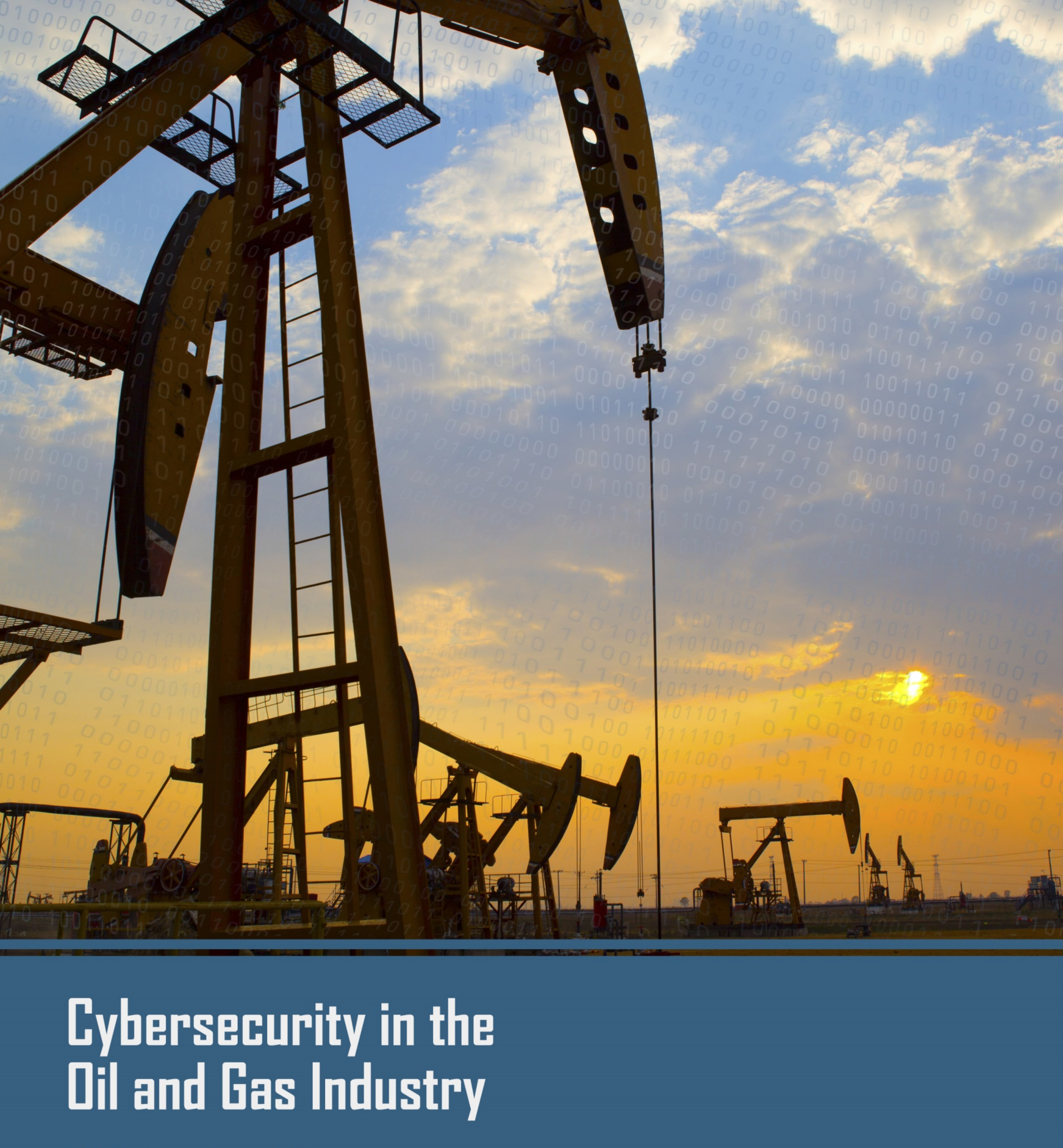


Cybersecurity in the Oil and Gas Industry

A White Paper Presented by:

Lockheed Martin Corporation

Cybersecurity in the Oil and Gas Industry

When discussing an unsuccessful attempt at drilling for oil in the Mukluk Prospect of the Beaufort Sea in 1983, the then President of Standard Oil of Ohio (Sohio), Richard Bray, once remarked "We drilled in the right place - we were simply 30 million years too late."

The story of millions of dollars lost in drilling into a dry bed in Mukluk underscores the risks associated with exploration and subsurface operations within the Oil and Gas industry. It was a pivotal learning experience that led to a better understanding in the industry on the value of proper risk management and risk implementation within decision-making.

The oil and gas Industry has always carried a unique set of risks. Unlike most other sectors where protecting intellectual property (IP) takes a prominent role within the corporate Risk Management Framework, the dangers associated with oil and gas places the security of people and the environment at the forefront of their risk policies.

The oil and gas industry always carries the dangers associated with dealing with a combustible element in extreme and often remote conditions. Add to those dangers the often unpredictable nature of sociopolitical events with the often inclement weather of drilling locations, and the very nature of finding, transporting, and refining oil and natural gas becomes daunting.

Losing money by drilling into a dry well, while damaging to the revenue stream, appears less drastic when compared to the damages incurred on any one of the major disasters that occurred over the last 30 years. If something goes wrong in this industry, lives, local habitats and even global economies are at risk.

It’s no wonder that this industry has pioneered the implementation of Health, Safety and Environment (HSE) as an organizational pillar universal in this sector. The safety and wellbeing of others takes prominent stage whether upstream, midstream or downstream, even before that of the hydrocarbons that each company struggles so hard to find, refine, transport and sell.

Few industries triage and escalate prospective (HSE) near misses with the purpose of predicting incidents with the same thoroughness as oil and gas companies. Fewer private sector companies promote the value of such seemingly innocuous acts as holding the handrails when climbing or descending stairs, or making sure to start each presentation with a safety slide describing the precautions or actions attendees must know about in the event of an emergency.

Intellectual Property Paradox

In the oil and gas industry Intellectual Property (IP) takes-up various forms. From volume, velocity and variety readings to geophysical equations, the data that flows throughout every part of an upstream, midstream, and downstream company is as varied as it is sacred to the present and future health of each organization.

Compounding the challenge in protecting IP in oil and gas is the accessibility of data crucial to the complete operation of the industry. In enhance exploration and production, for example, IP is being used not only to find new sources of oil and gas, but to reduce the non-productive time (NPT) of assets by predictive maintenance of critical components such as ESPs (electric submersible pumps).

IP is even being used to help reduce the Health, Safety and Environment incidents within drilling and production, and provide end-to-end views of hydrocarbon reservoirs and advanced pattern detection.
In refining and manufacturing, IP is used to reduce the NPT of assets through the predictive maintenance of critical components such as rotary equipment. IP can also include the data used to improve asset performance management through real-time metrics across different subsystems.

IP provides the competitive advantage that sets each company apart from the other in a highly-integrated industry. It also helps oil and gas companies better understand the current environment to deliver better future results.

The challenge with IP in the oil and gas sector is determining how to best keep the IP safe, yet accessible to those that need it.

In attempting to understand the complete dynamics that go into making safety and security a top priority in the Oil and Gas Sector, it's easy to overlook the importance of cybersecurity and the integration of information technology (IT) and operational technology (OT).

Operational Technology is hardware and software that a company uses to monitor or control an environment. OT commonly detects, measures, and executes a change, or event, within a given physical area. Most commonly associated with physical access devices or within manufacturing, OT has increasing become integrated within the IT backbone of many organizations. Understanding this technological merger is important step in understanding the threat landscape.

The Universal Trend

Depending upon your sources, the statistics on cyber-attacks varies. According to a recent Symantec study there was a 91 percent increase in targeted attack campaigns in 2013, which includes a 62 percent increase in the number of breaches. The same report cited that 1 in 392 emails contain phishing attacks and that web-based attacks are up 23 percent over a similar time last year.
http://www.symantec.com/security_response/publications/threatreport.jsp

A different report by IBM stated that in the United States alone, there was an estimated 1.5 million monitored cyber-attacks in 2013. That equates to roughly a 12 percent year to year increase in security events. (http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/)

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

- ***The rise in cyber-attacks***
- ***The increase in attack sophistication***

Over the last 30 years the oil and gas sector has endured a number of well-known cyber-attacks. One of the most famous attacks, perpetrated by an organization called the Cutting Sword of Justice, was the Saudi Aramco attack of 2012. This attack aimed at stopping oil and gas production in Saudi Arabia's largest exporter within the Organization of the Petroleum Exporting Countries.

This attack crippled 30,000 computers and disrupted Saudi Aramco for months. However, an important lesson from the attack pertains to the Business Continuity Planning (BCP) aftermath. If all your desktop computers suddenly became useless, could your organization operate completely on paper if it had to? Could your organization procure thousands of new hard drives if it needed to replace all of its computer systems? How long would that take? Where would those computers come from? What procedure would employees follow and how would they know what to do?

As devastating as the attack was on Saudi Aramco, in some respects it was fortunate. The cyber-attack focused on damaging 32-bit machines, leaving the 64-bit servers intact. The attack on RasGas Company Limited, possibly by the same organization just two weeks later, included an improved variant of the Aramco virus that infected 32 and 64-bit machines, making that devastation more severe. The main takeaway from this second attack is a lesson on how fast back-to-back attacks can occur, and how well attackers learn from their mistakes.

The attack on Saudi Aramco ultimately failed to disrupt production, but was one of the most destructive cybersecurity strikes against a single business.

More importantly, this attack echoed the need for oil and gas companies to evaluate the importance of a cyber-threat landscape with regard to attacks and uncovered vulnerabilities.

Understanding the Threat Landscape

The global oil industry is expected to spend $1.87 billion by 2018 in cyber-security. This figure is according to a 2013 study by ABI Research, which states that the oil and gas sector "is connecting its industrial control systems (OT) full of unpatched vulnerabilities to the Internet, where cybercriminals roam in all impunity."

The ABI Research study also describes the IT infrastructure 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 SCADA." As a measure to update their security infrastructure, this study predicts that the oil and gas sector will increase spending in IT and OT security significantly.

According to a similar report by Frost & Sullivan, entitled Global Oil and Gas Infrastructure Security Market Assessment, the total oil and gas infrastructure security market is expected to increase from $18 billion dollars a year in 2011 to $31 billion dollars by 2021. http://www.slideshare.net/FrostandSullivan/global-oil-gas-infrastructure-security-mkt-m83-dnov-2012

Finally, during a recent Cybersecurity for Oil, Gas, and Petrochemicals Summit, the organizers of the summit quoted the Global State of Information Security® Survey 2014, by Price Waterhouse Coopers, that demonstrated spending on cybersecurity solutions in the oil and gas sector increasing by average of 32% in 2013 from the previous year. http://www.cyberoilandgas.com/Opportunities.aspx

These reports allude to an increase in cyber-attacks by Advanced Persistent Threats (APTs), a term coined by the United States Government describing organized conglomerates of hackers and cyber-attackers that target specific companies or governments as part of an agenda. APTs are regarded as well-funded, well-supported and well-educated.

The reports also suggest three reasons that the oil and gas industry needs to move towards a more stringent application of cybersecurity:

1. Greater Integration within Value Chain

The very nature of the oil sector as a giant ecosystem comprised of upstream, midstream and downstream companies and organizations complicates the security landscape. This massive infrastructure made-up of Independent Oil Companies (IOCs), state-owned oil companies, smaller companies that focus on only certain streams and armies of service providers and third-party entities provides a ripe environment for security gaps and multiple points of entry.

The additional integration between these organizations within the oil and gas ecosystem can lead to ripple effects when a disruption such as a spill, an attack, or a sociopolitical issue occurs.

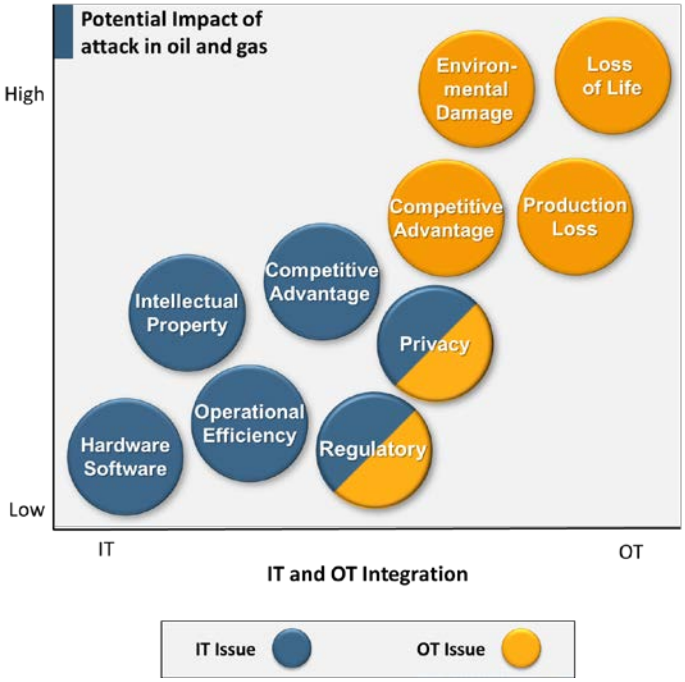
2. Availability, Integrity, Confidentiality (AIC)

The oil and gas sector was built with accessibility at its core. The entire nature of the industry, since its inception, is to focus on making oil and gas as accessible as possible whether removing it from the ground, transporting it to refineries or getting it to the consumer.

The need for accessibility at this level has created an industry that relies heavily on operating technology and an AIC model where the technology in place focuses more on availability and less on confidentiality:

- **A**vailability: Ensures that all resources (systems and data) are available when needed
- **I**ntegrity: Prevents the unauthorized modification of data including unintentionally inaccurate data. This could be a software programming, or system configuration error, absence of data, or added data.
- **C**onfidentiality: Ensures that only authorized people can access resources
  Source: http://rbubblog.wordpress.com/2012/06/03/security-triad-aic-cia/

Industries less reliant on OT use a more common CIA model of prioritization with confidentiality of IP and data as its top priority. However, the oil and gas industry was designed with availability of oil and gas, and the data that provides their availability, as its main focus. This is indicative on an industry heavily dependent on volume, numbers, and pressure readings. In the past the AIC model hadn't caused a significant security concern because the OT that provided much of this accessibility required physical access and was seldom networked for remote access. However, the integration between IT and OT is changing this very nature of OT to produce a potential opening for cyber-attacks.



In the oil and gas sector this integration is focused on making the OT remotely accessible to provide a faster understanding of the data and improve production performance, while providing remote support and diagnostics. Network-added capabilities to OT increase the availability of data and the subsequent accessibility of oil and gas that this industry needs to become more agile and minimize costs. The vulnerabilities associated with this integration, however, are two-fold.

First, by placing OT on the network it automatically makes it available to those that hack or breach the network those nodes are on. This places the confidentiality and integrity aspect of the AIC model at risk.

And secondly, by adding networking and remote controlling capabilities to operational technology often uses commercial off-the-shelf technologies (COTs). Desktops or laptops with standard 32-bit operating systems, USB port integration, embedded 802.11a,b,c and n antennas, Bluetooth, Ethernet—all of these technologies need patching, updating, antivirus and maintenance. OT, often built to provide unidirectional communication and legacy operating systems, can't rely upon an IT-centric approach to basic security such as anti-virus and patching.

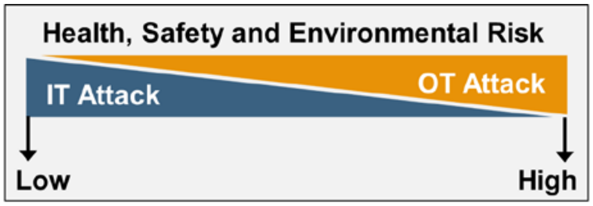
The result of this integration can be an out-of-date operating system that an organization hasn't updated with a patch because the patch requires a change. The system is tested (Factory Acceptance Test or FAT) in a certain configuration, which is signed off by the system vendor and the customer as functioning correctly. Any change from that configuration, including a patch, renders the FAT invalid and therefore the system invalid. Companies (and the vendors) have not seen the need to patch and in some cases, the vendor will not provide approved patches and void the warranty if any unapproved patches are applied.

3. Newer technologies

Adding to the complexities associated with a highly-integrated industry dealing with the combination of IT and OT are the new technologies on the horizon that could further blur the lines for a CIO or CISO attempting to protect the enterprise.

Digital oil fields connected to cloud systems that run Big Data initiatives, the use of drones in upstream oil and gas to run magnetic surveys, gravity anomaly surveys or monitoring for environmental issues and third-party companies that are now providing the ability to host 3D modeling for Well and Field Planning can complicate security policies. These are just a few of the cutting-edge technologies currently permeating the industry that could create additional vulnerabilities, particularly when paired with the integration of IT and OT.

The result of these vulnerabilities are the need to allocate spending on IT networks, industrial control systems and data security as well as emergency counter measures and the development of policies and procedures that provide the balance required between accessibility, confidentiality and integrity.



Cybersecurity and Health, Safety and Environment

The best approach towards mitigating the cyber-threat associated with IT and OT is to examine their integration in a collaborative environment. The discussion shouldn't be IT versus OT but rather IT and OT. The integration of the two technologies is inevitable, but the policies and procedures need to be bolstered to incorporate the capabilities, or requirements of and difference between, each technology. In many ways the safety of an organization and its IT is dependent on this successful integration.

According to the United States Occupational Safety & Health Administration (OSHA), before its creation 43 years ago, an estimated 14,000 workers were killed on the job every year. Today, workplaces are much safer, going from 38 fatal injuries a day to 12. https://www.osha.gov/dep/fatcat/dep_fatcat.html

Much of the success that the oil and gas sector has had in mitigating the risks and dangers around their day-to-day activities associated with working with a combustible element in a dangerous environment has been by implementing stringent procedures within HSE that include tracking incidents and near misses, not just injuries and fatalities.

Currently, the oil and gas industry tracks:

- the number of near safety misses
- the number of minor safety incidents
- the number of safety incidents that lead to a loss of time
- the number of fatalities

The current state of HSE is a study in evolution, generally created in 3-phases. The first phase of safety within oil and gas was aimed at trying to determine the safety-risk of an organization. When the reduction in accidents flattened out, the oil and gas industry entered phase two, which added procedures. In the wake of the Piper Alpha disaster of 1988, in which 167 oil rig workers lost their lives, these procedures focused primarily around work management. Finally, when that reduction flattened out, the oil and gas industry evolved to the current state of behavioral safety, which entails trying to get people to stop doing unsafe things and not cut corners or ignore procedures.

The true lesson in these phases of HSE evolution, which run in-parallel with the evolution of cybersecurity, is the need to address challenges through solutions that encompass people, processes and technology, in parallel. By adding this level of rigor, oil and gas companies are able to predict and mitigate the level of risk that their employees and local communities are subject to in the present and near future. This rigor is accompanied by comprehensive safety training that encourages the vigilant participation of all staff in looking-for and calling-out potential safety issues and incidents.

This process can be as effective with cybersecurity, and the vulnerabilities of integrating IT and OT, as it is with health, safety and the environment. If a tech, for example, is about to plug a USB device into a computer or OT device, and by following procedure, first scans the USB which then detects a virus, this should be recorded in a central log as a "near miss."

If a breach is detected by a cybersecurity analyst, and results in no data loss, this activity should be recorded as an "incident." If a loss of data or integrity is reported, this should be recorded as a "loss."

By standardizing, recording and tracking all cybersecurity activities in a manner similar to the way HSE records incidents, organizations can better mitigate the integration of IT and OT, and the risks associated with their technological ecosystems.

Aligning Solutions

The greatest challenge in mitigating the risks associated with IT and OT integration, and in standardizing, recording and tracking cybersecurity activities lies in finding a platform that centralizes all the moving parts of this strategy. All too often, cybersecurity platforms are too IT focused and don't incorporate the OT elements of data integrity and availability.

Lockheed Martin has approached this challenge by successfully combining the IT and OT landscapes with the integration of Industrial Defender. Industrial Defender is a security product company built on a robust history of OT security knowledge and experience. Industrial Defender helps organizations address the people (e.g. training), the processes (e.g. policy and procedures) and implement the security technologies needed to address modern OT security challenges.

Industrial Defender pairs these capabilities with a philosophy that continues to maintain and improve security in a perpetual fashion.

Security is a never ending journey, not a destination.

Throughout that journey, Industrial Defender provides the tools and technology that not only delivers security and compliance, but change management. All these capabilities are experienced through a single portal across a company's asset base. This solution includes deploying automation system agents that are purpose-built to integrate with technologies from leading automation vendors, and deliver critical capabilities that support the overall enterprise.

More importantly, this solution does not negatively impact operations or systems. It provides solutions supported by the operational and compliance requirements at the heart of each project.

When paired with Lockheed Martin's Intelligence Driven Defense (IDD), it creates a holistic approach that protects IT and IP from the Advanced Persistent Threats (APTs). This threat is comprised of well-funded, well-trained organizations trying to specifically target a company in an effort to steal data and impact their operational environment.

An approach to cybersecurity similar to HSE, combined with Intelligent Driven Defense and Industrial Defender solutions addresses the full-spectrum of threats in a manner that maintains the accessibility needed within oil and gas, while safeguarding the confidentiality and integrity integral to IT and OT.

Cybersecurity in the Oil and Gas Industry

For additional information on Cyber Security Solutions

Email: cyber.security@lmco.com

Phone: 855-LMCYBER – 855-562-9237

www.lockheedmartin.com/cyber