Definitive Guide to Cybersecurity for the Oil & Gas Industry

AN EBOOK PRESENTED BY LEIDOS

leidos

Table of Contents

leidos

Introduction

Energy specialist and former CIA Director James Woolsey famously proclaimed that Americans aren't addicted to oil, "but their cars 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.

Past attacks against this industry have proved the value of risk management and riskbased 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.

Few other industries triage and escalate near-miss safety and security incidents in order to predict incidents with the same thoroughness as the oil and gas industry through its HSE management systems. 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.

But in addition to the traditional physical and operational risks faced by the industry, the oil and gas sector also is susceptible to the escalating risk of cyber-attacks that threaten other companies, organizations and government agencies worldwide.

Statistics on cyber-attacks vary depending upon the source, but all agree that they are increasing. According to a recent **Symantec study** there was a 91 percent increase in targeted attack campaigns in 2013 over the previous year, which includes a 62 percent increase in the number of breaches. According to the same report, one in 392 emails contained phishing attacks and web-based attacks were up 23 percent over a similar time the previous year. A report from **IBM** stated that in the United States alone it monitored an estimated 1.5 million cyber-attacks in 2013. That equates to roughly a 12 percent year-to-year increase in security events from the previous year.

Regardless of the numbers, two common trends in cybersecurity are clear:

- Cyber-attacks continue to increase
- The attacks are becoming more destructive and the impact of the attacks is increasing

One of the best-known attacks against the oil and gas industry was the Saudi Aramco attack of 2012, claimed by the hacker organization calling itself the Cutting Sword of Justice. The attack, aimed at stopping oil and gas production by Saudi Arabia's largest exporter, eerily resembled the more recent Sony Pictures attack in which hackers gained access to millions of proprietary records and where successful in crippling the infrastructure of the targeted organization. But even more importantly, the Saudi Aramco attack effectively destroyed the hard drives of 30,000 computers, one of the first— if not the first—cyberattacks to actually damage computers on a wholesale scale and highlighting the industry's vulnerability.

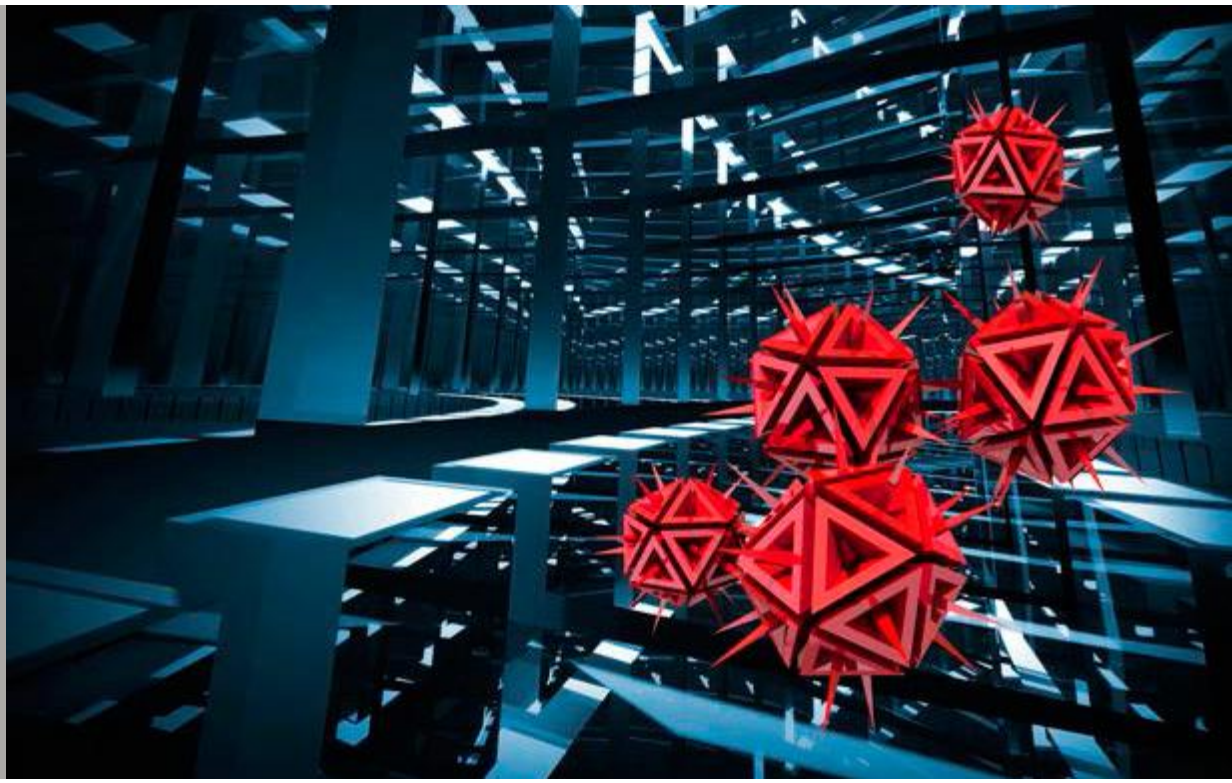
Disruptions caused by the attack echoed through Saudi Aramco for months, highlighting the importance of Business Continuity Planning (BCP) for cyberattacks as well as for natural and other manmade disasters. Could your organization continue to operate on paper if your desktop computers suddenly became useless? How long would it take to procure and install thousands of new hard drives to repair the damage to your systems? Do you know where those drives would come from? Would your employees know how to get their jobs done in the meantime?

Too often, these and other critical questions are not raised until after the fact or they are addressed only in outdated "shelfware," slowing recovery and degrading operations.

In some respects Saudi Aramco was fortunate— the 2012 attack damaged 32-bit machines, leaving the 64-bit servers intact. The attack on RasGas Company Limited, just two weeks later, included an improved variant of the Aramco virus that infected both 32- and 64-bit machines, making the damage more widespread.

This second attack demonstrated the speed with which motivated attackers can respond and adapt; and it illustrates not only the need for the oil and gas industry to quickly respond and adapt to events, but also the need to anticipate them through a risk-based security program that identifies risks in advance, eliminates or mitigates them where possible and practical, and prepare to deal with those risks that remain. And plans need to be in place in the event of a breach for recovery and a return to normal operations as quickly and efficiently as possible.

Understanding the Enemy



1. Current State of Cybersecurity
2. The Advanced Persistent Threat

leidos

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 riskbased 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.

CURRENT STATE OF CYBERSECURITY

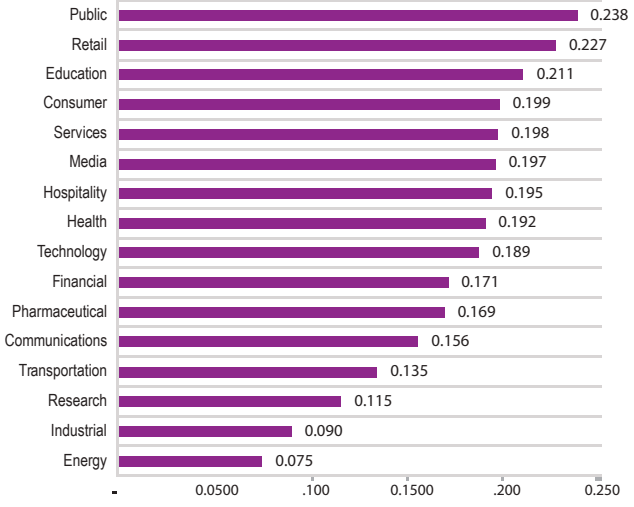
According to a study by Frost & Sullivan, "**Global Oil and Gas Infrastructure Security Market Assessment**," the total oil and gas infrastructure security market is predicted to increase from $18 billion dollars a year in 2011 to $31 billion dollars by 2021.

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 illadapted 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 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.

Costs of data breaches vary by industry (Figure 1). Heavily regulated industries including energy, healthcare, transportation, education, financial services, communications, and pharmaceuticals have higher costs, and the energy sector's $237 per record is significantly above the $201 average. Figures for the cost of cyber attacks against OT are hard to come by. Simple production shut-downs can cost millions in lost production. Attacks such as Stuxnet in Iran and the damage to a German steel making furnace reported in December 2014 show that equipment controlled by OT can be damaged with costs running to many millions of dollars.

Figure 1. Probability of a data breach involving a minimum of 10,000 records by industry



Source: 2014 Poneman Institute Survey

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.

THE ADVANCED PERSISTENT THREAT

The term Advanced Persistent Threat (APT) is often overused but the term itself has proved to be persistent, and it is a useful description of a type of attack and attacker that experience has shown to be stealthy, dangerous, and—all too often—successful. But network defense techniques that leverage information about the adversaries using these attacks can create an intelligence feedback loop and establish a state of information superiority, decreasing the adversary's likelihood of success with each subsequent attempt. Using the Cyber Kill Chain® to identify the Steps of an intrusion and map them to a response is a step toward instituting an intelligence defense.

The origination of the term "Advanced Persistent Threat" is credited to Air Force Col. Greg Rattray, who used it in 2006.

- The characteristics of an APT are: Advanced: It uses techniques that are sophisticated and/or that exploit previously unknown vulnerabilities (zero-day exploits), or some combination of exploits that enable it to quietly defeat a variety of defenses. Because of the use of combinations, and because not all APTs use zero-day exploits, some experts prefer the term "complex" over "advanced."
- Persistent: Attackers might spend months, or even years, achieving their goal. Once in, the attack is intended to be stealthy and to remain hidden in a compromised system, and if discovered to be difficult to remove. This stealth can be used to quietly steal data over a long period of time or can allow a destructive exploit to lie dormant until wakened by its master to execute its mission.

The book Reverse Deception: **Organized Cyber Threat Counter-Exploitation,** released in 2010, defines the criteria for identifying an APT:

- Objectives – The end goal of the threat, your adversary
- Timeliness – The time spent probing and accessing your system
- Resources – The level of knowledge and tools used in the event
- Risk tolerance – The extent the threat will go to remain undetected
- Skills and methods – The tools and techniques used throughout the event
- Actions – The precise actions of a threat or numerous threats
- Attack origination points – The number of points where the event originated
- Numbers involved in the attack – How many internal and external systems were involved in the event

It is difficult, if not impossible, to determine the number of APT attacks and the percentage of them that are successful. Because of their nature, a successful compromise can continue for years without discovery, and it is becoming commonplace to read accounts of companies that have suffered a compromise by an APT that have gone undetected for months or longer. It is likely that many compromises remain undiscovered. In some known cases information had been quietly exfiltrated, and in others malicious code has been found in critical infrastructure systems, apparently dormant and waiting for activation.

This illustrates the necessity of transitioning to a model of Intelligence-Driven Defense® which not only mitigates the vulnerabilities of a target system, but also reduces the threat by making it visible. Situational awareness—the ability to see and understand the operational status and risk posture of your assets and the current threats to them—is critical to the ability to protect against threats, whether or not they are advanced or persistent.

"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."

Situational awareness is not achieved by a single activity, tool or system. It requires knowledge of an organization's IT and OT resources, visibility into them, sensors to monitor their status in an ongoing fashion, and systems to analyze the results. Still, automated tools alone are not capable of detecting and responding to cybersecurity incidents—the systems must be augmented by trained people who can follow up on the results of the analysis. Understanding threats in today's environment also requires the sharing of information not only within an organization, but among companies within a sector, with government, and with the security research community.

A focused program that combines traditional security tools, automation techniques, cyber security standards and best practices, threat intelligence, and human analysis is essential for oil and gas companies to maintain an appropriate risk-based security posture.

leidos

II. Information Technology and Operational Technology

1. The Value Proposition of OT
2. The Threats to Oil and Gas

leidos

"OT is typically intended to perform one task, and reliability is its primary attribute. This puts a premium on stability and minimizes the opportunity for upgrades."

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.

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 use of Internet Protocols networking in OT systems can open these systems up to network attacks and can create backdoors into organizations' enterprise IT networks, putting both systems—and the information they contain—at risk. Managing these risks is complicated by the differing missions of the two systems and the fact that most OT network environments and devices are not monitored directly by security personnel.

THE VALUE PROPOSITION OF OT

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.

leidos

"Security refers to the ability to ensure availability, integrity and confidentiality of systems and data. Safety refers to the physical wellbeing of people, equipment and the environment; preventing injury and damage to people and things."

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.

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.

This is changing, however. With the integration of IP networking and the adoption of other standardized protocols in OT, cybersecurity now is becoming essential to safety with the ability for cyberattacks to produce physical world results.

Cybersecurity typically is achieved through frequent updates of software and equipment, which is anathema to those maintaining OT systems. When operational technology is acquired by an oil and gas company, the customer and vendor typically sign off on a Factory Acceptance Test for their equipment and systems, and a later Site Acceptance Test certifies that the technology is functioning correctly when installed. Any unauthorized change from that approved configuration, including security updates and patches, can invalidate the certification, which can void warranties and maintenance agreements and possibly create liabilities for the customer.

But security is becoming essential for these systems. OT monitors and measures conditions and activities in a process or in a physical area, and can control equipment and processes, including the execution of changes in operations. This makes the systems high-value targets for hackers, and there has been a marked increase in the number and sophistication of attacks against all types of control systems, including Supervisory Control and Data Acquisition (SCADA) systems. According to a March 2014 SCADA Security Survey conducted by the SANS Institute, "The number of entities with identified or suspected security breaches has increased from 28 percent to nearly 40 percent." More alarmingly, "only 9 percent can say with surety that they haven't been breached."

IT security is defined by the CIA triad— Confidentiality, Integrity and Availability:

- Confidentiality: Assuring that only authorized people or machines can access resources; through access control, rights management and encryption.
- Integrity: Preventing the unauthorized modification or destruction of data, both intentional and accidental.
- Availability: Assurance that all resources, both systems and data, are available when needed by those authorized to access them.

Because of the focus on reliability and uptime for OT, it puts Availability first in the triad.

Each of these three factors is necessary for adequate security. But in the OT arena, the critical nature of the processes that these systems control and the fact that the systems often have been made up of proprietary standalone equipment with few outside connections put an emphasis on availability. Simply put, as long as OT systems were not connected to the outside world, administrators did not have to worry about integrity and confidentiality.

This has all changed with the use of remote access and the implementation of Internet Protocols and standardized, off-the-shelf technology in OT systems. As with any advances, this one is a double-edged sword. Standardized equipment and the ability to access it through almost any Internet-enabled device bring economy, efficiency and convenience to the systems that monitor and control industrial processes. But they also extend the threats of the Internet into the operational domain, and there has been a lag in extending the necessary cybersecurity controls into this area.

Desktops or laptops with standard operating systems and USB ports, embedded WiFi connectivity, Bluetooth, and Ethernet all are being integrated into OT, and they require patching, updating, antivirus scanning and regular maintenance to remain secure. The owners of the OT systems often cannot use this IT-centric approach to security. A consequence of this integration can be out-of-date, unpatched operating systems and other components. The resulting threat is not merely to the OT systems and the processes they control, but also extends to the enterprise IT environment to which it is connected.

THE THREATS TO OIL AND GAS

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 sociopolitical 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 and CISO 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 entire enterprise.

Companies need to create comprehensive security policies, plan for the training to implement them, audit to ensure that the policies are being complied with, and monitor systems to detect changes in near real time. The nature of OT systems, with their emphasis on reliability and stability, means that some risks will remain in place, and policies need to address the mitigation and management of these risks based on their likelihood and their potential impact.

III. The Cybersecurity Maturity Model for Oil and Gas

1. The Government Standard

2. Cybersecurity and Health, Safety and Environment

leidos

"A maturity model is a framework that allows an organization to assess the rigor of its security practices and processes according to industry best practices."

A security breach is not a trivial incident. According to a **2014 Ponemon study sponsored by IBM**, the average cost to a company for each compromised record with sensitive or personal information was $201. And the cost in the oil and gas industry is significantly higher than the average—$237 per record.

Compromised data is not the only risk to companies in the Oil and Gas sector. Operations and physical facilities also are at risk. But the cost of compromised records is a simple tool to quantify and compare impact, and the study also found well-prepared organizations can reduce these costs. Companies that involved business continuity management in the remediation of a breach reported that they reduced the cost of a breach by an average of $13 per compromised record, and organizations with a strong security posture and a formal incident response plan in place prior to the incident could reduce the cost per record by as much as $38 compared with an unprepared company. Appointing a CISO to lead the data breach incident response team reduced the cost by another $10.

In other words, planning and policies for cybersecurity pay off, not only in savings in the event of a data breach, but also by reducing the likelihood of a breach. One aid to business continuity planning and improving the security posture is a cybersecurity maturity model.

A maturity model is a framework that allows an organization to assess the rigor of its security practices and processes according to industry best practices. This can help create a more robust security footing over time, reducing the number of successful cyber-attacks and enabling a quicker return to normal operations following a successful attack.

The maturity of an institution's security program can be plotted from basic—or immature—to comprehensive—or mature. It is probable that the cybersecurity of different parts of an organization, especially large ones, will be in different stages of maturity.

Maturity does not necessarily equal security. But higher levels of maturity mean that security practices and policies are repeatable and measurable, which can be tools to enable better security. An organization's security posture can be mapped to a maturity model, which can point out what steps are needed to improve security. Maturity can come at a cost, however. In large enterprises, progressing even one step up along the maturity model can be a significant undertaking fraught with challenges. Each organization must determine the proper maturity level to aim for, developing a maturity profile that provides it with an optimal mix of security and operational agility depending on the threats to that organization and the levels of risk it is willing to assume.

leidos

THE GOVERNMENT STANDARD

The U.S. Department of Energy (DOE) has developed a maturity model specifically for the industry, the **Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2)**. This model, part of a broader effort to improve security in the energy sector, is one of the few that includes both IT and OT and provides a mechanism to help evaluate, prioritize and improve cybersecurity capabilities in both areas. It is intended to help:

- Strengthen cybersecurity capabilities in the oil and gas subsector.
- Enable oil and gas organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities.
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities.
- Enable oil and gas organizations to prioritize actions and investments to improve cybersecurity

The model includes the core elements of the broader framework, as well as additional material tailored specifically for the oil and gas subsector. It contains a common set of industry-vetted practices for cybersecurity and includes a maturity model as well as an evaluation tool and DOE-facilitated selfevaluations. Companies can evaluate cybersecurity practices against the appropriate ONG-CSMS practices and assign a score in each domain. Scores can be compared with a target score, based on the company's risk tolerance for each domain.

The DOE is not regulatory and use of ONG-C2M2 is voluntary. The model is descriptive rather than prescriptive, allowing companies to select goals for themselves and establish the appropriate controls and policies for meeting them. The department expects that broad use of the model will help to establish benchmarks for the industry's current capabilities and help encourage implementation of the voluntary Cyber Security Framework for Critical Infrastructure developed by the National Institute of Standards and Technology.

Evaluating and tracking cybersecurity capabilities requires plotting and tracking key performance indicators (KPI), which are success metrics that align with organizational goals. Some common KPIs are improvement of cyber resiliency and response capabilities, which enable a company to return to normal operating procedures after a cyber incident. This requires solid information about what is happening and what controls already are in place within the enterprise. A tool that can deliver that level of accuracy is necessary before a serious effort to implement a cybersecurity maturity model can begin.

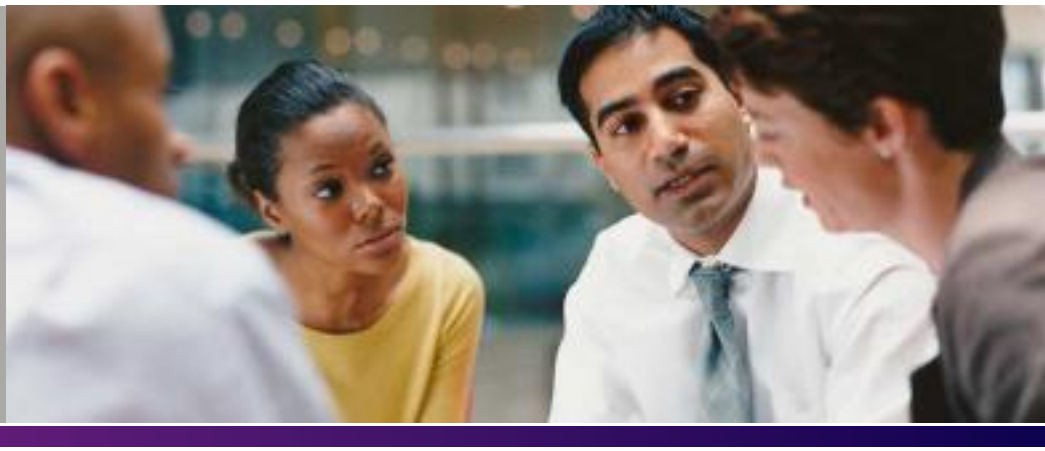
CYBERSECURITY AND HEALTH, SAFETY AND ENVIRONMENT

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.

"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."



HSE management includes stringent procedures for tracking and addressing all safety incidents and near misses in a facility, not just injuries and fatalities. The standards call for tracking:

- The number of near-miss safety incidents that occur,
- The number of minor safety incidents,
- The number of safety incidents that lead to a loss of time on the job, and
- The number of fatalities.

According to the **U.S. Occupational Safety & Health Administration**, at the time of its creation in 1971 there were an average of 38 fatal injuries in the workplace every day, or nearly 14,000 every year. Today, that average has dropped by more than two thirds to just 12 a day, and the industry continues to lead HSE improvements to keep improving.

Safety management in the oil and gas industry that has contributed to this drop in fatalities developed in three broad phases. The first was aimed at trying to remove risk from the environment by focusing on safety in the design and construction of plants. This had positive results, and when the reduction in accidents flattened out, phase two focused on procedures. In the wake of the Piper Alpha disaster of 1988, in which 167 oil rig workers lost their lives, safety procedures focused primarily on work management. The current phase focuses on behavioral safety, which aims to eliminate unsafe behavior, such as cutting corners and ignoring proper procedure to save time and effort.

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.

leidos

IV. Standards for Cybersecurity

1. The Cybersecurity Framework
2. Industry Standards

leidos

"Although oil and gas—like every sector—is unique and faces distinct challenges, there also is much that it shares with other enterprises that are operating Information Technology and Operational Technology networks."

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.

The U.S. government offers a comprehensive set of cybersecurity guidelines from the National Institute of Standards and Technology. **NIST's 800-series of Special Publications** provides guidance on implementing the best practices for cybersecurity.

FISMA is the foundation for cybersecurity for federal executive branch agencies, and although it is a government regulation, its requirements, guidelines and specifications can be applied in industry, as well. FISMA calls for a risk-based approach to cybersecurity, requiring agencies to have a complete inventory of their information systems and to assess the risk to each system as well as the impact of a compromise. Based on these assessments, the appropriate security controls are applied to address the risks. The risk-based approach recognizes that risk cannot be completely eliminated, and FISMA requires that someone in authority sign off on the operation of every IT system, approving the level of security that has been implemented and accepting the residual risk that must be managed. Information systems are to be monitored for vulnerabilities and compliance with the approved security controls, and periodically recertified for operation.

FISMA is a technology neutral, high-level regulation. Details for implementing its requirements are found in the library of NIST special publications, which provide guidelines and specifications for putting requirements into practice.

leidos

These publications are available to—and appropriate for use by—the general public and industry. **SP 800-82, Guide to Industrial Control Systems (ICS) Security**, which was revised in February 2015, provides guidance that is specifically applicable to OT.

A public-private collaboration has produced the **Critical Security Controls**, formerly known as the SANS Top 20 list, which identifies basic steps that organizations can use to enhance cybersecurity. Now in version 5, "the Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on 'What Works'." The list works on the 80-20 principle, the idea that a small number of vulnerabilities or problems are responsible for the majority of threats; prioritizing them can be a costeffective way to improve overall security.

THE CYBERSECURITY FRAMEWORK

More industry-specific guidance is offered in the **Framework for Improving Critical Infrastructure Cybersecurity**, "a set of industry standards and best practices to help organizations manage cybersecurity risk." This was published in 2014 by NIST in response to an **executive order** from President Obama on protecting privately-owned critical infrastructure. The goal is to better protect the critical infrastructure on which much of the nation's security depends, but which is outside the direct control of government.

Critical infrastructure is defined in the order as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. "This can apply to critical infrastructure in all nations, which "a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk," by owners and operators. "This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today."

CRITICAL SECURITY CONTROLS - VERSION 5

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
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Like other standards cited, it is voluntary and relies on “enlightened self-interest” to drive its adoption. It offers helpful guidance to owners and operators of infrastructure such as oil and gas production and distribution systems. The framework is intended to “enable organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.” It creates a shared cybersecurity vocabulary for risk management programs that can be used by companies in different industrial sectors.

NIST developed the framework in cooperation with the Department of Homeland Security and industry stakeholders, and it is composed primarily of already existing standards, many of them already included in NIST guidelines and proven in private industry to be useful in identifying, protecting from, responding to, and recovering from threats and attacks. Like other high-level standards it is technology neutral and does not specify applications or tools to be used.

“The framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure,” its authors write. “Organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.”

The framework consists of three basic elements:

- The Core, a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational profiles.
- Profiles to help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources; evaluate their current state of risk management; and prioritize actions to be taken for improvement.
- A set of four Tiers to provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. They describe the rigor of existing risk management and allow a determination of how closely it is aligned with business requirements.

Although the framework is not mandatory and is “based on business needs without placing additional regulatory requirements on businesses,” regulatory agencies are expected to harmonize their existing regulations to the framework, and government contractors are likely to see conformance requirements included in procurement language.

By remaining technology-agnostic and employing existing standards, guidelines and best practices, the framework is intended to provide multiple approaches to cybersecurity.

NIST says that the framework will remain a living document and will be updated with feedback and lessons learned from the companies implementing it.

INDUSTRY STANDARDS

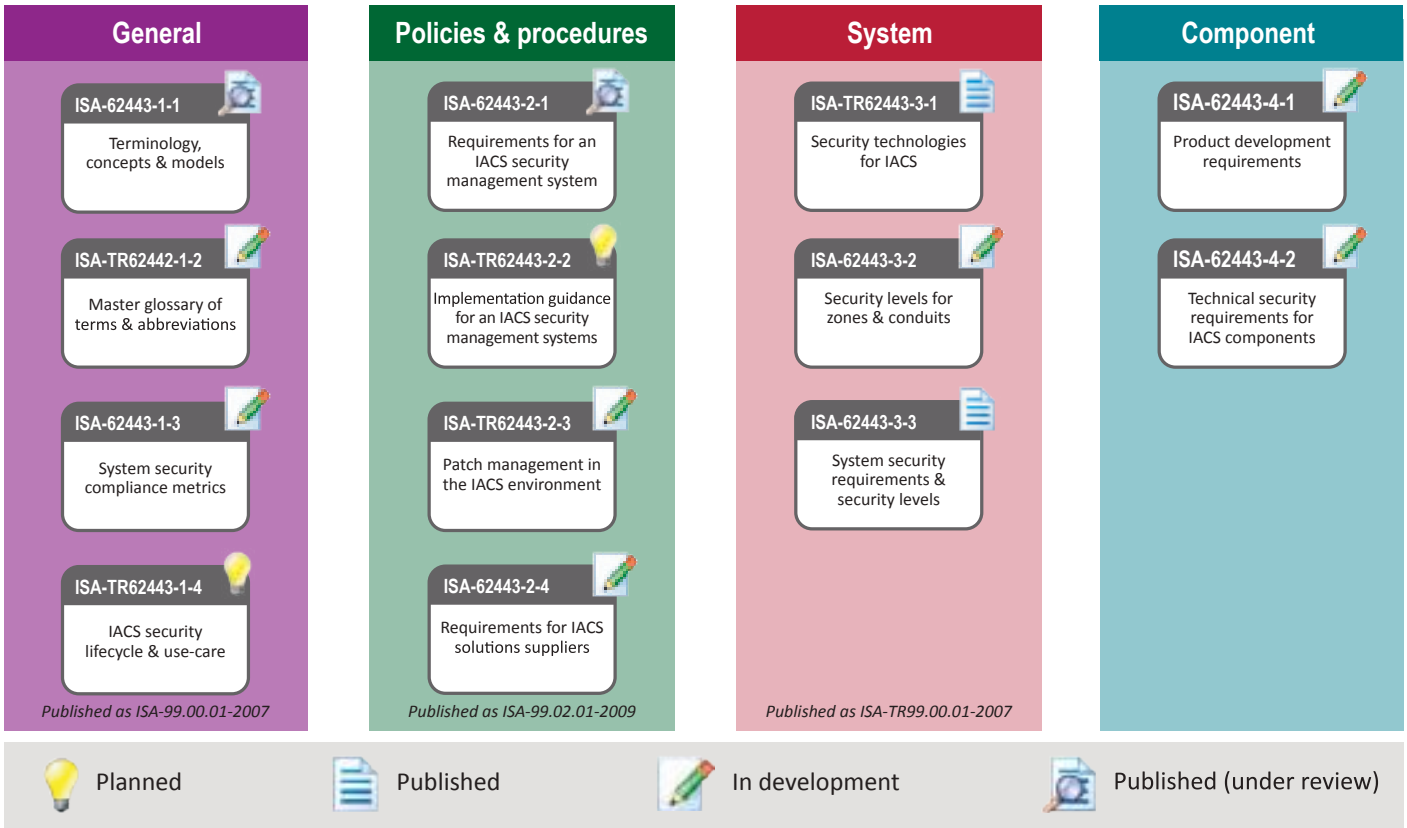
Standards-making organizations in the private sector are producing more specific guidance to help companies secure their operational technology, including standards on securing electronic Industrial Automation and Control Systems (IACS). ISA/IEC- 62443 is a set of standards and technical reports produced primarily by the International Society for Automation (ISA) to "define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance."

The standards were developed by the ISA99 committee and originally released by the American National Standards Institute. Originally they were known as ANSI/ISA-99. They have since been aligned with corresponding standards from the International Electrotechnical Commission (IEC) and have been renamed ISA/IEC-62443. The ISA99 committee on Industrial Automation and Control Systems (IACS), which includes more than 500 members from companies and industry organizations around the world, continues development of the evolving standards.

For the purposes of the standards, manufacturing and controls systems are defined broadly to include hardware systems such as distributed control systems (DCS); programmable logic controllers (PLC); supervisory control and data acquisition (SCADA); and networked sensors, monitors and diagnostic systems. It also includes the associated internal, human, network, or machine interfaces.

The standards help identify and address vulnerabilities in order to protect both the equipment and the information contained in control systems whose compromise could result in:

- Endangerment of public or employee safety
- Loss of public confidence
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Economic loss
- Impact on national security



Source: *The International Society for Automation*

They are organized in tiered categories:

- General, the top category, contains publications on basic elements, including terminology, concepts and models; a master glossary of terms and abbreviations; system security compliance metrics; and IACS security lifecycle and use-case.
- Policies and Procedures contains requirements aimed at the asset owner for an IACS security management system; implementation guidance for an IACS security management system; patch management in the IACS environment; and requirements for IACS solution suppliers.
- System contains publications with guidance for system design and integration on security technologies for IACS; security levels for zones and conduits; and system security requirements and security levels.
- Component, the final category, contains product development requirements and technical security requirements for IACS components for vendors.

Ultimately, oil and gas companies are responsible for the security of their own information and operational systems, with help available from industry organizations and government in the form of best practices and guidelines for implementing standards. The Department of Homeland Security also offers assistance to companies requesting it, with audits and advice on implementing cybersecurity plans and controls.

All 50 U.S. states have some computer hacking laws on their books criminalizing malicious activity, but there is little specific protection for the most sensitive elements of our cyber infrastructure. Only one state, Arizona, addresses critical infrastructure, elevating computer tampering involving a critical infrastructure resource to a class 2 felony, the most serious level of offense assigned to computer hacking.

Although the responsibility for protecting both IT and OT systems falls on the owners and operators, the job cannot be handled successfully by the company alone. Every company in the oil and gas industry must allocate adequate resources, both financial and personnel, to handle the task of security, but they do not have to do it all by themselves. Partnering with vendors who can provide the proper information and advice as well as products and services to protect essential technology resources can be critical to establishing the levels of security and the security controls appropriate for each company and the divisions within a company.

V. Solutions for Securing the Oil and Gas Infrastructure

1. Steps for Addressing Security
2. The Industrial Defender Solution

leidos

“Regardless of the organization’s level of awareness and maturity, assistance is available to help improve cybersecurity status. Leidos has the experience, knowledge and expertise to provide the consultant-based services an organization needs as well as an OTspecific security technology.”

No company in the oil and gas industry has to stand alone when securing its information and operational technology systems. Leidos offers the solutions and the professional services to help companies assess their current security status and chart a roadmap to full implementation of the technology, processes and practice needed to achieve the appropriate levels of security.

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.

Stuxnet is perhaps the best-known attack against an industrial control system, but German officials in 2014 confirmed that a cyberattack did massive damage to an unnamed steel mill. Key services, such as electricity, water, food processing, and transport, as well as oil and gas and refining, depend on OT systems to operate safely and reliably. If these services fail the impact on society can be rapid, with risks to both public safety and economies. A risk to an OT is a risk to the business itself, impacting safety, the environment, financial wellbeing, reputations, and contractual or regulatory requirements.

Integrated IT and OT security is a new trend in the oil and gas industry, although there are varying levels of awareness and implementation. Some organizations have little or no awareness of or interest in the issue, while some are aware of the need but are unsure how to proceed. Some are addressing security but are not as advanced as they believe, and others have misplaced confidence in IT perimeter defenses that cannot adequately protect OT systems. A very few have established a robust and on-going security program and management system.

Regardless of the organization’s level of awareness and maturity, assistance is available to help improve cybersecurity status. Leidos has the experience, knowledge and expertise to provide the consultant-based services an organization needs as well as an OT-specific security technology.

leidos

STEPS FOR ADDRESSING SECURITY

The Leidos 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.

Events such as the Stuxnet attack discovered in 2010, Project Shine, a global scanning project in 2012 and 2013 to discover Internet accessible ICS and PCS systems, together with the recently recognized cyberattacks in Turkey and Germany, have helped to bring the security issue to light. But the threat is far broader than a few high profile incidents at high value targets. Any organization can be a victim, and for every major breach that makes headlines, there are many other less well-known minor incidents and even more near misses. To fully understand security needs, executives should be aware of the full spectrum of incidents and threats that they face.

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.

When the review is completed, priorities can be established for the organization's immediate, mid-term and long-term goals with a recommended roadmap of options to achieve those goals. Change can be difficult in any organization, and the most significant factor in the time it takes to achieve long-term goals often is the organization's ability to absorb and adapt to changes rather than its ability to make them.

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. In PCN especially, some older systems cannot be upgraded; they would need to be replaced in order to bring them into full security compliance. More than likely, replacement will be impractical and the risks associated with the system will have to be accepted.

Accepting risk does not mean ignoring it, however. Attention must be paid to residual risk according to its severity, controls put in place to mitigate it and reduce the likelihood of an exploit, and response plans created to deal quickly with an exploit.

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.

"Industrial Defender ASM® does not do everything, but manages the common functions of various tools that make up the bulk of their activities, automating them as much as possible and providing a common interface for these activities."

Automation 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 automation that are practical in the control system environment. Although Intrusion Detections Systems can be valuable, for instance, Intrusion Prevention Systems are rarely if ever used in industrial and process control because the need to keep processes operating trumps the efficiency of an automated response to a detected intrusion.

Continual monitoring and maintenance: Once the desired end-state for an organization is achieved, it must be maintained. This can involve ongoing monitoring of the security of the systems, controls, and processes as well as on-site maintenance to ensure that configuration remains within intended parameters.

THE INDUSTRIAL DEFENDER SOLUTION

Just as there is no one path to effective cybersecurity, there is no one tool that can do it all. To achieve the needed situational awareness across multiple security tools, the Industrial Defender Automation Systems Manager® (ASM) offers applications engineered to address the overlapping requirements of cybersecurity, regulatory compliance and change management on a single platform. It provides a consolidated and unified view into control systems that is critical for effective management of a heterogeneous environment. An integrated approach to managing these functions increases the efficiency and effectiveness of security operations across each of the different tools, such as asset management, configuration and change management, policy management, event monitoring, and compliance reporting. Industrial Defender ASM® combines these functions to provide a single interface and a single plane of glass.

Managing these tools without the Leidos Industrial Defender ASM® would require purchasing and maintaining multiple products, which creates stovepipe environments with little or no integration.

Industrial Defender ASM® manages the common functions of various tools that make up the bulk of their activities, automating them as much as possible and providing a common interface for these activities.

This gives organizations situational awareness and allows them to monitor and evaluate compliance with regulations and with company policy, with automated tracking and documentation to satisfy audit needs.

Taking advantage of the services and solutions offered by Leidos can help companies in the oil and gas industry to achieve and maintain their specific security goals and achieve the levels of security needed to ensure the continued reliable and safe operation of critical systems and processes and to effectively manage risk for themselves, their partners, and their customers.

leidos

VI. About the Author

Jason Holcomb

Jason is a Principal Security Consultant for the Leidos Commercial Cyber Solutions group. He has 15 years of experience in cybersecurity consulting and research with a focus on Industrial Control Systems and Operations Technology. He has developed and executed assessment processes for Intelligence Driven Defense®, leads OT assessment service offerings, and has a lead role in the development of integrated IT/OT SOC environments for the Leidos commercial clients. His experience spans multiple industries including oil and gas, chemical, electric, nuclear power, and telecommunications. He has performed research for Leidos and Department of Energy projects, developed security tools and assessment techniques, and contributed to industry publications and conferences. Jason earned a BS in Computer Science from Evangel University and an MA in Computer Resources and Information Management from Webster University.

To find out more about how Leidos INTELLIGENSE DRIVEN DEFENSE® solutions including CYBER KILL CHAIN® cyber intelligence technology allows information security professionals such as yourself to proactively remediate and mitigate advanced threats in the future, please visit us at cyber.leidos.com

FOR MORE INFORMATION
855-56-CYBER / cyber.security@leidos.com
cyber.leidos.com