DYNAMIC POSITIONING CONFERENCE
October 10-11, 2017

Cybersecurity in the Oil and Gas Industry – What's here and What's Coming

---

Cybersecurity in O&G Industry

By Aarushi Goel

GoDaddy

Abstract

Cyber-attacks are increasingly targeting the O&G industry by myriad hackers: Trans-national terrorists for political reasons, cyber criminals for extortion by threatening attacks, and hacktivists for anti-energy policies. Because the critical infrastructure is a basis for our economic and national security, the U.S. government is generating new programs (i.e., the NIST Cyber Security Framework) and considering additional regulations. Current regulations are being re-interpreted under cyber security.

The existing oil and gas industry is an increasingly technologically complex one. More and more processes are being digitized; data mining and analytical programs are being used more frequently, and sensors are everywhere. This may lead to more efficiency, but it also makes systems more vulnerable to cyber-attacks. Security attacks in other industries can create disruption and monetary damages to businesses and individuals, but when security attacks compromise oil and gas industry SCADA systems and overtake their industrial control functions, the results can be disastrous — even deadly. If cyber hackers compromise the industrial control network running a pipeline, for example, they could adjust pipeline compressors to increase pressure until a weak point in the pipeline explodes. And all this can be done from anonymous, remote locations via the internet or other similar external communications pathways.

This presentation will justify the need for a cyber security architecture in Oil & Gas industry including the past/possible threats and the catastrophic impacts they may have on the industry. Lastly, this presentation will cover a specialized Oil & Gas NIST framework for effective implementation of security measures in current infrastructure in the form of standards, guidelines, and practices to promote the protection of critical infrastructure.

Abbreviation / Definition

IT – Information technology

OT – Operational Technology

ICS - Industrial Control Systems

NIST - National Institute of Standards and Technology

RAM - Risk Assessment Matrix

PCD - Process Control Domains

PLC - Programmable Logic Controllers

DCS - Distributed Control Systems

SCADA - Supervisory Control and Data Acquisition

SIS - Safety Instrumented Systems

BAS - Building Management/ Automation Systems

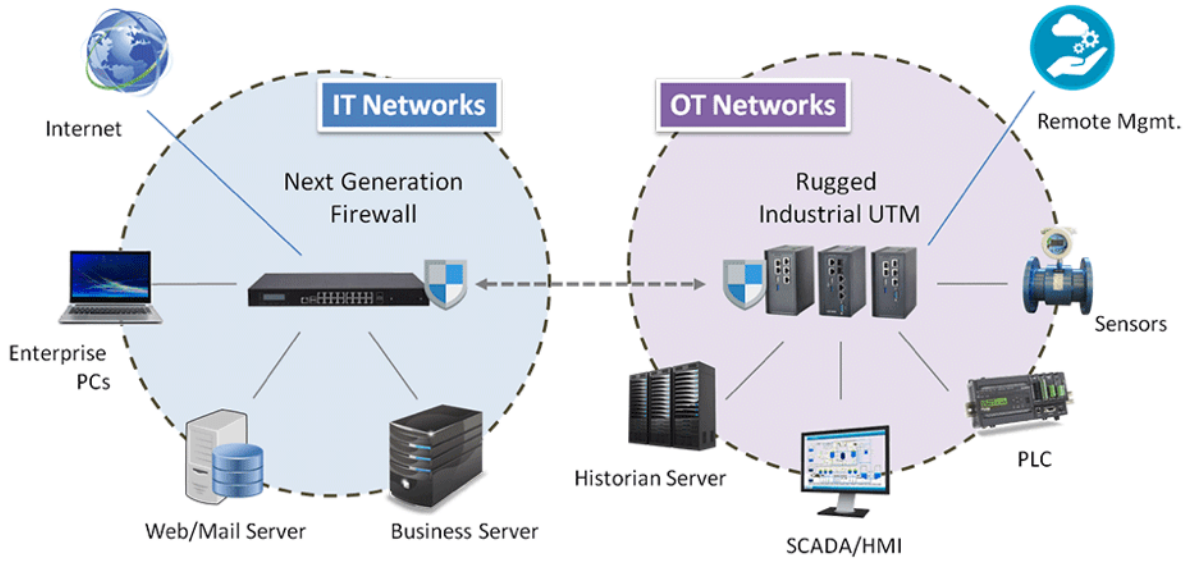
ERP - Enterprise Resource Planning

Introduction

Data can be disruptive. For a long time, the management of industrial technology was split across two camps: information technology (IT) and operational technology (OT). IT worked from the top down, deploying and maintaining data-driven infrastructure largely to the management side of business. OT built from the ground up, starting with machinery, equipment, and assets and moving up to monitoring and control systems. For a long time, these two divisions kept to their own turf and found their own effective solutions to problems.

A typical Oil & Gas framework would consist of an Operational Technology network that consists of hardware and software systems that monitor and control physical equipment and processes. This technology uses many specialized terms such as process control domains (PCD), programmable logic controllers (PLC), distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, safety instrumented systems (SIS), and building management/ automation systems (BAS), often collectively referred to as Industrial Control Systems (ICS). (Harp & Gregory-Brown)

Then came smart machines, big data, and the Industrial Internet, and the worlds of IT and OT suddenly collided. Data, once the purview of IT, is now ubiquitous on the operations floor. Using data to enhance productivity is central to the Industrial Internet. In order for that purpose to be fulfilled, IT and OT, developed separately with independent systems architectures, need to come together and find common ground to develop a new information-driven infrastructure. (Digital)



(Intel)

However, the sudden adaptation of these techniques could result in some unforeseen results. The poor segmentation of corporate and industrial networks can let a hacker gain unauthorized access to corporate network by exploiting known vulnerabilities in the network and then move laterally to intended industrial systems using compromised user credentials. As IT being not the main business of Oil and Gas companies, proper emphasis is not made to ensure secure IT operations. With the advancement in hacking techniques and terrorist hacktivities, a single loophole in the IT network is enough to compromise entire network of an organization.

Here are some of the risks a company may face in the case of a successful attack:

- Plant shutdown
- Equipment damage
- Utilities interruption
- Production circle shutdown
- Inappropriate product quality
- Undetected spills
- Safety measures violation resulting in injuries and even death

How Hackers Can Break into The Operational Technology (OT) Network

Stuxnet, a computer worm targeting industrial programmable logic controllers (PLCs) and SCADA systems, was a wake-up call to every industry. Despite the fact that it was not specifically designed to attack the petroleum industry, several oil and gas companies were infected with the virus.

The general idea is simple: Enterprise applications such as enterprise resource planning (ERP) or business intelligence (BI) systems are typically connected with numerous plant devices using different integration technologies to, for example, transfer data collected by these smart devices to a corporate network for further analysis. Unsecured connections between IT and OT environments can lead to vulnerabilities. The three most worrisome attack vectors are outlined below:

1. **Oil Market Fraud**
   Cybercriminals could conduct this type of attack by manipulating data from field devices and tank management systems within the company's ERP systems, and modifying parameters regarding oil in stock.

2. **Plant Destruction**
   Numerous processes like oil separation and refinery are also open to attack through burner management systems (BMS). These processes not only send information but are also managed remotely through business applications via special intermediate systems. These systems often use unsecured PLC devices, and vulnerabilities can be leveraged to create an explosion simply by turning off purge functionality, which BMS systems are responsible for.

3. **Equipment Sabotage**
   Remote plant equipment is at risk of data manipulation, including temperature and pressure measurements. A hacker could implant false data showing that there had been a breakdown in the equipment in a remote facility, leading the victim company to waste time and financial resources investigating.

There is no air gap between IT and OT systems, and there are business applications that exchange information with critical devices. So consider the secure settings of these connections and business applications, because those are the first line of defense against an attack. (Polyakov, 2017)

Categories of Oil and Gas network and their Cyber Security struggles

Different areas of oil and gas carry different types of risks and struggles, and thus require different types of combat strategies.

Upstream

The first abstraction layer of Oil & Gas network starts with Upstream that includes exploration, development and production of crude oil. It covers searching, and producing crude oil from underground or underwater fields. This would require conducting the entire drilling operations to bring the crude oil to the surface. The activities just described have been considered as part of Operational Technology(OT) network for years consisting of necessary tools and equipments.

Among the upstream operations, development drilling and production have the highest cyber risk profiles; while seismic imaging has a relatively lower risk profile, the growing business need to digitize, e-store, and feed seismic data into other disciplines could raise its risk profile in the future

A large O&G company, for instance: uses half a million processors just for oil and gas reservoir simulation; generates, transmits, and stores petabytes of sensitive and competitive field data; and operates and shares thousands of drilling and production control systems spread across geographies, fields, vendors, service providers, and partners.

What adds to this vulnerability is contrasting priorities of companies' operation technology and information technology departments. Operation systems close to drilling and well site operations such as sensors and programmable logic controllers are intended to perform tasks with 24X7 availability as their primary attribute, followed by integrity and confidentiality. In contrast, IT systems such as enterprise resource planning have a reverse priority order of confidentiality, integrity, and availability. This clash of objectives—safety versus security—plays out in drilling and production control rooms where engineers fear that stringent IT security measures could introduce unacceptable latency into time-critical control systems, impacting decision making and operational response.

The technical set-up of ICS also carries inherent security challenges. Decisions about ICS software are often made not centrally by corporate IT but, rather, at the field or unit level, resulting in products from different solution providers, based on different technologies, and with different IT security standards. The decade-plus life cycle of wells and ICS systems and ongoing asset sales and purchases add to the diversity problem, making it challenging to account, standardize, upgrade, and retrofit these systems frequently. About 1,350 oil and gas fields globally, for instance, have been producing for more than 25 years, using systems and equipment from different vintages throughout that period. (Mittal, Slaughter, & Zonneveld, 2017)

Midstream

In its simplest terms, Midstream acts as a middleware between upstream and downstream and constitutes processes involving storage and transportation of oil. While extraction of crude oil is a part of upstream, midstream is all about shipping the oil retrieved in the former process to the downstream refinery facilities so that it can be finished into various consumable products.

Eyeing on OT/IT operations, vast networks of pipelines are constructed and maintained as a part of midstream industry for being transported and distributed to various downstream vendors. While IT risks are most common and talked about, industry experts need to be aware of transportation and pipeline security risks.

The most important risks menacing this domain are undetected spills, illegal pipeline tapping, and attacks on maritime transport. A spill might occur unintentionally, but illegal pipeline tapping and attacks on

maritime transport are often the results of malevolent actions. Some of the other risks in this area: Compliance violation, safety violation causing mass casualties or significant health effect, pipeline intrusion for quality and chemistry modification, production suspension by destroying pipelines. Needless to say, some of the above risks are not only monetary losses, but may bring catastrophic damages to mankind.

Downstream

The last segment of Oil and Gas industry, Downstream, consists of refineries that refines crude oil, purifies raw natural gas and ultimately distribute these products to end consumers. All consumable end products – gasoline, kerosene, diesel oil, jet fuel and so on are produced in the refineries and transported to various consumers.

As one might think, downstream sector is a convoluted network of industrial control systems used in refineries as well as digitalized IT networks to manage production, inventory and user accounts. Lack of defined security zones, and unsecure connections between zones can open doors to various vulnerabilities and remote code execution. Unauthorized access to refineries, remote third party contractors unsecure access can be some of the loose ends in the network.

An unauthorized access to a refinery whether physical or digital using software vulnerabilities can be detrimental. It could be used to steal process knowledge or intellectual property. One might disrupt or alter normal operations causing devastating damage to business.

When consider OT operations, there are all sorts of other risks – uptime and reliability of systems, insufficient human resources to manage physical security, industry regulations, and accessibility of data for demanding business goals.

What to protect

Its Patriot Act of 2001 defined critical infrastructure as those "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."
Due to the increasing pressures from external and internal threats, Oil and Gas organizations recognized as one of the 16 critical infrastructures, need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization’s size, threat exposure, or cybersecurity sophistication today.

Needless to say, not just the individual organizations but US economy cannot sustain a breach in our over the years built oil and gas network that has spread over 72,000 miles making it largest pipeline network in the world. In order to maintain functioning of this network, different kinds of hardware and softwares are involved ranging from sophisticated machinery to highly convoluted software(like fibre optics, drilling equipment, refineries, data visualization etc). As the industry in itself is moving towards highly data centric, and integrated management, higher are the risks involved in data and hardware security. Having a central management with the use of simulators and internet capabilities definitely makes the whole process lot more efficient and controllable. But at the same time a single loss of data breach can result into remote access of the entire network.

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the National Institute of Standards and Technology (NIST) developed a voluntary Framework for reducing cyber risks to critical infrastructure in February 2014. The voluntary Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure and was developed in response to Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" through collaboration between industry and government.
The Framework enables 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. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. (Technology, 2014)

As NIST Cyber security framework is generic and aim to advocate all kinds of industries looking for cyber security standards, this paper is entitled to focus on standards and policies that are applicable to Oil and Gas in specific, in addition to some other solutions.

Cybersecurity Framework

NIST breaks Cyber Security processes into 5 main stages as follows:

1. **Identify** – This stage focuses on the elements and activities, that are necessary to identify current state of the infrastructure. It helps in having a configuration system to bind systems, assets, data and capabilities all in one place
   Examples include – Asset Management, Risk assessment, Business Environment

2. **Protect** – Developing and implementing policies, standards, and software controls that are responsible for maintaining CIA(Confidentiality, Integrity and Availability) of the system
   Examples include - Access Control; Awareness and Training; Data Security; I

3. **Detect** – The stage is significant in providing mechanism to detect occurrence of a cyber security event like a data breach, data anomalies.
   Note: This stage is one of the crucial stages in Cyber Security framework. With the nature of current hacking techniques, it has been observed that it goes years when companies notice possibility of cyber hacks in their system. The time of hacker in the system is exponentially proportional to the level of damage and information loss that can occur.
   Examples include – Continuous Monitoring and Detection processes, Anomalies and Events

   While the first three stages help in developing a secure environment in place, the next two stages are more responding and recovering from the damage of an attack. The first three stages can be termed as "Prevention", while the next two are "Cure". The author strongly feels that former stages are absolute necessary as part of any organization, and once they implement them successfully, they can move to become a mature cyber organization by implementing the next two stages.

4. **Respond** – Develop activities and procedure to follow in case a cybersecurity event has been detected. The way it is different from the previous stage is – Detect consists of activities to help in identification of a cybersecurity event while this stage consist of activities to be done after an event has been detected to have minimum possible damage in terms of loss of assets, data and anything identified as secure.
   Examples include – Response Planning, Analysis, Mitigation

5. **Recover** – The last stage in the framework is to recover the damage that occurred because of the cybersecurity event. It supports timely recovery to normal operations to reduce the impact from a cybersecurity event.
   Examples include – Recovery planning, Improvements and Communications

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures. (Technology, 2014)

Following are the broad categories and sub-categories identified by NIST framework for a successful Cyber Security framework. The chosen table format doesn't imply a specific implementation order or importance of categories and sub-categories. A Category in itself is a broad focus area that consists of different sub-categories.

FUNCTION	CATEGORY	SUBCATEGORY
Identify(ID)	**Asset management (ID.AM)** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and

		communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
		ID.GV-4: Governance and risk management processes address cybersecurity risks
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
		ID.RA-3: Threats, both internal and external, are identified and documented
		ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical

		infrastructure and sector specific risk analysis
PROTECT(PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
		PR.AT-2: Privileged users understand roles & responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
		PR.AT-4: Senior executives understand roles & responsibilities
		PR.AT-5: Physical and information security personnel understand roles & responsibilities
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected **PR.DS-2:** Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production

		environment
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained
		PR.IP-2: A System Development Life Cycle to manage systems is implemented
		PR.IP-3: Configuration change control processes are in place
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
		PR.IP-6: Data is destroyed according to policy
		PR.IP-7: Protection processes are continuously improved
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: A vulnerability management plan is developed and implemented
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

	components is performed consistent with policies and procedures.	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
		PR.PT-2: Removable media is protected and its use restricted according to policy
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality
		PR.PT-4: Communications and control networks are protected
DETECT(DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2: Detected events are analyzed to understand attack targets and methods
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
		DE.AE-4: Impact of events is determined
		DE.AE-5: Incident alert thresholds are established
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
		DE.CM-4: Malicious code is detected
		DE.CM-5: Unauthorized mobile code is detected
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
		DE.CM-7: Monitoring for unauthorized personnel,

		connections, devices, and software is performed
		DE.CM-8: Vulnerability scans are performed
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2: Detection activities comply with all applicable requirements
		DE.DP-3: Detection processes are tested
		DE.DP-4: Event detection information is communicated to appropriate parties
		DE.DP-5: Detection processes are continuously improved
RESPOND **(RS)**	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed
		RS.CO-2: Events are reported consistent with established criteria
		RS.CO-3: Information is shared consistent with response plans **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		RS.AN-3: Forensics are performed
		RS.AN-4: Incidents are categorized consistent with response plans

	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned
		RS.IM-2: Response strategies are updated
RECOVER(RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed
		RC.CO-2: Reputation after an event is repaired
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

How to use the Framework?

Organization can use this framework to make a streamlined, systematic process in identification, assessment and management of Cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program. (Technology, 2014)

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Establishing or improving a Cybersecurity framework

The following steps demonstrate how this framework can be established or embedded into an existing IT/OT framework to develop effective Cybersecurity program. These steps should be repeated as necessary for continually improving CyberSecurity:

1. **Baseline measurement** – A detailed mapping of the current state of the network to be performed. It includes detailing of current policies, current security standards, points of entry to the network, risks associated, a consolidated list of software and hardware managed by the company, third party vendor applications and so on.

   The organization develops a Baseline by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved

   A pro tip: The best way to carry this is in the form of Risk Assessments. It is a proven tool to examine current state of any network and work as a starting point to find loop holes in the network.
   Please find an example of Risk Assessment in Appendix A

2. **Target measurement** – With stakeholders on board, set parameters for target cyber security state. Keep in mind, projects like these are directly proportional to cost and inversely proportional to risk. Set budgets, identify work to be done, think about the risks it is mitigating and long term prospects.

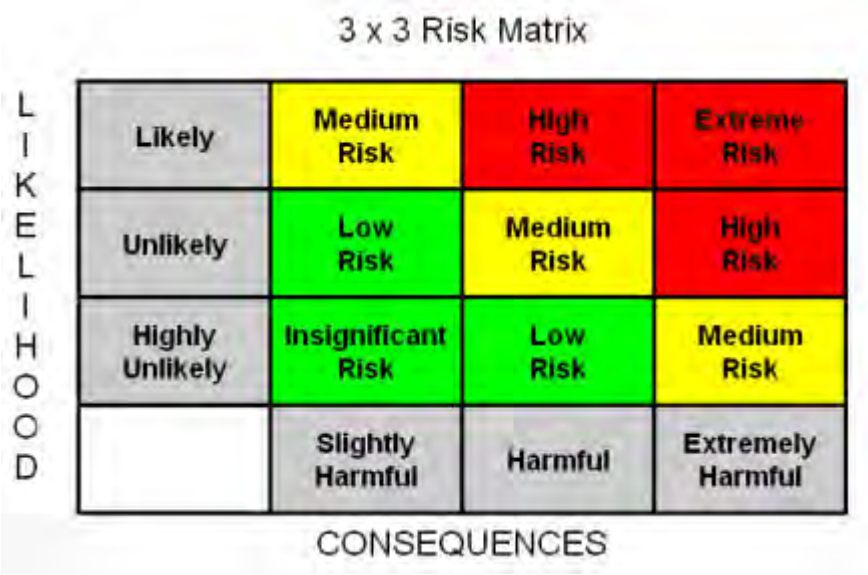
   The organization creates a Target measurement by assessing Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories in order to account for unique organizational risks.

3. **Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process -** In this step, the organization compares the baseline measurement with target measurement and identify gaps. Then it creates plans and target areas required to address these gaps. Once target areas are identified, the next step is to identify and prioritize them in accordance to Risk Assessment Matrix (RAM). A RAM is an effective way to categorize organizational targets by selecting the appropriate consequences if compromised with the probability of likelihood. The resulting Risk Rating helps in prioritizing targets in three main categories:

   - **High Risk** – Sign of critical infrastructure being affected if it is a high risk. Risk target should definitely be mitigated at all costs as early as possible
   - **Medium Risk** – Risk could be tolerated for short term, but efforts should be planned to

mitigate the risk target

- **Low Risk** – No immediate action required. The risk could also be avoided if not impacting business in longer run



(Risk assessment org, n.d.)

4. **Assess progress toward the target state** - This is the phase of actual implementation of risk mitigation. Based on the prioritized targets in the previous step, create a time plan, allocate resources, and assess step by step progress of the plan

5. **Communicate among internal and external stakeholders about cybersecurity risk** – This step is taken lightly and often neglected. Cybersecurity risk should be added in the list of business risks, not just IT risks, and any efforts made on it should be continuously well informed to all the stakeholders.

Conclusion

As the number of cyber enthusiasts are sky rocketing each day, there is practically no industry left untouched. Be it cars, alarm systems, traffic systems, medical devices like pacemakers, plane systems or critical infrastructures like power grids and dams, hackers have made their way in almost all the industries. Focusing on Oil and Gas network, the author feels there is strong need for the industry to adopt Cyber Security framework, in order to better prepare itself for the upcoming challenges and vulnerabilities.

According to recent studies on types of attacks, known but unmitigated vulnerabilities in the systems are among the highest cybersecurity risks faced by the organizations. The existing Cybersecurity forums and open source community have an exceptional coverage in providing day to day updates on new vulnerabilities, and ways to patch them. As an organization, it is imperative to have a framework in place in order to detect for these vulnerabilities in the infrastructure, and respond to them as quickly as possible using Cyber Security framework.

The Cyber Security framework discussed in this paper is a comprehensive way to tighten the security of any sized Oil & Gas organization, and emphasize on the specific needs of Oil & Gas organizations that may not be applicable to some other industries. The framework is not a care technical project, and thus can be easily embedded into the current architecture of any organization. Depending on the needs of the organization, the framework can be appended and implemented in different ways. There is not a right or wrong way to implement any security control defined in the framework, but the engineer should pay attention to the different use cases that have been discussed in every sub-category of this framework.

References

Digital, G. (n.d.). *IT and OT Converge and Conquer*. Retrieved from https://www.ge.com: https://www.ge.com/digital/blog/it-and-ot-converge-and-conquer

Harp, D. R., & Gregory-Brown, B. (n.d.). *IT OT Convergence - Bridge the gap*. Retrieved from https://ics.sans.org: https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

Intel. (n.d.). Retrieved from https://simplecore.intel.com: https://simplecore.intel.com/insight-tech/wp-content/uploads/sites/45/2017/07/LannerFig1.png

King, A. D. (1998). Inertial Navigation - Fourty Years of Evolution. *GEC Review, Vol 13, No. 3*, pp. 140 - 148.

Mittal, A., Slaughter, A., & Zonneveld, P. (2017, June 26). *Protecting the connected barrels Cybersecurity for upstream oil and gas.* Retrieved from https://dupress.deloitte.com: https://dupress.deloitte.com/dup-us-en/industry/oil-and-gas/cybersecurity-in-oil-and-gas-upstream-sector.html#endnote-sup-10

Polyakov, A. (2017, April). *Cyber Security Risks To Be Aware Of In The Oil And Gas Industries.* Retrieved from https://www.forbes.com: https://www.forbes.com/sites/forbestechcouncil/2017/04/03/cyber-security-risks-to-be-aware-of-in-the-oil-and-gas-industries/2/#331647a84031

Risk assessment org. (n.d.). *3 * 3 Risk Matrix*. Retrieved from https://www.risk-assessments.org: https://www.risk-assessments.org/risk-assessment-matrix-3x3.html

Sagnac, G. (1913). The luminiferous aether demonstrated by the effect of the wind relative to the aether in a uniformly rotating interferometer. *Comptes rendus de l'Academie des Sciences Vol.95*, 708-710.

Technology, N. I. (2014). *Framework for Improving Critical Infrastructure Cybersecurity* (Vol. 1.0).