronic barriers provided by that software, essentially allowing disruptions from that damaged line to spread throughout the grid.

Such legacy OT systems are providing lucrative entryways for attackers to capture a vast number of mission-critical assets.

## How Risk-Based Compliance Verification Builds a Constant, Long-Term Defense

Investing in risk-based compliance verification allows an organization to build cyber resiliency from the ground up. It will help you understand:

- Your current cybersecurity status and how you can use it to set a baseline for long-term systems and business security
- How to strengthen data-collection processes so you will have trusted reports to measure progress and success
- Ways to ensure accountability and team alignment based on fundamental principles observed throughout the organization.

Building effective risk-based compliance verification begins by understanding the dependencies between your critical operations and your cyber systems. Start by identifying mission-critical assets within your organization that must be protected. Then determine where they are, how critical they are to your daily operations, and who or what systems have access to them through network connectivity.

## Building a Robust Risk-Based Compliance Framework

During the past 15 years, most energy organizations have already built the culture and the tools to handle effective year-round compliance verification. Here's how to develop a heightened risk focus into the picture. In the energy sphere, leaders should start by reviewing its respective regulatory resources made available by NERC, the Federal Energy Regulatory Commission (FERC), and relevant organizations like the National Institute of Standards and Technology (NIST).

Once a compliance framework is established around those regulatory relationships, leaders should identify a dedicated compliance task force with clear roles and assignments close to key parts of company infrastructure. That team should work within an independent process with clear separation of duties.

As an example, organizations can better protect their mission-critical assets by leveraging the critical infrastructure protection (CIP) requirements from the NERC compliance framework. The requirements specifically tied to network segmentation include:

- **CIP-002 R1:** Identify each of the medium and high impact bulk electric system cyber assets
- **CIP-005 R1.1:** All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP
- **CIP-005 R1.2:** All External Routable Connectivity must be through an identified Electronic Access Point (EAP)
- **CIP-005 R1.3:** Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default
- **CIP-005 R2.1:** Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset
- **CIP-005 R2.2:** Interactive Remote Access sessions must be encrypted to the Intermediate System to protect the confidentiality and integrity of the communications (Figure 1)

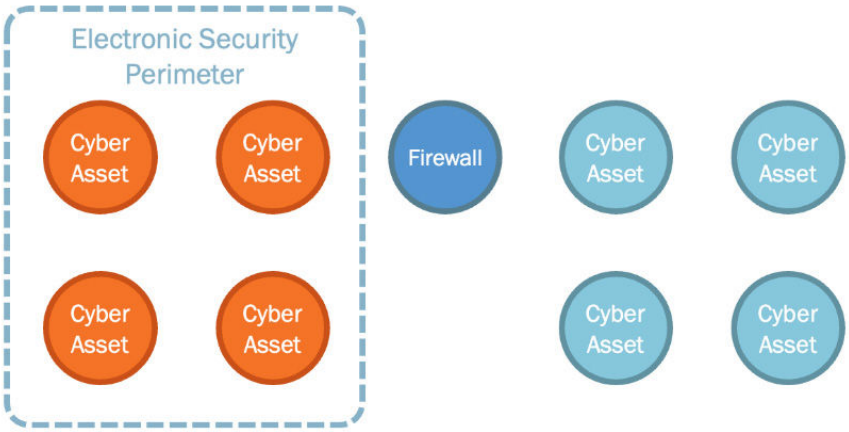



**Figure 1—**Per NERC CIP, cyber assets that are critical for operations should be identified through an electronic security perimeter and protected by firewalls.

# Step-by-Step Independent Network Risk Verification Process

Organizations don't need a size requirement to develop an effective risk-based compliance verification process. Most companies can begin with these three steps:

## Step 1: Collect Access Policy Documentation

- Collect network access policy requirements based on the risk assessment framework
- Review existing documentation for network topology and asset inventory
- Identify connected critical assets: which applications require network access and why

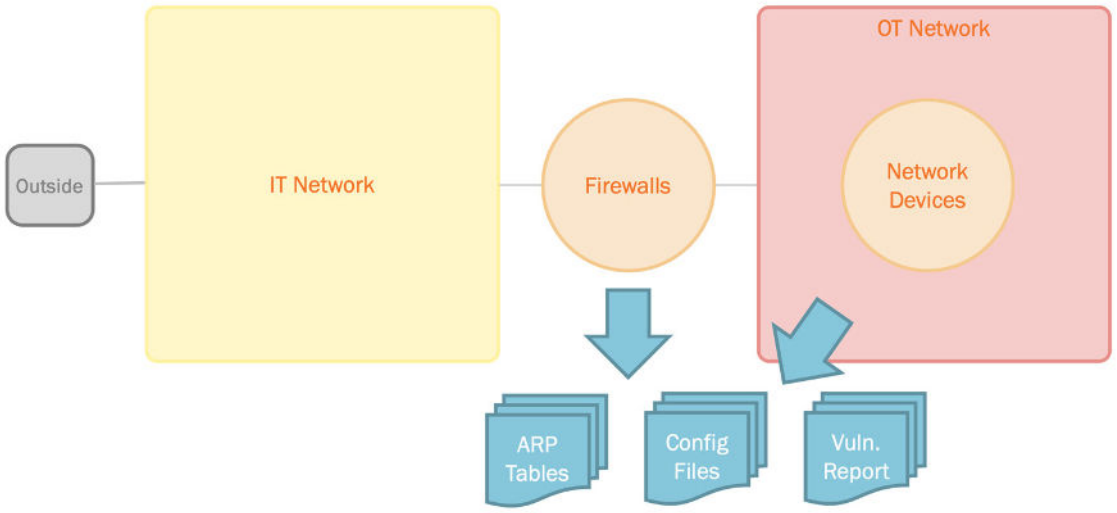



**Figure 2—**Establish your baseline.

## Step 2: Establish Your Baseline

- Collect network device configurations, including firewalls, routers, and layer-3 switches (Figure 2)
- If possible, identify connected assets using the address resolution protocol (ARP) tables of your network switches
- If available, gather end-point vulnerability information from existing scan reports (Figure 3)
- Generate your network topology diagram and add network zone information
- Identify your respective "crown jewels" that need protection — such as critical cyber assets and their locations (this is the Electronic Security Perimeter (ESP) in the case of NERC CIP)

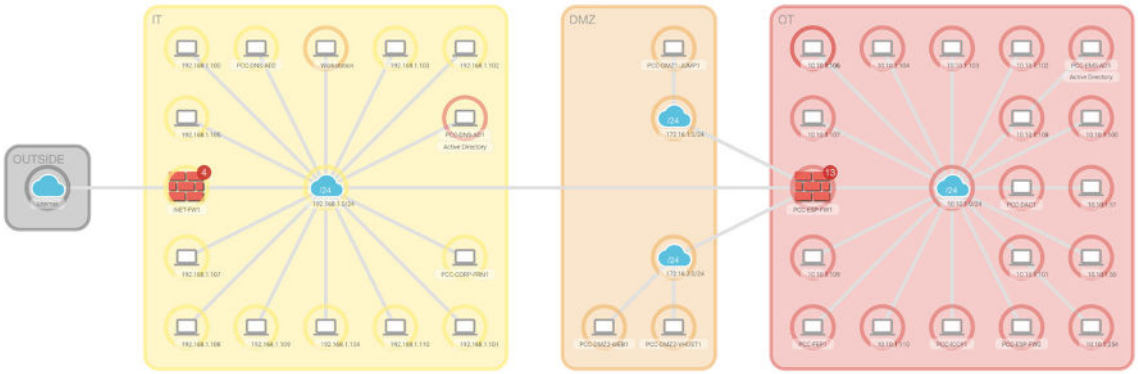



**Figure 3—**If available, gather end-point vulnerability information from existing scan reports.

## Step 3: Compare Your Policy Against Your Baseline and Document the Gaps

- Verify that access rules allowing inbound and outbound connectivity to and from the zones hosting your crown jewels match authorized communications
- Run a network path analysis to clearly identify system-to-system and interactive remote access (Figure 4)
- Document overly permissive rules, misconfigurations, and incorrect network segmentation (Figure 5)

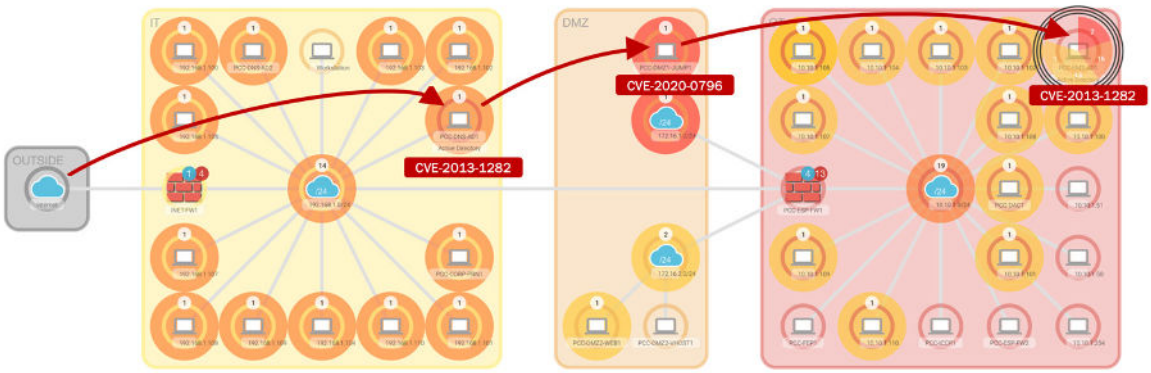



**Figure 4—**Run a network path analysis to clearly identify system-to-system and interactive remote access.

| Top Access Policy Risk | Recommendation |
|---|---|
| Lack of egress access | Apply principle of least privilege in all directions: verify the scope of outbound access rules |
| Lack of documentation | Adopt a disciplined change tracking and firewall rule justification workflow |
| Overly permissive rules | Apply principle of least privilege: verify the scope of source, destination, service |
| Insecure services | Replace outdated protocols with secure versions |
| Access list complexity | Adopt a disciplined change tracking and firewall rule justification workflow. Periodically clean up unused rules. |

**Figure 5—** Document overly permissive rules, misconfigurations, and incorrect network segmentation.

## Conclusion: Cyber Resiliency Begins with a Solid Risk-Based Compliance Verification Process

Only resilient organizations can defend against sophisticated cyberattacks. Remember these steps in creating and conducting an efficient risk-based compliance verification process:

- Adopt and leverage a cybersecurity compliance framework
- Develop an independent review process to establish your baseline configuration
- Compare your baseline against your intended access policy and document your gaps

If you have questions or would like to know more about risk-based compliance verification to ensure correct network segmentation, contact the Network Perception team at:

**(872) 245-4100 | info@network-perception.com**
**portal.network-perception.com**

### We're always ready to share ideas

Reach out to our **CEO Robin Berthier** | Visit our **White Paper Library**
Check our **Upcoming Events Schedule**