WHITE PAPER

An Industry Under Attack: Protecting the Oil & Gas Sector

Introduction

The oil & gas industry is navigating an era of rapid digital transformation, integrating Information Technology (IT) and Operational Technology (OT) systems to optimize operations. However, this convergence has also introduced critical cybersecurity vulnerabilities that pose significant risks to both data and physical processes. The integration of IT and OT is the industry's Achilles' heel, making it one of the most pressing security challenges today. Moreover, the need for remote access to these systems for increased flexibility and the move towards the cloud to further enhance operational efficiency have widened the attack surface, making these systems more visible and vulnerable to cyber threats. This white paper takes a deep dive into how to secure this integration, providing strategies to address the risks posed by interconnected environments and mitigate the impact of cyberattacks.

Beyond IT/OT integration, there is another crucial element: a unified security governance model. Managing IT, OT, and physical security separately often leads to blind spots and weakened defenses. Instead, a cohesive approach where a Chief Security Officer (CSO) oversees all security areas can bring everything into alignment. This model not only tightens up operations but also gives senior leadership a single point of accountability for all things security, a concept that has proven invaluable over my years as a CSO.

This report also digs into the unique cybersecurity challenges that the industry faces across its three main sectors: upstream, midstream, and downstream. Each has its own set of hurdles, from keeping remote drilling sites secure in the upstream, to protecting vast pipeline networks in the midstream, to safeguarding OT systems and sensitive customer data in downstream refining and retail. These challenges require tailored strategies for each sector, acknowledging the varied environments and threat landscapes they operate within. Understanding these differences is crucial for developing effective security measures that ensure the resilience of the entire industry.

Focusing on securing IT/OT integration and advocating for a unified governance approach, this paper aims to offer a clear path forward for oil & gas companies.

Upstream: Exploration and Production

Overview

In the oil & gas industry, the upstream sector—covering exploration and production—relies heavily on advanced technologies to enhance efficiency and maintain safe operations, even in some of the most remote and challenging locations. Think about offshore drilling platforms, isolated onshore fields, and vast production sites. These operations are powered by a variety of OT systems, from drilling control and production platforms to geophysical data systems, all working in real-time. While these technologies have undoubtedly boosted productivity and performance, they have also opened the door to new cybersecurity risks as more systems become interconnected through digital networks.

Cybersecurity Challenges

The upstream environment brings its own set of cybersecurity headaches, largely due to the complexity of its operations and the nature of working in remote, often unmanned sites. When IT and OT systems converge in this sector, they create a ripe target for cyberattacks that can disrupt production, damage infrastructure, or even trigger safety incidents. Here are some of the big challenges:

- **Securing Remote Production Sites:** Many upstream operations are isolated in hard-to-reach areas, whether on offshore platforms or remote onshore sites. Often, these locations have minimal staffing or are entirely unmanned, which makes them especially vulnerable to physical and cyber intrusions. Attackers can exploit weak network connections or unsecured systems to infiltrate critical OT systems from afar. Without strong protection, these remote sites can become an easy prey for attackers.

- **Protection of Proprietary Data:** The data generated during exploration and production—think seismic surveys and geophysical data—are the crown jewels of upstream operations. A breach here can mean more than just lost data; it can give competitors an edge or skew decisions that hinge on accurate resource data. A sophisticated cyberattack targeting this data can undermine years of work and significant investment.
- **Legacy OT Systems:** Today, many upstream facilities are still running on legacy OT systems that were designed long before cybersecurity was a major concern. Upgrading or patching these systems is not always straightforward, which makes them prime targets for attackers. The problem gets worse when these older systems are integrated with modern TCP/IP networks, creating potential pathways for attacks to jump from IT to OT systems, and turning a data breach into a full-blown operational crisis.
- **ICS and SCADA Vulnerabilities:** Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are the backbone of upstream operations, automating drilling rigs, monitoring pipelines, and controlling production platforms. They are indispensable for optimizing extraction processes and ensuring safety. But here is the catch: these systems often do not have the

robust security measures that come standard with modern IT networks. This makes them particularly vulnerable to attacks that could not only disrupt operations but also cause physical damage, turning a cyber incident into a real-world hazard.

Midstream: Transportation and Pipeline

Overview

When it comes to the oil & gas industry, the midstream sector plays a crucial role, moving and storing the lifeblood of the industry—oil and gas. Think of the vast network of pipelines stretching across countries, storage terminals, trains, and tanker trucks all working to ensure that these resources make their way smoothly from production sites to refineries. It's a massive logistical puzzle, with pipelines and facilities spread out over vast distances, often crossing borders. And with this scale comes some serious cybersecurity challenges: keeping those OT systems secure and staying a step ahead of threats from nation-state actors and organized cybercriminals.

Cybersecurity Challenges

It probably comes as no surprise that many of the same cybersecurity issues we see in the upstream sector also crop up in midstream operations. But midstream has its own set of headaches, particularly when it comes to dealing with international borders. Many pipelines weave their way through different countries, which means midstream operators have to navigate a maze of regulatory requirements. Each border brings a new set of rules and standards, making compliance a bit of a balancing act. And as regulations around cross-border data flows get stricter, keeping everything in line without missing a beat becomes even more of a challenge.

Downstream: Refining and Retail

Overview

The downstream sector is where crude oil gets its makeover—refining it into everyday products like gasoline, diesel, petrochemicals, and lubricants. But it does not stop there; it also ensures to bring those products to the end consumers, whether through gas stations or direct sales. As refineries digitize, IT systems become more embedded in retail operations, and automation takes on a bigger role, the downstream sector has become a prime target for cyberattacks. The stakes are high, and the risks have only grown as the sector evolves.

Cybersecurity Challenges in Refining Operations

Refining is complex and the stakes are high. It is not just about financial losses if something goes wrong—it is also about safety, the environment, and maintaining the trust of the public. Unlike midstream operations, which are more focused on transportation and storage, refining is all about intricate chemical processes. Advanced process control systems need to keep tight control over temperatures, pressures, and reactions. A cyberattack that disrupts these systems could lead to catastrophic outcomes—think explosions, toxic releases, or severe environmental damage. It is a delicate dance, and one misstep can have serious consequences.

Cybersecurity Challenges in Retail Operations

On the retail side of downstream, things are changing fast. Digital payment systems, customer loyalty programs, and smart tech are transforming gas stations, but they are also opening up new opportunities for cybercriminals. Here is a closer look at some of the challenges:

- **Integration of Internet of Things (IoT) in Retail Operations:** Gas stations are getting smarter with IoT tech—think smart pumps, real-time inventory management, and environmental monitoring (like fuel leak detection). But every IoT device is a potential door for attackers. If one gets compromised, it could give bad actors access to payment networks, customer info, or even key fuel management systems.
- **Hybrid Retail Operations:** These days, many gas stations are more than just places to fill up your tank. They are convenience stores, offering food, drinks, and other services. This means blending different systems—point of sale (POS), supply chain management, payment processing, and more. With all these systems working together, there is a lot more room for vulnerabilities and potential fraud.
- **Loyalty Programs and Personal Data:** Customer loyalty programs are great for business, but they also mean collecting lots of sensitive data. If these systems are not locked down properly, cybercriminals could get their hands on that information, leading to breaches that could damage a company’s reputation and result in serious legal issues, especially when it comes to meeting data protection regulations.

Cybersecurity Strategies for the Oil & Gas Industry

Cybersecurity Strategies for the Oil & Gas Industry

As the oil & gas sector goes all-in on digital transformation, the stakes are high when it comes to cybersecurity. With systems becoming more interconnected, a solid cybersecurity strategy is non-negotiable if we want to keep critical infrastructure safe.

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
NIST

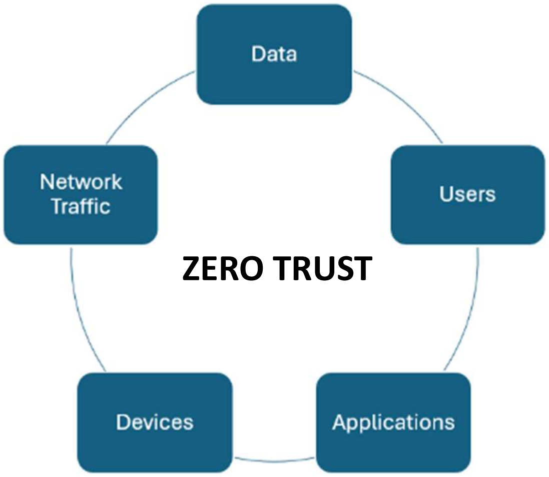
The industry has a few key playbooks to guide the way, like the TSA Pipeline Security Guideline, NIST SP 800-82 (Guide to Operational Technology Security), CSA Z246.1-17 (Security Management for Petroleum and Natural Gas Industry Systems), and the ISA/IEC 62443 standards. These documents set the bar for what it takes to keep systems secure, offering best practices and benchmarks for assessing how well you are doing. Instead of going deep into each, I will highlight the key pillars and encourage you to dig into the standards themselves if you are looking for more detail.

Zero Trust Architecture

Zero Trust is not just a buzzword—it is a game-changer for cybersecurity in oil & gas. The idea is simple but powerful: trust no one and verify everything, whether they are inside or outside your network. It is about making sure every access request is scrutinized before you open the door. For oil & gas, this means strict identity checks, multi-factor authentication (MFA), and giving people the least amount of access they need to get their job done. Zero Trust shines when it comes to high-stakes environments like control systems, refineries, and pipelines, where even a small breach can lead to big problems.

Network Segmentation and Access Control

Think of network segmentation as building firebreaks in a forest. The objective is to create separate zones within your network so that if a fire starts in one area, it cannot easily spread to others. For oil & gas, that means keeping OT systems isolated from the broader corporate IT network. This approach minimizes the damage if a breach does occur, stopping attackers from roaming freely across systems. And with role-based access control (RBAC), you can make sure that people only have access to what they actually need based on their role, with regular reviews to tighten things up as needed.



Incident Response

We all hope for the best, but in cybersecurity, you have got to plan for the worst—because when a breach happens, it is often fast, disruptive, and costly. That is where a strong and well-rehearsed incident response plan comes into play. In a sector as interconnected as oil & gas, a cyber incident can lead to not just financial losses but also costly downtime, operational chaos, regulatory fines, reputational damage, or even physical harm. A well-structured response plan defines roles, establishes a clear communication flow, and outlines decisive actions for containment and mitigation when things go south. But a plan is only as good as its execution, which means companies need to run regular drills—simulated cyberattacks, red-team exercises, and crisis response training—to keep teams sharp and ready. Without constant testing and updates, response plans quickly become obsolete, leaving companies exposed to evolving threats.

Further, considering the accelerating impact of climate change, companies must enhance their ability to respond to crises—both cyber and environmental. For the upstream sector of the oil & gas industry in Canada, forest fires in remote areas have become an increasing concern, posing serious risks to personnel and infrastructure. As climate-related events grow in frequency and severity, organizations must develop integrated incident response capabilities, ensuring resilience through proactive planning, resource allocation, and cross-sector collaboration. Effective crisis response is no longer optional—it is essential for safeguarding infrastructure, operations, and the communities they serve.

Supply Chain Security and Vendor Risk Management

The oil & gas supply chain is an intricate web, linking equipment manufacturers, software providers, subcontractors, and service vendors—each a potential entry point for cyber attackers. Breaches often originate from compromised third-party vendors, escalating into full-scale security incidents that disrupt entire operations. Attackers are increasingly targeting supply chains, exploiting indirect access through trusted partners rather than launching direct attacks.

To manage this risk, oil & gas companies must implement robust vendor risk management programs that go beyond basic compliance. This includes rigorous security assessments, real-time monitoring, and strict security requirements for suppliers. Many major cyberattacks in recent years have not just stemmed from outdated systems but from compromised third-party products before deployment. These incidents highlight the urgency of ensuring vendors follow “secure by design” principles, proactively mitigating risks and complying with industry standards. Strengthening supply chain resilience and enforcing strict security oversight is critical to minimizing cascading breaches and ensuring operational integrity in an increasingly complex threat landscape.

Securing IT/OT Integration

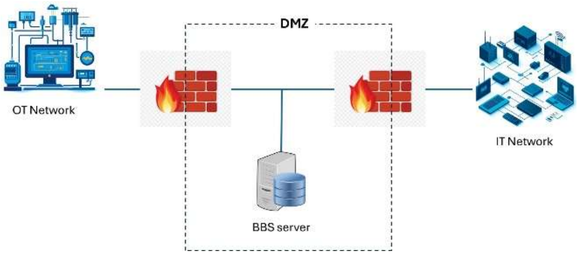
One of the toughest challenges the oil & gas industry faces today is integrating IT and OT systems securely. For years, these two environments lived in their own worlds—OT systems running the physical processes like drilling and pipelines, while IT systems managed data and communications. But the push for digital transformation has brought these worlds together, and with it, a whole new set of vulnerabilities. Now, a cyberattack targeting the IT side can ripple over and impact physical operations, creating serious security risks.

Securing this integration goes beyond basic network segmentation—it requires a high level of assurance to truly shield OT systems from IT networks. Easier said than done! NIST, CSA, and TSA guidelines call for network isolation but offer limited detail on how to achieve it. That is why this white paper dives into practical solutions to bridge that gap.

Files Transferred to the OT Network

One of the Achilles' heels of the oil & gas industry is transferring data from the IT network to the OT network. These file transfers can carry hidden risks, such as zero-day malware that can compromise OT systems, leading to disruptions or safety risks. To mitigate this, I propose to use a secure intermediary based on the old Bulletin Board System (BBS) concept[1] to ensure proper isolation between IT and OT networks. This approach allows for thorough scanning and validation of files before they reach critical OT systems, adding an extra layer of security to the data transfer process. Here is how to make it work:

- **BBS Server as an Intermediary:** Think of the BBS server as a fortified, neutral zone that sits between the IT and OT networks, usually within a Demilitarized Zone (DMZ). Authorized users or systems can upload files from the IT side, while the OT side retrieves them later without any direct connection between the two. This setup keeps the networks separate and minimizes the risk of cross-contamination.



- **Secure File Transfer Protocols:** It is essential that every file sent to or retrieved from the BBS server is protected in transit. That is why the BBS server should enforce secure transfer protocols like SFTP (Secure File Transfer Protocol) or FTPS (File Transfer Protocol Secure). This way, no one can tamper with or intercept the data while it is on the move.
- **Digital Signatures and Validation:** Before files hit the BBS server, they should be digitally signed. This guarantees their authenticity and integrity when the OT systems pick them up. The BBS server can then validate these signatures to ensure nothing has been altered along the way.
- **Malware Scanning and Validation:** To add another layer of defense, the BBS server should have malware scanning tools—like an EDR (Endpoint Detection and Response) solution—checking each file before it is made available for download. This ensures that any hidden threats are neutralized before they can reach the OT network.

- **Controlled Access and Authentication:** Not everyone should have access to this system. Only a select few, properly authorized users, can upload or retrieve files. Further, access to the BBS should require MFA, making sure only trusted personnel can get in.
- **Automated File Retrieval:** On the OT side, we can automate the process by using a scheduled script (such as PowerShell) to periodically check the BBS server (ex., every 5 minutes) for new files and forward them to the appropriate recipient. This setup ensures updates happen promptly and securely without the need for manual intervention.
- **Activity Logging and Auditing:** Every action on the BBS server should be logged and audited—from who posted or downloaded a file to the time and nature of the actions taken. These logs create a detailed trail, ensuring compliance and making it easier to trace any issues that might arise.

Remote Access to the OT Network

Sometimes, technicians need to access a site remotely to deal with specific issues. But here is the challenge: those external access points into the OT network are a prime target for cybercriminals. That is why we cannot afford to cut corners on security. Here is how to tighten things up:

- **CITRIX Connection via DMZ:** Any external access should be routed through a CITRIX connection, but not directly into the OT network. Instead, it goes through a DMZ that is set up to restrict access only to authorized users and trusted devices and create a log of activities. Further, to ensure that the security measures of the previous section are not bypassed, the CITRIX setup must prevent any attempts at file transfers.
- **Restricted Protocols:** The DMZ should only allow communication protocols that are absolutely necessary to access the OT network. By keeping unnecessary protocols out, you minimize the potential avenues for an attacker to exploit.
- **Hardened Devices:** Only company-hardened computers should be allowed to access the OT environment remotely, and these machines need to be equipped with EDR (Endpoint Detection and Response) solutions and application whitelisting. This means only authorized, digitally signed software can run on those devices.
- **Multi-factor Authentication:** Every connection to the OT network must be secured with MFA.
- **Detailed Monitoring and Logging:** Comprehensive logging and continuous monitoring of all traffic between the networks can help you spot anomalies early and give you a clear audit trail if something goes wrong.

Remote Dial-Up

In certain cases, having a permanent TCP/IP network connectivity to a remote site is not possible, which is why many oil & gas companies rely on the use of wireline dial-up modems, many of them configured with passwords that are never changed. While there are still many dial-up modems in use, companies rely more and more on cellular routers and even satellite terminals (ex., via StarLink) for remote sites.

- **Wireline Dial-Up Modems:** As a general rule, you should use dial-up modems designed to work in a NERC-compliant[2] environment, as they offer the required security protection: data encryption, MFA, and call control filtering to restrict connection with pre-authorized callers.

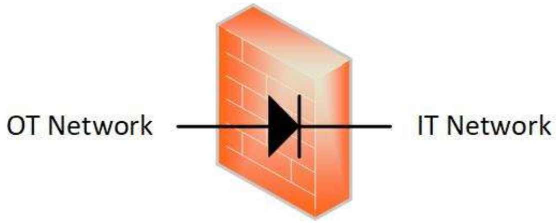
> *“Use dial-up modems designed to work in a NERC compliant environment.”*

- **Cellular Routers.** As a minimum, these devices should have the following built-in security features: IPSEC Virtual Private Network (VPN) data encryption, firewall, intrusion detection and MFA.
- **Satellite Terminals:** As a minimum, the following security features should be enabled on these devices: a secure boot process that ensures only authorized firmware can run on the device, VPN data encryption, firewall, and MFA.

Data Diodes

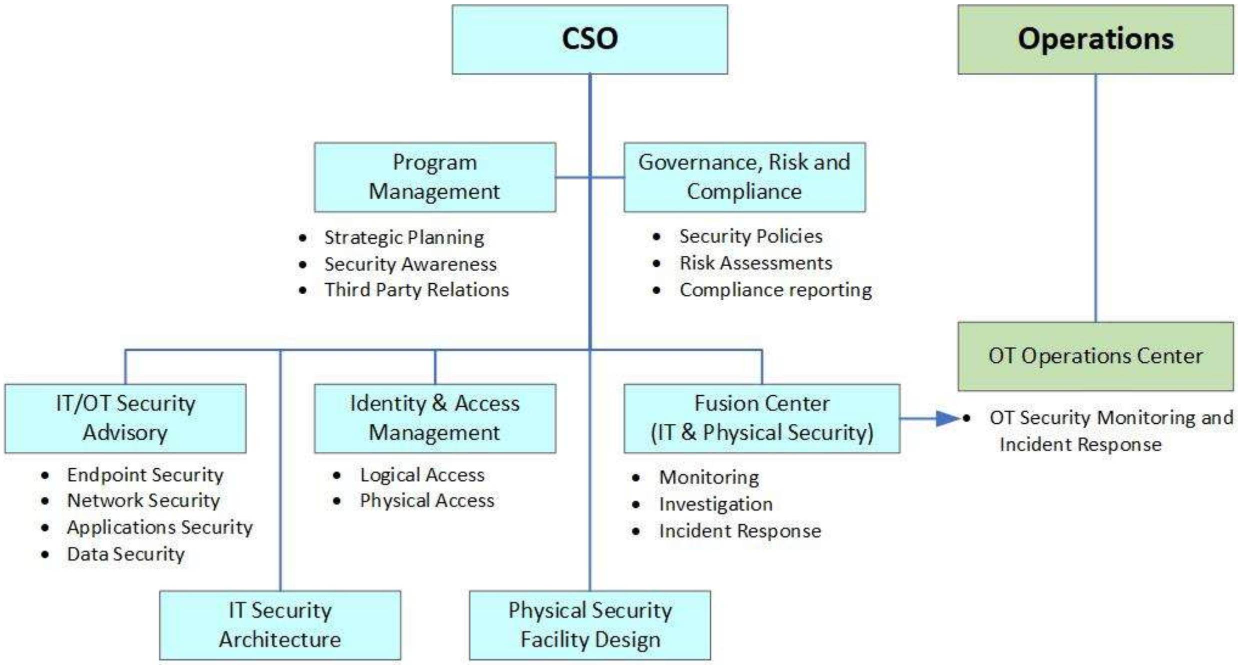
In many industries, including oil & gas, power generation, and manufacturing, OT systems manage critical physical processes. These processes generate valuable data related to system performance, equipment status, production output, and environmental conditions. This data often needs to be transferred to the IT network (or the cloud), for several reasons, including data analysis optimization, Enterprise Resource Planning (ERP), billing, compliance reporting, etc.

A data diode is a specialized security device designed to ensure that data flows in only one direction, making it a critical tool for protecting OT environments from external threats. Unlike software-based solutions, which can be vulnerable to malware or manipulation, true data diodes are entirely hardware-based, providing a robust and tamper-resistant barrier. This hardware-driven design ensures that no data or commands can flow back into the OT network, eliminating the risk of information leakage or attacks propagating in reverse.



With no software to override or manipulate, data diodes offer a high level of assurance that communication between the IT and OT networks remains one-way, significantly reducing the attack surface. They are particularly valuable in industries like oil & gas, where even a small breach could have severe safety, environmental, and financial consequences. By using data diodes, organizations can safely transfer operational data for analysis and reporting while maintaining the strict isolation of their most critical systems, ensuring compliance with industry regulations and maintaining operational integrity.

Governance



Although most oil & gas companies have access to substantial budgets and resources to secure their IT, OT, and physical infrastructure, security breaches continue to occur. In many cases, the root cause lies not in the lack of investment but in a weak security governance model. Often, IT, OT, and physical security teams operate in silos, with each focusing on their own domain, leading to fragmented efforts and communication gaps. These silos create blind spots across the security landscape, leaving the organization vulnerable to threats that span multiple domains.

Throughout my career as a CSO in the private sector, I have seen firsthand the impact of effective security governance. While I could easily dedicate an entire book to reviewing the various governance models and their strengths and weaknesses, in this white paper I have opted to focus on a model that has consistently proven its value over the years. This approach centers on a unified security governance framework that seamlessly integrates IT, OT, and physical security. By breaking down silos and fostering collaboration across all security domains, this model not only enhances the overall effectiveness of the security program but also provides senior leadership with a clear point of accountability—what they often refer to as "one throat to choke" on all security-related matters, something leadership particularly values in terms of clarity, responsibility… and budget management.

The organizational chart above outlines the key functions within a unified Security organization. While the number of personnel required will vary depending on the size and complexity of the organization, all the listed functions are essential and need to be done. In larger organizations, a dedicated team may be needed to fulfill each role, while in smaller environments, individuals may need to wear several hats and take on multiple responsibilities. Here is a short description of each function:

Chief Security Officer

The CSO, typically reporting to the Chief Risk Officer or Chief Executive Officer, is responsible for managing all security risks across IT, OT, and physical domains. The CSO is accountable for safeguarding hardware, software, networks, data, and the physical facilities where these assets are kept, ensuring comprehensive protection throughout the organization.

Program Management

This function oversees the overall security strategy, balancing the organization's risk tolerance, regulatory compliance, operational requirements, and budgetary constraints. It also manages the security awareness program and contractual relationships with third-party providers, such as security guard companies, executive protection services, and security equipment maintenance.

Governance, Risk, and Compliance (GRC)

This team is responsible for drafting IT, OT, and physical security policies in collaboration with relevant stakeholders. Once approved, they oversee audits to monitor compliance with both internal policies and external government regulations. The outcomes of these audits are regularly presented to the regulators and Leadership Team as part of regular security risk assessments.

IT/OT Security Advisory

A multidisciplinary team handles this function, ensuring that the appropriate security requirements are established for new IT and OT systems. They are responsible for performing certifications and accreditations before releasing new systems, or after major upgrades and changes to ensure that all security protocols are followed.

IT Security Architecture

Senior security architects manage this function by creating and maintaining the IT security roadmap. Their work ensures the organization stays ahead of evolving cyber threats while integrating new solutions to meet both technological advancements and the company's operational needs.

Identity and Access Management (IAM)

IAM oversees the entire lifecycle of user identities and access control, whether they are employees or contractors. This includes managing logical access, such as user IDs, passwords, and MFA, as well as physical access, including badges, keys, and padlocks, ensuring secure and appropriate access for personnel.

Physical Security Facility Design

In collaboration with the real estate and facilities teams, this function establishes physical security specifications during the design phase of new buildings and sites, aligning physical security measures with the level of criticality and threat exposure. Additionally, they conduct periodic physical security audits to ensure ongoing protection.

Fusion Center (IT/Physical Security)

The Fusion Center provides 24/7 security monitoring, investigation, and response for IT infrastructure and physical facilities, including alarms, CCTV cameras, and access control systems. But what about OT security monitoring and incident response? Given the increasing cyber threats targeting operational technology, ensuring effective OT security oversight is critical. There are three potential approaches to consider:

- **Dedicated OT Security Center:** This option involves establishing a separate, OT-focused security center dedicated solely to monitoring and responding to OT threats. While it offers specialization, it comes with high costs and lacks operational synergy with the OT team—an essential factor for ensuring an efficient response. The isolated nature of this setup can also hinder coordination, particularly in major incidents that require cross-functional collaboration.
- **Integration with the Fusion Center:** This approach centralizes security monitoring by integrating OT security within the existing Fusion Center. While it may seem like a logical choice, it requires routing all OT monitoring and incident response traffic through the DMZ, which can compromise network segmentation between IT and OT. Maintaining strict separation between these environments is a fundamental security principle, and weakening this isolation increases risk. Additionally, the physical and operational distance from the OT team can lead to delays in handling false alarms or responding effectively to complex OT-specific threats.
- **Integration with the OT Operations Center:** A more cost-effective and operationally efficient solution is to integrate OT security monitoring within the existing OT Operations Center, which already operates around the clock. By adding dedicated cybersecurity resources to handle traffic monitoring and incident response, this setup enhances collaboration between cybersecurity and OT personnel. These security professionals remain part of the CSO's organization but gain valuable real-time insights by working directly with the OT team. This close coordination significantly improves response times, reduces miscommunication, and ensures a more effective, informed, and context-aware incident management process.

Conclusion

The oil & gas industry is at a crossroads, facing unprecedented cybersecurity challenges as it embraces digital transformation. The integration of IT and OT systems has introduced new complexities and vulnerabilities, making it essential for companies to adopt a proactive and comprehensive approach to securing their infrastructure. While the industry has made significant strides in increasing operational efficiency through technology, this progress has come with a price—the heightened risk of cyberattacks that can disrupt operations, cause financial damage, and threaten the safety of personnel and the environment.

Throughout this white paper, we have examined the distinct cybersecurity risks faced by the upstream, midstream, and downstream sectors of the oil & gas industry. From securing remote production sites and safeguarding critical pipelines to protecting refineries and retail networks, the challenges are multifaceted and require tailored solutions. Recent incidents have served as stark reminders of the vulnerabilities within this sector, underscoring the urgent need for more robust defenses.

The key to addressing these risks lies in a unified security strategy that integrates IT, OT, and physical security under a cohesive governance model. By implementing advanced cybersecurity practices such as Zero Trust Architecture, network segmentation, and strong incident response plans, companies can enhance their resilience against evolving threats. Additionally, securing IT/OT integration, protecting supply chains, and leveraging emerging technologies will be critical to safeguarding operations in the future.

> “*As the oil & gas industry continues to evolve, the companies that will thrive are those that prioritize security as a foundational element of their digital transformation.*”

As the oil & gas industry continues to evolve, the companies that will thrive are those that prioritize security as a foundational element of their digital transformation. With the right governance, strategies, and technologies in place, the industry can protect its critical infrastructure, maintain operational continuity, and ensure a secure future in an increasingly connected world.

References

[1] What is Bulletin Board System? Geeks for Geeks. https://www.geeksforgeeks.org/what-is-bulletin-board-system/. 2024

[2] North American Reliability Corporation (NERC) https://www.nerc.com/pa/comp/Pages/default.aspx

About the Author

Gaétan Houle is the Canadian Enterprise CISO at Fortinet. He is a seasoned security professional with over 35 years of experience specializing in the protection of IT and OT systems for both the public sector and major corporations. Throughout his career, he has served as a Chief Security Officer (CSO) for several large organizations in North America and Europe, gaining extensive expertise in all aspects of security.

He can be reached at: ghoule@fortinet.com

This document was originally published by the author through GH Inc. It has been updated and rebranded under Fortinet with his permission.

February 6, 2025

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.