2nd. International Conference on
INNOVATION in Science & Technology
15 December 2016 Singapore www.2istconf.com
istconf

Cyber Security For Petroleum Industry

Mehdi Foroozanfar

PhD Candidate in Petroleum Engineering at University of Tehran

m.foroozanfar@ut.ac.ir

Abstract

Countries are not addicted to oil , “but their industries are.” This pithy assessment underscores the modern world’s dependence on oil and illustrates why the industry’s security is critical to the security of every nation. From military aggression to cyber threats, the oil and gas sector is a high profile target for adversaries intent on disrupting production, intercepting sensitive data, and crippling national and global economies.

Keywords : Oil , Security , Threat , Data , Economy

Introduction

Past attacks against the oil industry have proved the value of risk management and risk based security policies for stakeholders. As a critical infrastructure, the oil and gas industry faces additional risks beyond those in many organizations. In addition to the intellectual property that any company must protect in its corporate Risk Management Framework, threats to the oil and gas infrastructure also put at risk the physical wellbeing of people and the environment as well as the national security. Losing intellectual property through a security breach can damage a company's revenue stream, but the damage caused by a major industry disaster such as the Deepwater Horizon spill, or the blow-out of the Ixtoc I exploratory well in the Bay of Campeche on June 3, 1979, which resulted in the release of about 475,000 metric tons of oil to the waters of the Gulf of Mexico, endangers lives, local environments and even global economies.

Exacerbating the challenges of securing its infrastructure, the industry faces the dangers of dealing with a combustible element in extreme conditions and often in remote locations. In addition to the difficulties of operating in harsh environments, complex socio-political events make the process of finding, transporting, refining and distributing oil and natural gas a high-risk endeavor.

The major Independent Oil Companies (IOCs) have responded to these risks with Health, Safety and Environment (HSE) standards and management systems, an operational keystone to safeguard the wellbeing of companies, employees, the public and the environment, whether upstream, midstream or downstream in the exploration, extraction and refinement processes. The management systems determine how companies identify and mitigate HSE risks throughout their operations, covering everything from basic safety requirements such as holding the handrails when climbing or descending stairs, to managing major accident hazards that could destroy facilities.

Understanding the Adversary

Unfortunately, there is no single adversary and no single threat to the information technology (IT) and operational technology (OT) infrastructures of the oil and gas industry, and no silver bullet for security. Attackers run the gamut from unsophisticated script kiddies through hacktivists and cybercriminals to terrorists and state-sponsored hackers, each with their own skillsets, toolkits and motives. Although the differing motives notoriety, money, business advantage or military superiority can to an extent determine the targets of each category, the interconnected nature of our world means that any organization could find itself a target of any of these attackers.

This means an organization should be prepared to protect itself from the full range of threat actors. This is a daunting task, but it is simplified somewhat by the concept of risk based security. While hackers with relatively low levels of skill, motivation and resources present a smaller risk than well financed, highly motivated and more sophisticated criminals and state-sponsored groups, the risk an organization faces also depends on the maturity of its security, the criticality of its infrastructure and the impact of a breach, and the vulnerabilities present. Defenses should be planned accordingly.

Although firewalls and traditional signature based antivirus no longer are adequate to protect your infrastructure, they still are valuable tools for eliminating a broad swath of low level opportunistic attacks, leaving intelligent security tools and the human beings behind them to deal with the more serious risk of targeted attacks from sophisticated attackers.

Figure 1 . Understanding the Adversary

Current State of Cybersecurity

According to a study by Frost & Sullivan, “Global Oil and Gas Infrastructure Security Market Assessment,” the total oil and gas infrastructure security market is predicted to increase from $18 billion dollars a year in 2011 to $31 billion dollars by 2021.

Despite this spending, the ABI Research study describes the Process Control Networks (PCN) in many oil and gas companies as “poorly protected against cyber threats… at best, they are secured with IT solutions which are ill-adapted to legacy control systems such as PCN.”

One of the drivers for increased spending on cybersecurity is the increasing costs to a company of a breach. A recent study on the cost of data breach incidents for companies in the United States by the Ponemon Institute shows that the costs of a data breach have increased across the board from 2013. The average cost for each lost or stolen record containing sensitive and confidential information rose from $188 to $201. The total average cost paid by organizations per breach increased from $5.4 million to $5.9 million. But just as significant is the impact of a breach of operating technology (OT) systems, which can not only expose data but also disrupt operations, damage equipment and physical facilities, and endanger the lives and safety of people. This could be far more damaging and costly.

The increase in the number of cyberattacks combined with the increasing costs of a breach ramp up the risks for oil and gas companies, especially the risks from complex, highly targeted attacks against the industry’s high-profile, high-value infrastructure and intellectual property.

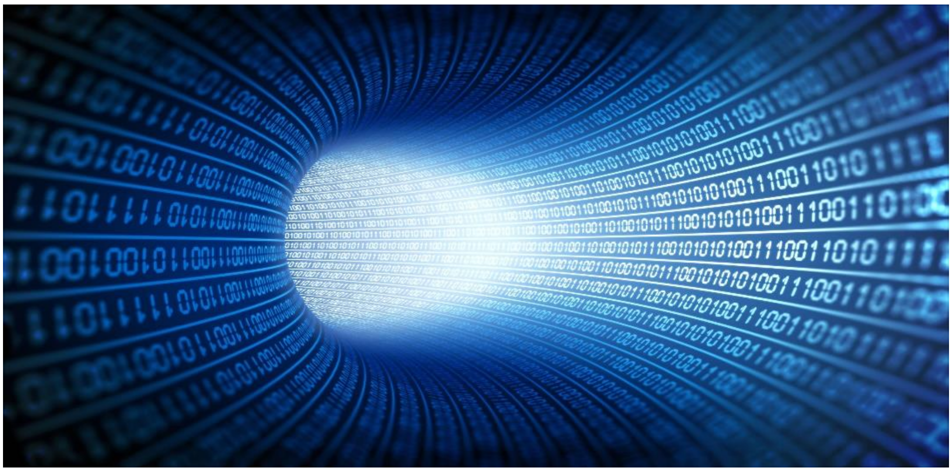

Figure 2. Cyber Attack

Operational Technology Systems

The Operational Technology (OT) systems that oversee the volume, velocity, location and other vital activities in the production and distribution of oil and gas not only produce a wealth of sensitive and proprietary information, they are essential to the economic health and physical safety of the company, its facilities and its people.

Although there is not a single term generally agreed-upon in the industry, there are substantial differences between the mission and the nature of the equipment that makes up OT systems and Information Technology (IT), but with the growing use of remote access for OT systems, the two electronic infrastructures are becoming interconnected. This interconnection of disparate systems presents special challenges in protecting the data they contain, the equipment they control, and the systems themselves.

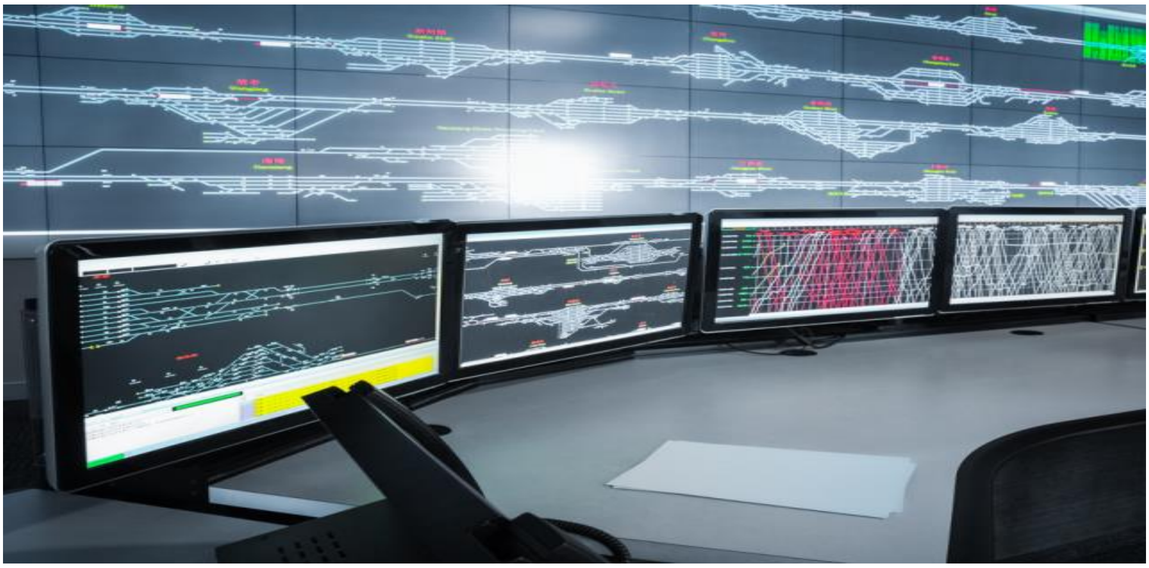

Figure 3. Operational Technology Systems

Unlike IT equipment and software, which can be deployed to perform a range of tasks and can be frequently updated and upgraded, OT is typically intended to perform one task, and reliability and safety are its primary attributes. An OT system simply has to work over extended lifecycles. This puts a premium on stability and minimizes the opportunity for upgrades.

The Value of Operational Technology(OT) Systems

Access to data is crucial to the oil and gas value chain. Proprietary data is used in finding new petroleum reserves, and operational data from equipment reduces the non-productive time of assets by supporting predictive maintenance of critical components in the extraction, refinement and distribution of products. Technology, both operational and information, also helps enable compliance with Health, Safety and Environment management standards. Technology also can help improve asset performance management by producing real-time metrics across different subsystems.

This operational data and intellectual property provide the competitive advantage that sets each company apart in a highly-integrated industry. It also helps companies better understand the current environment and plan for the future. But because OT systems work with physical equipment and processes, the security of these systems is critical for continuing operations and human safety as well as for the protection of data.

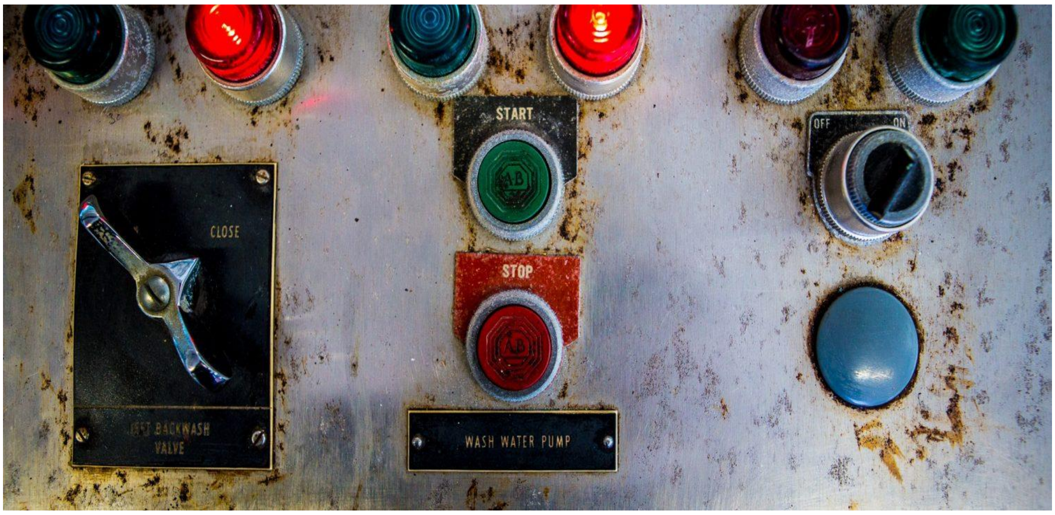

Figure 4 . Operation System

Many of the differences between the two types of systems are defined by the differences between “safety” and “security.” Although these two concepts are related, they have fundamentally different requirements. Security refers to the protection of the technology systems and the information they contain; the ability to ensure availability, integrity and confidentiality. Safety refers to the physical wellbeing of people, equipment and the environment; preventing injury and damage to people and things. Because safety traditionally has been the imperative for OT systems, and safety depends largely on the stability of the systems, cybersecurity has been a secondary consideration for OT systems, if it has been considered at all.

The Threat to Petroleum Industry

The challenges created by the integration of IT and OT for any organization are further exacerbated in the oil and gas industry by two major issues.

First there is greater integration in the value chain than in many other industries. The oil sector is an ecosystem composed of upstream, midstream and downstream companies and organizations engaged in different aspects of the business, which complicates the security landscape. This environment includes independent oil companies, state-owned oil companies, smaller companies that focus on only certain streams, and armies of service providers and other third parties. This integration provides a ripe environment for security gaps and multiple points of entry.

The integration of these organizations can create ripple effects when a disruption such as a spill, an attack, or a socio-political event occurs.

Secondly there are newer technologies coming into the industry at a rapid pace. Adding to the complexities of a highly-integrated industry already dealing with integrated IT and OT systems are the new technologies on the horizon that could further complicate the job of the CIO(Confidentiality Integrity Operational) and CISO(Confidentiality Integrity Security Operation) responsible for ensuring the security of the enterprise. Digital oil fields connected to cloud platforms running big data analytics, the use of drones in upstream oil and gas to run surveys or monitor for environmental issues, and third-party companies hosting 3D modeling for well and field planning are a few of the new technologies entering the industry that could create additional vulnerabilities.

As a result of these vulnerabilities there is a need to adequately budget for both IT and OT network security as well as for the security of the data they contain. There is no getting around the fact that managing and protecting both the physical and cyber assets of any large organization is always a challenging proposition; and within the energy industry the challenges can be even greater than in other sectors. The oil and gas infrastructure is geographically dispersed and it includes remote stations and legacy operational technology with differing capabilities that is being integrated into the IT infrastructure. These factors combine to create a large attack surface for critical assets where continuous operation is required. Defending this environment requires extending cybersecurity to the entre enterprise.

Cybersecurity and Health , Safety and Environment

Implementing effective cybersecurity across both the information and operational domains should be a collaborative effort, involving all stakeholders. The discussion shouldn’t be about IT or OT, but rather IT and OT. The integration of the two technologies, with tightly controlled bi-directional data flow and remote access from the IT domain, is taking place, but the goals and capabilities in each domain remain distinct. These differences must be taken into account when establishing policies, procedures and controls for each.

In a report on IT and OT integration, Gartner cited the Oil and Gas industry as an industry sector in which the convergence is having an impact, and said that the relationship between the technologies needs to be better managed and that managers need a better understanding of how OT is changing so that the two can be better aligned.

The Health, Safety and Environment (HSE) management standards, a set of practices for tracking and mitigating the risks and dangers faced by workers in their day-to-day activities, have helped to improve safety in the industry. HSE is the product of a process that includes not only the physical environment and policy, but human behavior.

The lesson in the evolution of safety standards, which parallels developments in cybersecurity, is the need to address challenges through solutions that encompass people, processes and technology, in parallel to achieve improvements in security at a far faster pace than was achieved in safety. By adding this level of rigor, oil and gas companies are able to measure and mitigate the level of safety risk that their employees and local communities are subject to now, and predict those risks for the near future.

This comprehensive approach can be effective with cybersecurity in the struggle to address the vulnerabilities of integrating IT and OT. It requires not only effective policies and technical controls, but the active participation of workers to track incidents and behavior in order to effectively identify and mitigate risks. By adopting the HSE model to standardize cybersecurity activities to track near misses (such as a worker being stopped before plugging an unscanned USB device into a computer), incidents (such as an attempted breach or a breach without loss of data or with no operational impact) and losses (the loss or compromise of data or equipment), organizations can mitigate risks and reduce the vulnerabilities introduced by the integration of IT and OT.

The combination of malicious activity, human error and technical failures that are responsible for data breaches points to the need to treat cyber incidents with the same broad level of scrutiny as the oil and gas sector uses in its approach to Health, Safety and Environment.

Although compliance with regulation and industry best practice is a complicated process, successfully implementing a security program that provides both security and compliance can be accomplished by breaking down the challenges into steps and pairing talented people with the tools and processes they need to accomplish their jobs in a complex environment.

Criterion For Cybersecurity

There is little direct regulation of cybersecurity in the oil and gas sector, but there is a body of standards and best practices from both industry and government to help companies ensure that their policies and status meet their needs for securing their own infrastructures and data. They also ensure that companies are able to meet the needs and expectations of partners and customers. While these are guidelines voluntary and not mandatory a company that ignores cybersecurity policies and procedures that have become recognized as best practices in the industry could find itself not only at greater risk to cyber threats, but also a threat to the rest of the ecosystem in which it operates.

The industry has not hesitated to adopt best practices in other areas of operation. ConocoPhillips held a workshop on best practices in environment and sustainable development in 2014, and Exxon Mobil and Chevron have conducted studies that show that use of best practices in production can produce gains in efficiency of up to 30 percent. But cybersecurity, especially in the operational domain using process control systems, has not received the same level of attention that environmental safety and productivity have received.

Although the oil and gas sector is unique and faces distinct challenges, there also is much that it shares with other enterprises that are operating Information Technology (IT) and Operational Technology (OT) networks. This means that the basics of cybersecurity apply, and there is plenty of guidance available on implementing the basics.

Figure 5. Oil and Gas Infrastructure

Security Controls

1. Inventory of Authorized and Unauthorized Devices .
2. Inventory of Authorized and Unauthorized Software .
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers .
4. Continuous Vulnerability Assessment and Remediation .
5. Malware Defenses .
6. Application Software Security .
7. Wireless Access Control .
8. Data Recovery Capability .
9. Security Skills Assessment and Appropriate Training to Fill Gaps .
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.

Companies have different needs and are at different levels in the maturity of their security programs, and so will have different paths to their desired end state. Unfortunately, awareness of the critical nature of cybersecurity often is lacking in the industry, particularly regarding Operational Technology systems, which can include industrial and process control systems (ICS and PCS), Distribution Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. Spending on OT system security too often is viewed as a cost rather than an investment. Safety budgets used to be seen this way in the oil and gas industry, but that has changed. Companies now realize that being safe is good business as well as a regulatory requirement. Recognition of the need for security in operational technology systems is now rapidly growing through the industry and is catching up to the acceptance of safety in industrial systems.

As Conclusion ; Steps for Implementing Security

Lockheed Martin's Process Control Security Team provides professional services to help organizations along the path to better security. Each path is different and the specific process will differ from one company to another, but there is an orderly set of steps that the team uses to help apply the lessons learned across numerous environments to provide recommendations to help accelerate the specific security objectives.

Raise awareness and achieve stakeholder buy-in: This is not necessary for everyone; some companies are keenly aware of the need for securing process control systems. But more often some education on the issue is required, especially to include all stakeholders, to attain the strategic direction and funding in the context of the day-to-day operations.

Situational review: The next step is a high-level review of the organization's current level of security. This often can be done quickly, producing an overview of the company's security posture. In most cases the findings show that there still needs to be more focus on the basics of security. Companies need to begin with core activities including having security policies and plans in place, having an up-to-date inventory of control systems, identifying critical systems, identifying the risks to these systems, assessing the level of impact of an incident compromising each system, and providing security training for personnel.

Detailed assessment: Once priorities have been established, a more in-depth look at the security situation can be done to help get proper policies into place and assess compliance with them. This can include a survey of the infrastructure, the security controls and procedures being used, an assessment of vulnerabilities and the impact of their exploitation.

This assessment can identify the gaps between the organization's present state of security and the desired end state, and allow for planning on how to address those gaps. Not all gaps in security plans can be eliminated.

Implementation: With priorities and gaps identified, technology can be put into place along with the people and processes that will be responsible for security. Security training is an organization wide effort that should include not only security officials, but all employees so that they know their roles and responsibilities in ensuring the security of the organization's systems.
Automaton is a key factor in effective security, speeding responses and freeing humans from routine manual tasks to focus on more critical analysis. But there are practical limits to the degree and types of automaton that are practical in the control system environment.

References

[1]. Wadsworth, Andrew. Holcomb , Jason. “Definitive Guide to Cybersecurity for the Oil and Gas Industry” ,2015 .
[2]. Hackers' Favorite Target: Big Oil and All That Deadly Equipment .
[3]. The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems .
[4]. Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised .
[5]. Internet attack could shut down US gas stations .

[6]. Oil and Gas Production Handbook .
[7]. Burner Management System SIMATIC BMS400F .
[8]. Burner Management System (BMS) - Safety Solution for the Power Generation Industry .