ISSN: 0975-833X

Availableonlineathttp://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 12, pp.76865-76876, December, 2018

DOI: https://doi.org/10.24941/ijcr.35045.12.2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

PROTECTING "CYBERSECURITY & RESILIENCY" OF NATION'S CRITICAL INFRASTRUCTURE - ENERGY, OIL & GAS

***Anil Lamba**

Department of Computer Science, Charisma University, Turks and Caicos Islands

ARTICLEINFO

Article History:
Received 18th September, 2018
Received in revised form
15th October, 2018
Accepted 10th November, 2018
Published online 31st December, 2018

Key Words:
Smart grid, Cyber-Attacks, Vulnerabilities, Confidentiality, Availability, Integrity, Accountability, IDS, Cryptography, Network Security, Oil & Gas, Energy, Resiliency.

**Corresponding author: Anil Lamba*

ABSTRACT

Cyber-secure, resilient energy is paramount to the prosperity of the United States. As the experience and sophistication of cyber adversaries grow, so too must the US power system's defenses, situational awareness, and response and recovery strategies. Traditionally, power systems were operated with dedicated communication channels to large generators and utility-owned assets but network connectivity in today's industrial entities, including electrical utilities, has exposed many digital communication and control aspects to the threat of cyber-attacks. When forward-looking improvements including smart grid, smart meters and other advancements are considered, security is of foremost concern. In fact, governments around the world have recognized the existing vulnerability and need to protect the grid infrastructure. To solve the problem, regulations and standards are being developed to ensure that the proper security steps are taken. In addition, cyber attackers have targeted crude oil and natural gas (O&G) companies, with attacks growing in frequency, sophistication, and impact as the industry employs ever more connected technology. But the industry's cyber maturity is relatively low, and O&G boards show generally limited strategic appreciation of cyber issues. This research paper documents the current Cyber security gaps across Energy, Oil & Gas sector systems spread throughout US, highlights required security enhancements and recommendations to foster Cyber Security & Resiliency of our Critical Infrastructure.

***Citation: Anil Lamba,* 2018.** "Protecting "cybersecurity & resiliency" of nation's critical infrastructure - energy, oil & gas", *International Journal of Current Research*, 10, (12), 76865-76876.

INTRODUCTION

With rare exceptions, energy & utilities (Oil & Gas) do an excellent job of managing traditional types of risks facing their operations. However, cyber security is the one category of risk that remains stubbornly opaque and resistant to attempts to manage, monitor, and measure. Determining the likelihood and severity of cyber security risks, as well as the efficacy of approaches to mitigate them, continues to be a challenge.

Executive Summary: Protecting America's energy systems from cyber-attacks and other risks is a top national priority. This Cybersecurity Research report identifies collaborative actions to reduce cyber risks in the U.S. energy sector. This research identifies the goals, objectives, and activities that can be pursued to reduce the risk of energy disruptions due to cyber incidents. Reliable energy and power is the cornerstone of our advanced digital economy and is essential for critical operations in transportation, water, communications, finance, food and agriculture, emergency services, and more. Today, any cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. As nation-states and criminals increasingly target energy networks, the Federal Government must help reduce cyber risks that could trigger a large-scale or prolonged energy disruption. A multi-pronged approach to Cybersecurity preparedness is required. System operators must have the capacity to operate, maintain, and recover a system that will never be fully protected from cyber-attacks. Relevant issues that need to be addressed include cloud security, machine-to-machine information sharing, advanced Cybersecurity technologies, outcome-based regulation to avoid prolonged outages and increase system resilience, and international approaches to Cybersecurity.

Executive Order 13800 (EO 13800): In 2017, President Trump issued Executive Order (E.O.) 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" because the risks of cyber threats to critical infrastructure are perceived as a national security imperative. The growing anxiety among United States policy-makers, and the American energy sector in particular, about cyberattacks on the nation's energy infrastructure was vividly underscored recently in a front page article in The Wall Street Journal headlined, 'U.S. Officials Push New Penalties for Hackers of Electrical Grid. Widespread connection of Distributed Energy

Resources will increase digital complexity and attack surfaces, and therefore require more intensive Cybersecurity protection.

A Power Sector in Transition: A modern functioning society requires highly reliable electricity. Electric utilities are vulnerable to cyber and physical attack and will be more so in the next decade as utility systems have more digital and complex controls, and the same digital interconnectedness that increases efficiencies, increase risks. Connection of Distributed Energy Resources (DERs) will increase cyber vulnerabilities. Protecting a nation's electricity grid from widespread cyber or physical attack or electromagnetic pulses are important national security issues, and require wise risk-based analysis and planning by electric utilities. Utilities throughout the world need resilience and contingency planning, to contain and minimize the consequences of cyber and physical incidents.

Envisioning a Future with Distributed Energy Resources: Cybersecurity, Resilience, and Privacy: Cybersecurity threats to the distribution system can be expected to challenge the industry for many decades. Throughout the world, utilities and non-utilities that interact with the grid need resilient systems and must be prepared to contain and minimize the consequences of cyber incidents. In a National Cybersecurity Summit, DHS Secretary Kirstjen M Nielsen said, *'I believe that cyber threats collectively now exceed the danger of physical attacks against us'.*

The 'largest interconnected machine' in the world: To put the American threat into larger context, the US electricity grid, which has been referred to as the 'largest interconnected machine' in the world, consists of 'more than 7,000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of miles of low-voltage distribution lines. In June, the President's National Infrastructure Advisory Council, which includes many energy sector leaders, said, *'The US needs to prepare for a "catastrophic power outage"* possibly caused by a cyberattack. 'Given the interconnected nature of critical systems and networks, new broad-scale approaches are needed to adequately prepare for, and respond to, and recover from catastrophic disasters that can create significant power outages with severe cascading impacts to multiple critical sectors.

The crippling of Ukrainian utilities: US electric utilities are not the only ones to have been targeted by cyber attackers. According to reporting in The Wall Street Journal, *'Cyber hackers working for Russia crippled three Ukrainian utilities on Dec. 23, 2015, plunging hundreds of thousands of civilians into the darkness on a chilly winter's eve'.*

Growing Concern: Most Americans probably don't give a lot of thought to critical infrastructure, even though it's something they rely on every day. The industry sectors that encompass the nation's critical infrastructure cover virtually every aspect of people's lives, including power generation, oil, gas, and manufacturing — to name a few. In this digital era, securing the networks, systems and data in these sectors is of vital importance. But as the numerous compromises of the past few years have shown, a lot of work needs to be done to protect critical infrastructure organizations against increasingly sophisticated and targeted attacks.

This research report & whitepaper offers best practices that can help IT and security executives at these organizations deliver the protection they need.

What is critical infrastructure and why is it so vital?: Critical Infrastructure represents a national security vulnerability that is not within the direct purview of the U.S. government. *Any cyberattack against an organization that provides critical infrastructure products or services presents a potentially significant risk to the American public.* According to the U.S. Department of Homeland Security (DHS), the nation's critical infrastructure *"provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health.* We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family." In all, *the DHS considers 16 sectors to be part of the critical infrastructure.* These include, but are not limited to, chemicals, communications, defense, emergency services, *energy*, food and agriculture, government, healthcare, manufacturing, and transportation. The incapacitation or destruction of systems and networks operated by organizations in these industries could have a debilitating and potentially monumental impact on other business or government agency Cybersecurity systems, economic security, national public health or safety, or any combination thereof, according to DHS. *For example*, if the power grid for part or all of the country were to be shut down for a substantial period, that would affect hundreds of millions of individuals as well as businesses and other organizations throughout the world. In December 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers. The disruption was due to a third party's illegal entry into and attack against its computer and SCADA systems. *The outages caused about 225,000 customers across various areas to lose power.* The power grid breach provides a real-world example of how critical infrastructure attacks can cause large-scale disruption, and illustrates how similar incidents could happen elsewhere without adequate protection in place. Organizations also must deal with the challenge of having their operational technology (OT) connected to their IT networks and systems, putting both at risk of attacks that were not previously possible.

Key Challenges of Cybersecurity & relevant high-level recommendations

Cybersecurity Preparedness

- Increasing sophistication and frequency of cyber threats on a growing attack surface. The network environment has grown with the increased deployment of new digital devices (e.g. the internet of things (IOT)) that are located outside the physical boundary the department. These devices potentially introduce a greater variety of cyber-attack vectors.
- Monitoring capabilities of the critical data streams and communications pathways in networks must be bolstered to identify and ultimately disrupt emerging cyber-attacks.
- Meeting stringent privacy and security requirements while exchanging data - Real-time threat monitoring and analysis often requires exchanging sensitive data from operating environments, triggering privacy and liability concerns.
- Real-time threat monitoring requires technical products and assessments that meet the requirements of systems and ensure protection of sensitive data.

- Effective assessments require specialized expertise - Effective assessment of Cybersecurity risks and capabilities requires consistent, industry-accepted tools and best practices.
- Departmental Element sites, particularly smaller sites may lack the skills and resources on staff to conduct assessments and prioritize mitigations without tools and resources.
- Information sharing requires processes in place prior to the threat - Vital information concerning high-level Cybersecurity threats and risks is often classified. This makes it difficult to distribute the information widely if partners lack clearances and if information sharing processes are not in place prior to an event or threat.
- More efficient processes are needed to identify and prioritize private-industry partners who have a "need to know" and grant them appropriate security clearances.

Incident Response and Recovery

- Coordinating roles among many diverse stakeholders - Federal support of Cybersecurity and incident response cuts across multiple government agencies and disciplines, from intelligence, to law enforcement, to emergency response.
- National leadership is needed to avoid issues such as conflicting roles and responsibilities and activities that are redundant or poorly aligned.
- Developing flexible, adaptable procedures - Cyber threats evolve quickly, and government hierarchies may not be well-suited for a rapid reprioritization of activities.
- Continuous coordination across the Federal Government is required to unify national efforts and limit the strain on the private sector of partnering with multiple departments and agencies.
- Coordinating geographically dispersed and diverse functional resources - Unlike many physical events, cyber events may affect infrastructure across a wide geographic area, and the consequences of an incident may be different for each affected system.
- Cyber incident response also may require a different set of resources, personnel, and skills than traditional energy disruptions. Some of these skills may not be included in traditional incident response procedures and training and may not be frequently tested.

Resilient Systems

- New solutions must support the business case - Develop Cybersecurity tools and technologies that are economical, cost effective, and support operations, effectively making the system easier and less expensive to operate.
- Diverse legacy and modern devices - Cybersecurity solutions must integrate with existing systems that often contain a mix of new and legacy devices, a mix of platforms and vendors, and devices with different levels of computational and communications resources available to support Cybersecurity measures.
- Solutions from diverse vendors and third-party providers must interoperate - New tools and technologies must be built to common standards to allow devices from different vendors to connect and operate without issue.
- Interoperable Cybersecurity solutions require common standards development.
- Securing devices sourced from a global supply chain - Departmental Elements must ensure the integrity of the system hardware, firmware, and software components as they traverse the supply chain.
- Anticipating security in the future grid - Designing future systems with built-in cyber resilience requires anticipating future cyber threat scenarios and protection requirements.
- Meeting the growing demand for Cybersecurity professionals - To manage and defend increasingly complex and sophisticated cyber systems, universities must build the nation's Cybersecurity workforce.
- The current workforce increasingly faces heavy workloads, a shortage of critical skills, and constantly evolving expertise needs.

Case Study 1 - Smart Grid's Cyber Security

"Types of Attacks, their Impact and Proposed Countermeasures"

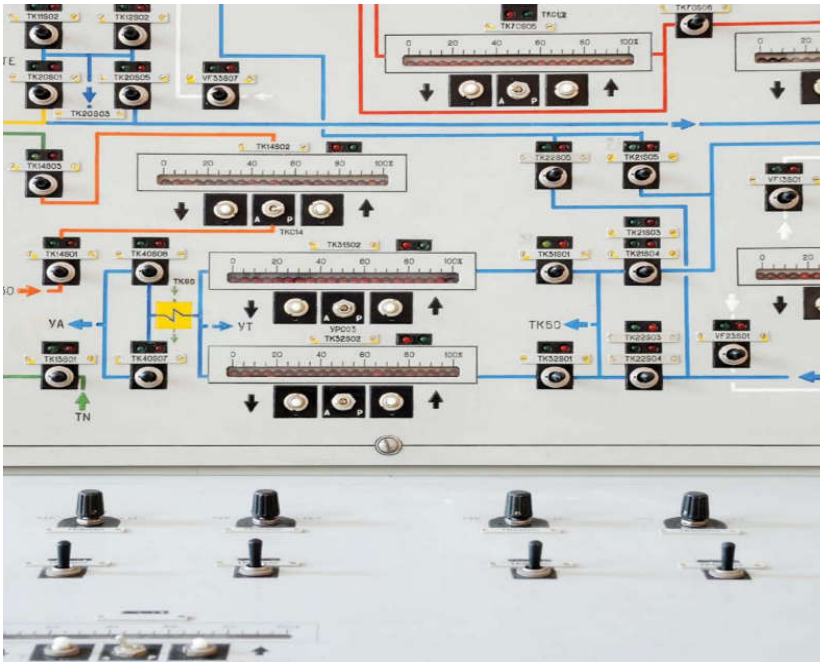
Introduction

Smart grid uses the power of information technology to intelligently deliver energy to customers by using a two-way communication, and wisely meet the environmental requirements by facilitating the integration of green technologies. Although smart grid addresses several problems of the traditional grid, it faces a number of security challenges. Because communication has been incorporated into the electrical power with its inherent weaknesses, it has exposed the system to numerous risks. Any interruptions in power generation could disturb smart grid stability and could potentially have large socio-economic impacts. The purpose of this paper is to review the security requirements and investigate in depth a number of important cyber-attacks in smart grid to diagnose the potential vulnerabilities along with their impact. In addition, I propose a cyber security strategy as a solution to address breaches, counter attacks, and deploy appropriate countermeasures. Finally, some future research directions are shared.

Security Attacks and Countermeasures in Smart Grid

Smart grid attacks: In general and as shown in Fig. 3, there are four steps used by malicious hackers to attack and get control over a system, namely reconnaissance, scanning, exploitation, and maintain access.

- During the first step, reconnaissance, the attacker gathers and collects information about its target.
- In the second step, scanning, the attacker tries to identify the system's vulnerabilities. These activities aim to identify the opened ports and to discover the service running on each port along with its weaknesses.
- During the exploitation step, he/she tries to compromise and get a full control of the target.
- Once the attacker has an administrative access on the target, he/she proceeds to the final step which is, maintaining the access.



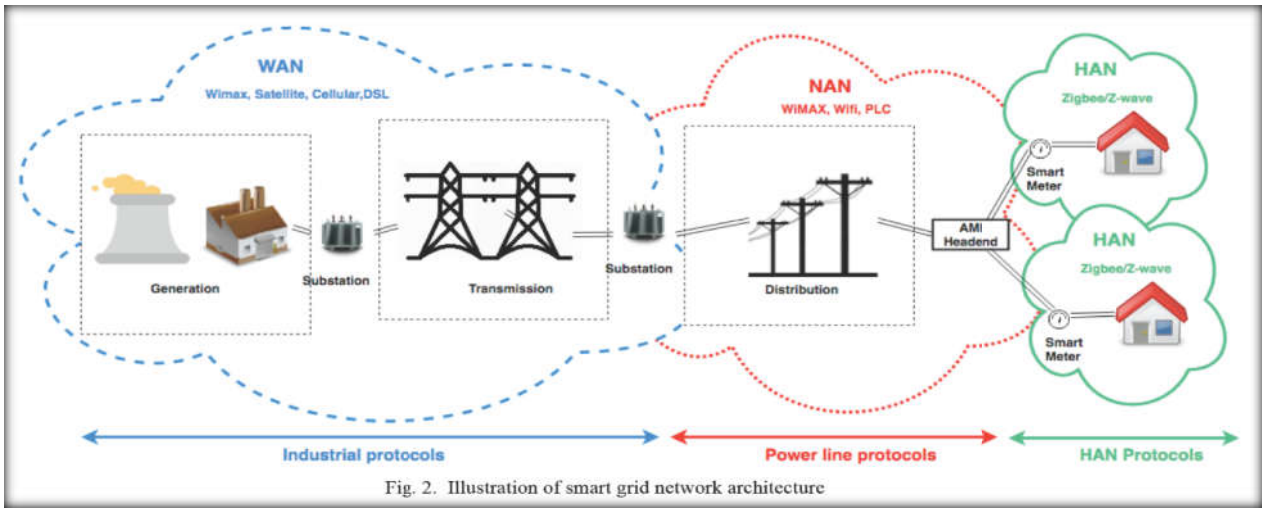
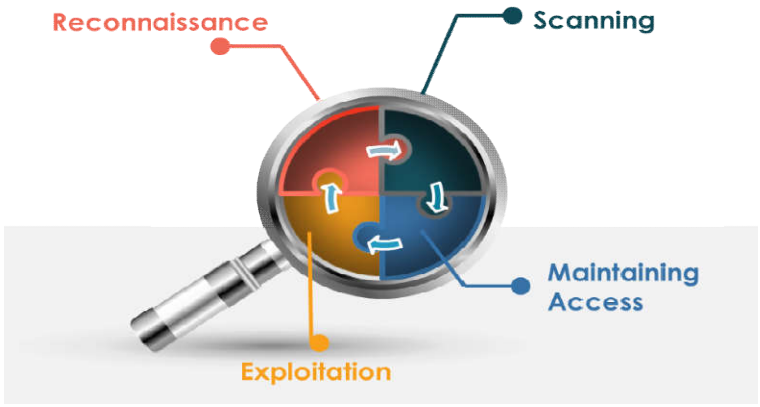


Fig. 2. Illustration of smart grid network architecture



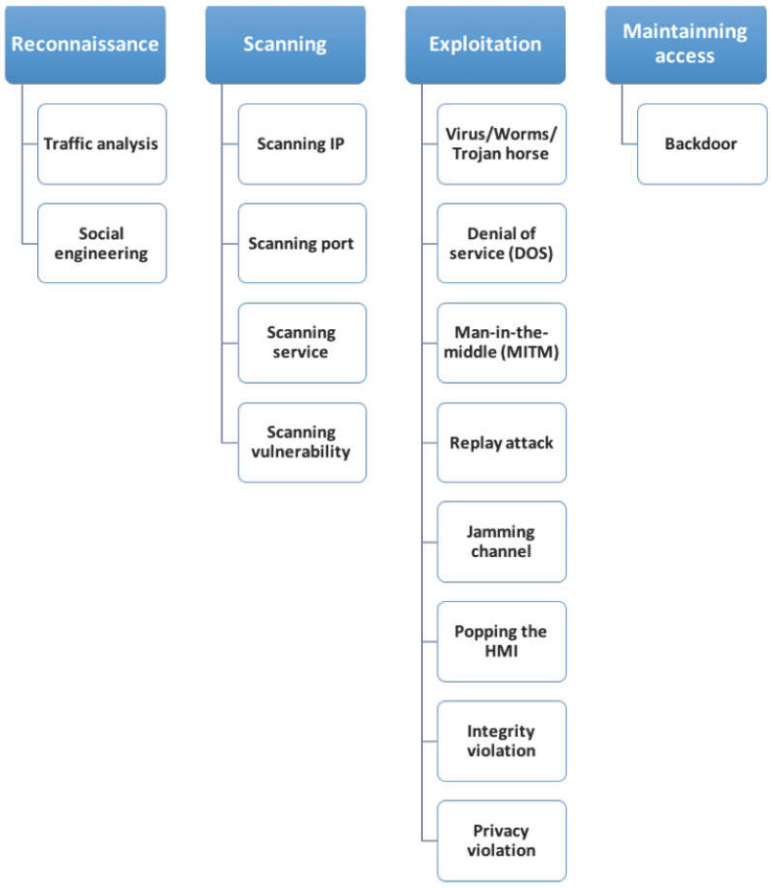


Fig. 4. Types of attacks across various steps

Table 2. Shows the likelihood of each attack to be performed and its associated level of severity

		Severity of the Attack		
		Low	Medium	High
Likelihood of the attack to be performed	High	- Traffic analysis - Privacy violation		- Virus, worms, Trojanhorse - DOS - Backdoor
	Medium	- Social engineering - Scanning	- MITM - Replay attack	- Jamming channel - Masquerade attack - Integrity violation
	Low			- Popping the HMI

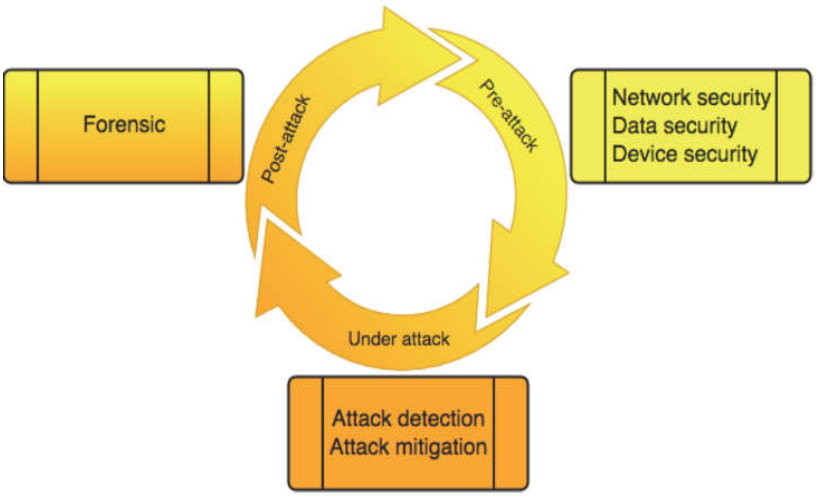


Fig. 5. Cyber security strategy for smart grid

Fig. 4. Cyber Attacks in Smart Gird, Their Impacts and Countermeasures

Attacking Cycle Step	Attack Category (Attack Example)	Compromised smart grid's application /protocol	Compromised Security's Parameter	Possible Countermeasures
Reconnaissance	Traffic analysis Social engineering (Phishing, Password pilfering)	Modbus protocol, DNP3 protocol	Confidentiality	Secure DNP3, PKI (SKMA, SMOCK), TLS, SSL, Encryption, Authentication
Scanning	Scanning IP, Port, Service, Vulnerabilities (Modbus network scanning, DNP3 network scanning)	Modbus protocol, DNP3 protocol	Availability	IDS, SIEM, Automated security compliance checks
Exploitation	Virus, worms, Trojan horse (Stuxnet, Duqu)	SCADA PMU, Control device, SCADA	Confidentiality Integrity Availability Accountability	DLP , IDS , SIEM, Antivirus , Diversity , technique
	Denial of service (DOS) (Puppet attack, TDS, TSA)	AMI Instability of smart grid systems, PMU, smart grid equipment's GPS	Availability	SIEM, IDS, flow entropy, signal strength, sensing time measurement, transmission failure count, pushback, reconfiguration methods
	Man-in-themiddle (MITM) (Eavesdropping attack , Intercept/ alter)	HMI, PLC SCADA DNP3, SCADA AMI	Confidentiality Integrity	Secure DNP3, PKI (SKMA, SMOCK) [7], TLS, SSL, encryption, authentication
	Replay Attack	Authentication scheme in AMI	Confidentiality Integrity	Secure DNP3, TLS, SSL, encryption, authentication[1] PKI (SKMA, SMOCK) [7],
	Jamming Attack (MAS-SJ)	PMU CRN in WSGN	Availability	JADE, anti-jamming (FHSS, DSSS)
	Popping the HM1	SCADA, EMS, Substations	Confidentiality Integrity Availability Accountability	DLP, IDS , SIEM , Antivirus, automated security compliance checks
	Masquerade attack	PLC	Confidentiality Integrity Availability Accountability	DLP, IDS, Secure DNP3, SIEM, TLS, SSL, encryption, authentication, PKI (SKMA, SMOCK)
	Integrity violation (FDI)	Smart meter, RTU EMS, SCADA, AMI	Confidentiality Integrity Availability Accountability	DLP, IDS ,SIEM, Secure DNP3, TLS, SSL, encryption, authentication, PKI (SKMA, SMOCK)
	Privacy Voilation	Demand Response program, Smart meters.	Confidentiality	Secure DNP3, PKI (SKMA, SMOCK)[7], TLS, SSL, encryption, authentication
Maintaining access	Backdoor	SCADA	Confidentiality Integrity Availability Accountability	IDS, SIEM,Anti-virus , Diversity technique

This step is achieved by installing a stealthy and undetectable program; thus he/she can get back easily to the target system later. In smart grid, the same steps are followed by attackers to compromise the security's criteria. During each step, they use different techniques to compromise a particular system in the grid. Thus, attacks can be classified based on these steps.

Reconnaissance: The first phase, reconnaissance, includes the attacks: social engineering and traffic analysis. Social engineering (SE), relies on social skills and human interaction rather than technical skills. An attacker uses communication and persuasion to win the trust of a legitimate user and get credential and confidential information such as passwords or PIN number to log on into a particular system.

Scanning: Scanning attack is the next step used to discover all the devices and the hosts alive on the network. There are four types of scans: IPs, ports, services, and vulnerabilities. Generally, an attacker starts with an IPs scan to identify all the hosts connected in the network along with their IP addresses. Next, he or she goes deeper by scanning the ports in order to determine which port is open. This scan is executed on each discovered host on the network. The attacker then moves on to the service scan in order to find out the service or system running behind each opened port. For instance, if the port 102 is detected open on a particular system, the hacker could infer that this system is a substation automation control or messaging. If the port 4713 is open, the target system is a Phasor Measurement Unit (PMU). The final step, vulnerabilities scan, aims to identify the weaknesses and vulnerabilities related to each service on the target machine to exploit it afterward. Modbus and DNP3 are two industrial protocols vulnerable to scanning attacks. Given that Modbus/TCP was designed for communication rather than security purpose, it can be compromised by an attack called Modbus network scanning. This attack consists of sending a benign message to all devices connected in the network to gather information about these devices. Modscan is a SCADA Modbus network scanner designed to detect open Modbus/TCP and identify device slave IDs along with their IP addresses. It is recommended to scan the DNP3 protocol and discover hosts, specifically, the slaves, their DNP3 addresses, and their corresponding master. As one can see, these attacks target mainly the confidentiality of the smart grid.

Exploitation: The third step, exploitation, includes malicious activities that attempt to exploit the smart grid component's vulnerabilities and get the control over it.

These activities include viruses, worms, Trojan horses, denial of service (DOS) attacks, man-in-the-middle (MITM) attacks, replay attacks, jamming channels, popping the human machine interface (HMI), integrity violations, and privacy violations.

Here is a brief about all 16 types of attacks on smart grid

A virus is a program: used to infect a specific device or a system in smart grid. A worm is self-replicating program. It uses the network to spread, to copy itself, and to infect other devices and systems. A Trojan horse is a program that appears to perform a legitimate task on the target system. However, it runs a malicious code in the background. An attacker uses this type of malware to upload a virus or worm on the target system.

In denial of service (DOS) attacks: Several methods are used, particularly SYN attacks, buffer overflow, teardrop attacks, and smurf attacks, puppet attack, time-delay-switch (TDS), and time synchronization attack (TSA). A SYN attack exploits the three-way handshake (SYN, SYN-ACK, ACK) used to establish a TCP session. The attacker floods a target system with connection requests without responding to the replays, forcing the system to crash. The Modbus/TCP protocol is vulnerable to these attacks since it operates over TCP.

In buffer overflow attack: The attacker sends a huge amount of data to a specific system, thereby exhausting its resources. For example, the ping-of-death is considered as a buffer overflow attack as it exploits the internet control message protocol (ICMP) by sending more that 65K octets of data. It then makes the system crash.

In a teardrop attack: An attacker alters and modifies the length and the fragmentation offset fields in sequential IP packets. Once the target system receives these packets, it crashes because the instructions on how the fragments are offset within these packets are contradictory.

In smurf attack: The attacker targets not only a specific system, but it can saturate and congest the traffic of an entire network. It consists of three elements: the source site, the bounce site, and the target site. For source site, the adversary sends a spoofed packet to the broadcast address of the bounce site. These packets contain the IP address of the target system. Once the bounce site receives the forged packets, it broadcasts them to all hosts connected to the network and then causes these hosts to replay, saturating the target system.

In puppet attack: Targets the advanced metering infrastructure (AMI) network by exploiting a vulnerability in dynamic source routing (DSR) protocol and then exhausting the communication network bandwidth. Due to this attack, the packet delivery drops between 10% and 20%.

The time-delay-switch (TDS) attack: Consists of introducing a delay in control system creating instability in the smart grid system.

The time synchronization (TSA) attack: Targets mainly the timing information in smart grid. Because power grid operations such as fault detection and event location estimation depend highly on precise time information, and also most of the measurement devices in smart grid are equipped with global positioning system (GPS), attack such as TSA, which spoof the GPS information, could have a high impact on the system. DOS represents a significant threat to the smart grid system because communication and control messages in such a system are time critical, and a delay of few seconds could compromise the system availability.

The man-in-the-middle (MITM) attack: Is performed when an attacker inserts itself between two legitimate devices and listens, performs an injection, or intercepts the traffic between them. The attacker is connected to both devices and relays the traffic between them. These legitimate devices appear to communicate directly when in fact they are communicating via a third-device.

Intercept/alter attack: Is another type MITM attack. It attempts to intercept, alter, and modify data either transmitted across the network or stored in a particular device. For example, in order to intercept a private communication in advanced metering infrastructure (AMI), an attacker uses electromagnetic/radio-frequency interception attack.

avesdropping attack is also another MITM attack's type, where the attacker intercepts private communications between two legitimate devices. All these MITM attacks attempt to compromise the confidentiality, the integrity, and the accountability.

In replay attack: As the industrial control traffic is transmitted in plain text, an attacker could maliciously capture packets, inject a specific packet, and replay them to the legitimate destinations, compromising then the communication's integrity. Intelligent electronic device (IED), which is a device designed for controlling and communicating with the SCADA system, could be targeted by replay attacks so that false measurements are injected in a specific register. Replay attack could also be used to alter the behavior the programmable logic controllers (PLC). In AMI, where an authentication scheme is used between smart meters, a replay attack involves a malicious host to intercept authentication packets sent from smart meter and re-sending them at a later point in time, expecting to authenticate and gain unauthorized entry into the network.

In the jamming channel attack: An adversary exploits the shared nature of the wireless network and sends a random or continuous flow of packets in order to keep the channel busy and then prevents legitimate devices from communicating and exchanging data. Due to its time-critical nature, smart grid requires a highly available network to meet the quality of service requirements and such an attack can severely degrade its performance.

Popping the HMI is an attack: That exploits a known device's vulnerability, especially device's software or OS vulnerabilities, and then installs a remote shell, allowing the attacker to connect remotely to the server from his computer to get unauthorized access in order to monitor and control the compromised system. SCADA systems, substations, or any system running an operation system with a console interface is considered as a potential target of this attack.

In the masquerade attack: A malicious person may pretend to be a legitimate user in order to gain access to a system or gain greater privileges to perform unauthorized actions. attack could tamper with the programmable communicating thermostat (PCT) which is used to reduce electric power at a residential site. It compromises the availability, integrity, confidentiality, and accountability of the system.

Integrity violation attacks: Aim to violate the integrity and/or the accountability of the smart grid by altering intentionally or unintentionally the data stored in a given device in the network. For instance, a customer could perform this attack to alter the smart meter data in order to reduce his electricity bill.

Privacy violation attack: Aims to violate privacy by collecting private information about customers. For example, as smart meters collect electricity usage many times per hour, information about the user electricity's consumption could be obtained. Thus, if a meter does not show electricity usage for a period of time, that commonly indicates that the house is empty. This information could then be used to conduct a physical attack like burglary.

Maintaining access: In the final step, maintaining access, the attacker uses a special type of attack to gain permanent access to the target, especially backdoors, viruses, and Trojan horses. A backdoor is an undetectable program, stealthy installed on the target to get back later easily and quickly. If the attacker succeeds in embedding a backdoor into the servers of the control center of the SCADA, he or she can launch several attacks against the system which can cause a severe impact on the power system. Since the devices' vulnerabilities documentation are publicly available, a hacker may simply use open source tools such as MetaSploit and Meterpreter to launch such an attack. Therefore, this attack has high severity and it is very likely to be performed.

Smart grid countermeasures: A number of attack detection and countermeasure techniques are proposed in the literature to counter cyber-attacks. Security solutions today contribute to the smart grid's security however, they are insufficient to face sophisticated and blended attacks. We believe that security cannot be achieved through one specific solution, but by deploying several techniques incorporated into a global strategy. In this section, and as Fig. 5 shows, we propose a cyber security strategy composed of three phases: pre-attack, under attack, and post-attack. As follows, and for each phase, relevant published solutions in terms of security protocols, security technology, cryptography, and other cyber-attack countermeasures are described.

Pre-attack: During this first phase, pre-attack, various published solutions are recommended to enhance the smart grid's security and to be prepared for any potential attack. Security countermeasures commonly fall into three categories, namely network security, cryptography, and device security.

Network security: Firewalls should be associated with other security technologies such as intrusion detection system (IDS), security information and event management systems (SIEM), and network data loss prevention (DLP). This secured version named secure DNP3 added a secure layer for encryption and authentication between the TCP/IP and application layer. *Using such a protocol, several attacks can be avoided,* for example, authentication mechanism can protect against MITM attack, whereas encryption decreases eavesdropping and replay attacks. Network DLP is a system responsible for preventing the loss or the theft of the data across the network. In addition to these security systems, secure network protocols such as IPsec, transport layer security (TLS), secure sockets layer (SSL), Secure DNP3 can also be used to enhance security in the network.

Cryptography for data security: Encryption mechanisms aim to ensure data's confidentiality, integrity, and no nrepudiation. There are two types of key encryptions: symmetric and asymmetric. In symmetric key encryption, or single-key encryption, one key is used to encrypt and to decrypt data. Asymmetric key encryption, on the other hand, uses two keys to encrypt and decrypt data: private key and public key. Both symmetric and asymmetric key encryption can be used, and the selection depends on several factors, including data criticality, time constraints, and computational resources. Key management is a crucial approach for encryption and authentication. Public key management (PKI), or shared secret key management, can be used to ensure authenticity for communication across networks. Due to the distributed nature of smart grid, some specific requirements should be considered to design a cryptography key management, particularly efficiency, evolve-ability, scalability, and secure management.

The choice of a framework relies on different criteria, including scalability, computational resource capability, and support for multicast.

Device security: Device protection is the third crucial element in the supply chain of smart grid security. In several security technologies have been recommended, particularly, host IDS, anti-virus, and host data loss prevention (DLP) along with an automated security compliance check. Such a tool performs a check against all smart grid components to verify that each device's configuration is up to date, especially the device's firmware and the current configuration file. As the smart grid components are highly connected and a weakness in one component can expose the entire system to risk, a compliance check is a crucial tool.

Defense-in-Depth: Defense-in-depth is the concept of layering multiple security features within the network such that the system is no longer attractive to would be attackers. Network operators must deploy intrusion detection systems, intrusion prevention systems, and DMZs, on control networks and use protection mechanisms such as moving target defense, protected (enclaved) computing, obfuscation, and other defense-in-depth techniques (e.g. cryptography, privilege zones, etc.).

Based on the DHS defense-in-depth recommended practice, *the five key countermeasures for networks are:*

- Identify, minimize, and secure all network connections.
- Harden the network and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.
- Continually monitor and assess the security of systems, networks, and interconnections.
- Implement a risk-based defense-in-depth approach to secure systems and networks.
- Manage the human element—clearly identify requirements for networks; establish expectations for performance; hold individuals accountable for their performance; establish policies; and provide PV network security training for all operators and administrators.

These countermeasures should be incorporated at the device and network levels to secure the communications system.

Additional Best Practices and Strategies: These best practice technologies, processes, and operational protective strategies can reduce the risks to the distribution grid.

With appropriate application, the risk of a major service outage resulting from a breach within the distribution grid can be minimized, if not eliminated, by following established best-practices and protocols.

The following suggested best practices and strategies can be taken to reduce risks:

•***Changing default passwords:*** Standard protection solutions offered today on workstations and servers need to be extended to distributed energy devices. Device manufacturers should employ a technology that requires changing default passwords when a device is first connected. This requirement could also be integrated into existing standard processes, such as generator interconnection or permitting. A significant share of successful cyber incursions occur through unchanged factory default passwords.

•***Maintenance of passwords:*** In addition to changing default passwords, it is important to remove access to existing or old passwords for users who should no longer have access. Often, employees and service providers will save passwords for future access. These passwords can be compromised, depending on how they are stored, and they can also be used by the bearer for unauthorized access.

•***Updating malware and software protection:*** All parties must accept that they have a responsibility to ensure software patches and malware protection are kept up-to-date on all devices, regardless of regulatory mandate. Requirements such as these could be integrated into UL 1741 listing requirements.

•***Encrypting messages:*** Encryption solutions with minimal resource requirement and high protection should be chosen. When utilizing encryption, the latest NIST standards should be followed. Endpoint devices should not share secret and/or private keys.

•***Firmware protective measures:*** At the device level, firmware should be signed by the device manufacturer and it should not be possible for unsigned firmware to be loaded into the device.

•***Isolation:*** Network segmentation with distinct security enclaves and enabling groups of devices to interact by securely sharing a certificate, such that the DER resource can communicate to other devices on the premise.

•***External interface protection limitations:*** Interfaces should be disabled at the operating system level and not available for use unless specifically activated. Applications or operating systems (OS) that run on the device should have the ability to be securely updated or patched as needed.

•***Penetration testing:*** Comprehensive penetration testing should also be done prior to release and periodically thereafter to validate that no vulnerabilities have been introduced.

•***Customer data protection:*** Platforms should incorporate strict requirements to address issues ranging from secure transfer and storage of customer information to authentication protocols when interacting with devices and utility systems.

Only essential information should be collected by platforms (i.e., name, email, address, time zone, Wi-Fi name (SSID), device IP address). Personally Identifiable Information and device-related information should be stored on a hardened and encrypted server with multiple layers of security control.

•***Third-party cloud security:*** Cloud vendors utilized by these platform providers should be fully compliant with applicable security standards and undergo periodic Statement on Standards for Attestation Engagements (SSAE) auditing.

•***Incorporating:*** such communication protocols and end-to-end encryption for server storage and data access prevents the device or the network itself from being exploited by packet sniffing, IP spoofing, and Man-in-the-Middle attacks.

•***Reliable operations:*** Network redundancy methods should be employed for data storage, distributed across multiple servers, to ensure 24/7 availability of data. All data changes should be logged into an audit trail, by capturing the user, date and time of the change, and the application that was used (e.g., web or mobile). Databases used must be backed up using a method that was designed for high availability.

•***User security measures:*** Energy platforms must utilize role-based access controls in accessing application functions and data access within the software platform, log all events for reporting purposes, and require multi-factor authentication for all users.

These recommendations must be balanced against the high cost of Cybersecurity attacks. Cybersecurity practices for advanced and intelligent distribution grids should be developed and deployed in a manner that enables, rather than constrains, innovation and advancement in energy technology.

Under attack: This step is divided into two tasks: *attack detection and attack mitigation*. Several approaches and technologies can be used during each task, to detect the malicious activity, and then deploy the appropriate countermeasures.

During the attack detection, all the deployed security technologies are recommended, including SIEMS, DLP, and IDS. But, some of these solutions have a number of limitations and need improvements, particularly IDS as it has high rate of false positives. The IEC61850 IDS was capable of detecting many attacks such as a DOS attack, a password cracking attack, and an ARP packet sniffer attack. The combination of two classifiers SVM and AIS have produced satisfactory results in terms of detection malicious traffic. *Once the attack are detected*, mitigation can be executed using the following methods. In pushback method, the router is configured to block all the traffic coming from the attacker's IP address. In the reconfiguration method, the network topology is changed to isolate the attacker. For jamming attacks, anti-jamming schemes such as frequency hopping spectrum spread (FHSS) and direct sequence spectrum spread (DSSS) are advised to mitigate attacks.

Post-attack: When an attack is not detected, such as in the case of Stuxnet, the post-attack period is an important step. Forensic analysis is the primary technique used during the post-attack. Smart grid forensic studies collect, analyze, and intercept digital data in order to identify the entity involved in the event. They are also useful to determine and address cyber and physical vulnerabilities of the smart grid in order to anticipate potential attacks. In addition, forensic analysis in smart grid plays an important role in the investigation of cyber-crimes such as hacking, viruses, digital espionage, cyber terrorism, manipulating the operation of the smart grid, violating the consumer's privacy, and stealing valuable information including intellectual property and state secrets. Fig. 4 below illustrates the category of attacks during each step, compromised smart grid's application or protocol, compromised security's parameter and possible countermeasures.

Challenges and Future Direction: In heterogeneous systems such as smart grid, different devices coexist and communicate through various network protocols. This heterogeneity represents a great challenge and a potential threat for the smart grid security. Furthermore, *the majority of industrial network protocols used in smart grid such as, DNP3, ICCP, Modbus, and Profibus were designed for connectivity but not for security purposes.* Thus, these protocols cannot ensure a secure communication channel, in addition, they may also be used as an attack surface. Though there are some secure version of many industrial protocols, such as secure DNP3. However, the problem with this new version is its incompatibility with legacy installations. In addition to network protocols, operating systems and physical equipment in smart grid may be vulnerable and expose the system to a wide variety of attacks. I believe that smart grid cyber-attacks may be mitigated more effectively by combining several security mechanisms through a cyber security strategy. Such a strategy have several benefits, including, addressing the system's vulnerabilities, detecting a number of cyber-attacks, deploying the appropriate countermeasures, and identifying the involved entity.

Conclusion

Smart grid is a system composed of distributed and heterogeneous components to intelligently deliver the electricity and easily integrate the renewable technologies. However, this critical system suffers from a number of security weaknesses. In this study, a comprehensive overview of Cybersecurity in smart grid and investigate in depth the main cyber-attacks threating its infrastructure, its network protocols, and its applications is provided. In addition, *I have proposed a strategy composed of possible countermeasures designed to address potential components' vulnerabilities, detect malicious activities, enhance communication security in the network*, and protect the customer's privacy.

Introduction

This report 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 risk-based security policies for stakeholders. As a critical infrastructure, the oil and gas industry faces additional risks beyond those in many organizations. In addition to the intellectual property that any company must protect in its corporate Risk Management Framework, *threats to the oil and gas infrastructure also put at risk the physical wellbeing of people and the environment as well as the national security.* 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. 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

In a recent study from the Ponemon Institute – The State of Cybersecurity in the Oil & Gas Industry: United States it was reported that, on average, *46 percent of cyber-attacks are*

believed by respondents to go undetected, and nearly 70 percent of oil and gas companies were hacked in the past year. Cyber-attacks in the oil and gas industry can have catastrophic effects on the economy and to national security. Many of the recent attacks on Oil & Gas operational technology (OT) infrastructure, or Industrial Control Systems (ICS), resulted in the loss of confidential exploration and production information.

However, compromise and malicious hacking of OT in critical infrastructure may also result in the following:

- Reportable Safety Incidents from Harm to Operators
- Utility or Power Interruption to Production Facilities
- EPA Compliance Violations
- Plant Sabotage/Shutdown
- Equipment Damage
- Production Disruption
- Lower Product Quality

Only 41 percent of respondents claimed that their organizations have continuous monitoring set up on their OT infrastructure and that they are still in the early to middle stages of cyber security maturity.
Most of the respondents felt that OT is at greater risk than the IT environment, and many organizations are now outsourcing OT security operations because they do not have the expertise internally.

Current State of Cybersecurity: According to a study by Frost & Sullivan, *"Global Oil and Gas Infrastructure Security Market Assessment," the total oil and gas infrastructure security market is predicted to increase from $18 billion dollars a year in 2011 to $31 billion dollars by 2021.* Despite this spending, the ABI Research study describes the process Control Networks (PCN) in many oil and gas companies as "poorly protected against cyber threats… at best, they are secured with IT solutions which are ill-adapted to legacy control systems such as PCN." 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.

"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."

Steps for Addressing Security: Here is the orderly set of steps that can be used to help apply proposed recommendations to help accelerate the specific cyber 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-levelreview 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 beenestablished, 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

- 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 thedesired 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.

Additional Measures for oil and gas organizations: Oil and gas organizations have the broad experience necessary to manage and support complex operations linked by large-scale networks and with many points of ingress and egress. They should apply this experience to securing these environments by:

- Implementing security monitoring capabilities
- Enhancing response plans
- Working more closely with public sector security bodies and security partners
- Leveraging the strong health and safety culture that already exists to instill a true security culture

Technical measures to achieve the above would include but are not limited to:

- Segregate corporate and ICS networks to reduce island-hopping attacks
- Reduce and protect privileged users to detect and prevent lateral movement
- Employ application whitelisting and file integrity monitoring to prevent execution by malicious codes
- Reduce the attack surface by limiting workstation-to-workstation communication
- Deploy robust network IPS (Intrusion Protection services), application-layer firewalls, forward proxies, and breach detection with sandboxing or other dynamic traffic and code analyzes
- Use and monitor host and network logging
- Implement pass-the-hash mitigations
- Deploy anti-malware reputation services to augment traditional, signature-based anti-virus services
- Run host intrusion-prevention systemsQuickly shield and patch known operating system and software vulnerabilities.

Conclusion

Both increasing IT/OT integration imposed by raising business requirements in the oil and gas industry and cutting-edge security capabilities sourced in different delivery models (capital expenditure (CAPEX), as-a-Service)) result in developing a very wide and complex environment to protect.

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.

REFERENCES

Utility of the Future Study: Cybersecurity, W. Draffin.
Digitization and cyber disruption in oil and gas, Ciepiela.
Best practices for cyber security in the electric power sector, IBM.
Definitive Guide to Cybersecurity for the Oil & Gas Industry, Jasn Holcom.
Proactive steps Builds a Stronger Security Posture, Cilance.
Photovoltaic Cybersecurity, Jay Jason.
Smart Grid's Cybersecurity, Z. Elrabetl, H. Elghazil, N. Kaboch

****