AUTHORS: **Moreno Herrero, Jesús / Moreno Hernández Diego**

TÍTULO / TITLE: Cibersecurity: the next oil&gas challenge.

FORUM: F17 - Cyber security and new technology risks

***KEY WORDS*: Oil & Gas, cybersecurity, cyberattacks, IT, OT**

ABSTRACT (máx. 300 palabras):

The importance of technology in Oil&Gas is undisputable. It is present in every part of the value chain.However, are companies aware of the risks that this implies? Are they enough prepared against cyber-attacks?

The aim of this paper is toanalyze the cybersecurity situation in Oil & Gas industry, the cyberattacks occurred, how companies faced them and what the future will bring.

Nowadays, cyber-crime is on the top 10 business risks, being the energy sector with 79 %, the highest percent of cyber-attacks. Unfortunately,most of them have been hidden by the attacked companies themselves. They do not want to show their vulnerability and try to avoid making it public.

Some of the most critical infrastructures, pipelines and operations are now being controlled by digital networks and the threat of cyber-attacks is real and countable, with over 5493 security incidents. For Oil &Gas companies, cybersecurity is no longer merely an information risk but a corporate responsibility.

The widespread use of devises in business in order to help with daily tasks and new sensors and transmission grids to control the operation has made Operation and Information technology become two different areas of cyber espionage.Cyberattacks imply considerable costs. The estimated average financial losses per company attributed to cybersecurity incidents within the oil and gas sector are around$2 billion by 2018.

The new security models address the convergence of operational technology (OT) and information technology (IT). Yet,Oil &Gas companies continue to rely on compliance with outdated policies and guidance. IT, OT, networking and physical security still act as islands, thus exposing weaknesses to potential attackers.

The main conclusions that the paper shows are: the low companies concern about cybersecurity, the future stronger regulation and the real threat of cyber-attacks and cyber terrorism.

Research of Cybersecurity at Oil and Gas Industry

Authors

Moreno Herrero, Jesús

Moreno Hernández, Diego

15/02/2016

Table of Contents

TABLE INDEX

FIGURES INDEX

Acronyms

ICT: Information and communication technology.

SCADA: supervisory control and data acquisition.

DCS: distributed control systems.

PLC: programmable logic controller.

RTU: remote telemetry unit.

DNS: Domain Name System

MSSP: Managed Security Services Provision

CSIRT: Computer Security Incident Response Team

DDoS (Distributed Denial of Service attack) is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

SQLi (SQL Injection) it is one of the many web attack mechanisms used by hackers to steal data from organizations.

Ransomware: is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back.

Cuckoo Miner: is a currently active campaign against financial and banking institutions.

1. INTRODUCTION

Nowadays, Information Technology is present in every company of every sector. IT helps companies to improve services, optimize processes and increase profits. However, this IT dependency turns the industry into a vulnerable industry. It is one of the main concerns of the companies, to be protected against cyber-attacks. In fact, the cyber-crime is on the top 10 of business risk, according to the Allianz Risk Barometer 2015:

			2014 Rank	Trend
1	Business interruption and supply chain	46%	1 (43%)	-
2	Natural catastrophes	30%	2 (33%)	-
3	Fire/explosion	27%	3 (24%)	-
4	Changes in legislation and regulation	18%	4 (21%)	-
5	Cyber crime, IT failures, espionage, data breaches	17%	8 (12%)	▲
6	Loss of reputation or brand value (e.g. from social media)	16%	6 (15%)	-
7	Market stagnation or decline	15%	5 (19%)	▼
8	Intensified competition	13%	7 (14%)	▼
9	Political/social upheaval, war	11%	18 (4%)	▲
10	Theft, fraud, corruption	9%	9 (10%)	▼

Illustration 1 Top business risk 2015 *Source: Allianz Risk Barometer*

The Allianz Risk Barometer 2015 survey was conducted among global businesses and risk consultants, underwriters, senior managers and claims experts. There were a total of 516 respondents from a total of 47 countries.[1]

Oil & Gas industry is not an exception. Oil & Gas companies have a high dependency on Information Technology, and every indicator shows that this is a growing trend. IT is present in every part of the oil value chain, from geophysics data acquisition on the exploration side of the business to financial information of the companies. This situation, in addition to the fact that Oil & Gas is an strategic sector in the global economy, makes Oil & Gas companies a cyber-attacks target. It's an unavoidable duty of companies, to have their IT system well protected.

2. STATE OF THE ART

2.1 Recent History of Cybersecurity in the Oil and Gas Industry

Today, the increase of frequent and visible cyber events (computer viruses, network denial of service attacks, cybercrime, malicious insiders, etc.) has made cyber a 'top of mind' issue in society.

The widespread use of digital devices in business has created a suitable environment for cyber espionage and deployed malware to steal corporate data.

These "unmasking" may result in the loss of confidence in the services and global corporations as well as in the emergence of the idea of global services analogues, but within the boundaries of the states.

Employees are the favorite target of cybercriminals. Malicious correspondence is sent primarily to those of of Public Relations and Human Resources.

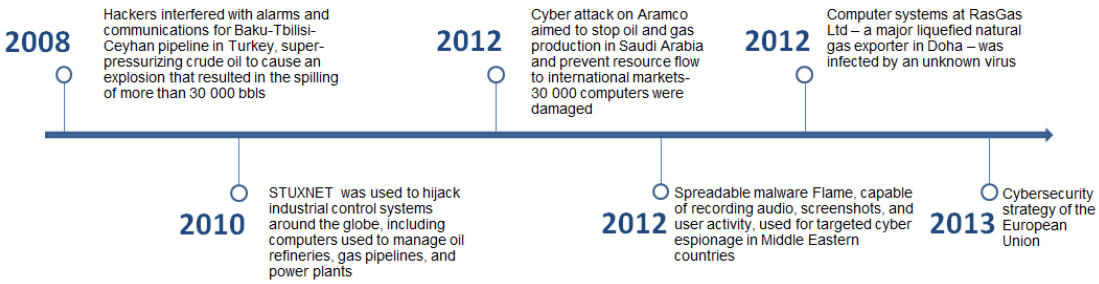

Illustration 2 Recent Cybercrime events. *Source: Internal Analysis*

In May 2013, hacking group Anonymous announced its intention to throw security attacks against the oil & gas sector. The main objectives of such attacks were companies in the oil industry, telecommunications, scientific research, aerospace and other fields related to the development of high technologies. For that reason, European Union started a new and advantage strategy.

The highest percentage of cyber-attacks take place in the energy sector, 32%, well above the industrial one (27%), Health (15.6%), Telecommunications (14.6%), Public Administration (13.5%) or financial sector (3.1%) [2.]

Oil and gas networks can be especially likely to suffer from internal incidents as many devices in such networks run 24 hours a day, seven days a week, and often lack the security updates and antivirus tools required to protect them against vulnerabilities. Adversaries are definitely taking advantage of this characteristic.

The state of the oil and gas industry is more perilous than ever, and energy and utilities companies must take new steps to defend themselves from cyber-attacks.

In 2014, the number of security incidents detected in the Oil and Gas sector in US was lower than in the power and utilities one. However, the estimated average financial losses

per company attributed to security incidents within the oil and gas sector was $4M while in the power and utilities sector, it was $1.2M.

Table 1 Impact of Security Incidents in the Energy Sector. *Source: PwC*

	O&G Sector	Power & Utilities Industry
Number of security incidents	5.493	7.391
Financial losses on average	**$4 Million**	**$1.2 Million**
Information Security spend	$5.7 million annually	$3.7 million annually
Spend onIntrusion-detection tools	64%	55%

The threat of cyber-attacks is real but the oil and gas industries and utilities sector do not seem to be spending an important amount of money to face it. According to PwC, companies in the utilities industry spend an average of $3.7M per year on information security while oil and gas firms spend $5.7M annually on average. [3]

Experts from multinational companies say that thanks to the fact that infrastructure and IT systems are similar everywhere, the US data can be extrapolated to other Western countries, such as Spain, with similar technological development, attacks on the Internet or theft of confidential information's management, as, indeed, on the Internet there are no boundaries.[4]

The British government estimates that oil and gas companies in the UK have already lost ~GBP400M per year as a result of cyber-attacks. [5]

2.2 Type of incidents at the Oil & Gas Industry

The Repository of Industrial Security Incidents contains a database of cyber-security incidents that have affected process control, industrial automation or Supervisory Control and Data Acquisition (SCADA) systems. This information for the Oil industry has been recorded since 1992 and EEUU accounts for almost 40% of it.[6]

Table 2 Incidents in Oil & Gas Industry. *Source: RIS*

Title	Year	Country
CIA Trojan Causes Siberian Gas Pipeline Explosion	1982	Russian Federation
Oil Company SCADA System Impacted by RF Interference	1989	United States
Olympic Pipeline Rupture and Subsequent Fire	1999	United States
Hacker Takes Over Russian Gas System	1999	Russian Federation
Accidental Remote Uploading of PLC Program	2000	Canada
Code Red Worm Defaces Automation Web Pages	2001	United States
Electronic Sabotage of Petroleum Company's Gas Processing Plant	2001	United States
Anti-Virus Software Prevents Boiler Safety Shutdown	2001	United States
Virus Infection of Operator Training Simulator	2002	Canada
Electronic Sabatoge of Venezuela Oil Operations	2002	Venezuela
Whitehat Takeover of DCS Consoles	2002	Canada
Control System Infected with SQLslammer Worm	2003	Unknown
Blaster Infects Onshore Oil Production Control System	2003	United States
Virus/Worm Infects New Oil Platform	2003	Norway
MUMU Infection of Operator Training System	2003	United States
MUMU Infection of Fiscal Metering System	2003	United Kingdom

Title	Year	Country
MUMU Infection of Leak Detection System	2003	United Kingdom
Welchia Worm Infects Automation Network	2003	United States
SQL Slammer Impacts Drill Site	2003	United States
Slammer Impacts Offshore Platforms	2003	United States
Slammer Infected Laptop Shuts Down DCS	2003	United Kingdom
Telco Shuts Off Critical SCADA Comms	2003	Canada
Worm attack on Drilling Control system	2004	United Kingdom
Sasser Worm Infection in Process Control System.	2004	United Kingdom
Two Viruses Cause Near Miss With Process Control Networks (PCN) in Africa	2004	Chad
Ping Sweep Caused DOS on PCN Firewall	2005	United Kingdom
Hacker Disabled Offshore Oil Platforms	2008	United States
Refinery Explosion and Fire Caused by Non-Functioning Computerized Level Monitoring System	2009	United States
Trans-Alaska pipeline spill	2010	United States
Computer Glitch Prevents Return of Gas Service	2011	Israel
Shamoon virus knocks out computers at Qatari gas firm RasGas	2012	Qatar
Process Control Network Infected with a Virus	2012	
Gas Company Virus Infection	2012	
Computer Virus Targets Saudi Arabian Oil Company	2012	Saudi Arabia

Incidents have happened everywhere and in all the areas of the oil industry value chain, from drilling and exploration systems to computers at headquarters.

Most cybersecurity threats and incidents are unintentional and occur within industrial networks. In the next table there is a summary of the main threats per incident.

Table 3 Industry Threats *Source: Repository of Industrial Security Incidents, 2011*

Threat Source	Percentage of industrial network incidents	Incident Type	Location of Source
Hackers and terrorists	9.4%	Intentional	External
Malware	30.4%	Unintentional	External
Insiders	10.6%	Intentional	Internal
Human Error	11.2%	Unintentional	Internal
Device and software failure	38.4%	Unintentional	Internal

Industry research shows that internal – not external – sources make up more than 60% of all cybersecurity threats.

Some recent studies have evaluated which are the attack techniques that oil and gas companies are most concerned about, and the result is in the Illustration 3: Recent Cybercrime events. ***Source: Oil & Gas iQ*** shows that the Illegitimate access it is the most important in companies.[7]

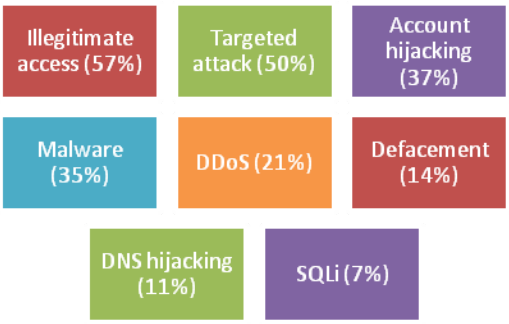

Illustration 3: Recent Cybercrime events. *Source: Oil & Gas iQ*

Nowadays it is important to know what would be the main prime concern if a mayor cyber intrusion was to occur. Illustration 4 represents the result of a recent survey where the system downtime it is the main prime concern.

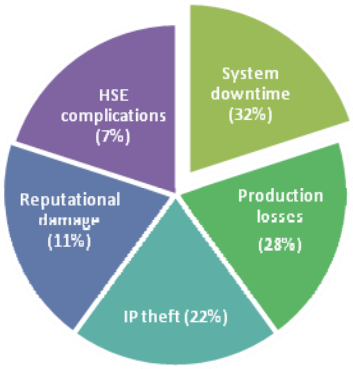

Illustration 4 Cyber intrusion preoccupation *Source: Oil & Gas iQ*

2.3 Incidents Scope

The scope of the incidents covers a wide range of threats and focuses on seeking access to IT infrastructure, both business and control systems, including the following methods among others:

- Access to and use of the Internet facing devices data acquisition (SCADA) ICS / Supervisory Control and unauthorized

- Zero-day vulnerabilities in control system devices and software

- Infections of malware in networks control system with air holes

- SQL Injection by exploiting vulnerabilities in web applications

- Network scanning and probing

- Lateral movement between network areas

- Campaigns targeted spear-phishing; doing a bad advertisement of security of the company. Bad Brand reputation

- Strategic Website compromises; key names, contacts

Most of the incidents are classified as having an "unknown" access vector. In such cases, the organization confirmed their compromise; despite this, forensic evidence does not point to a method of intrusion because of the lack of detection and surveillance capabilities within the network compromised.

2.4 Cybersecurity Solutions

Oil companies should feel that their systems are beyond the reach of attackers. Cybersecurity is becoming an increasingly prevalent threat within modern day business and operations. There is an ongoing digitalization in operations and services resulting in more vulnerability within the organization's framework. With some of the most critical infrastructure, pipelines and operations now being controlled by digital networks, Cybersecurity is no longer merely an information risk but a corporate responsibility.

With cyber-attacks becoming more sophisticated, targeted and malicious, many factors will play a crucial role to favor an organization's ability to prevent, detect, respond and mitigate a breach. The monitoring and surveillance centers are useful to acquire greater expertise while sharing the cost of tools and equipment in all technologies.

Cybersecurity could be grouped as a set of technologies, procedures, processes and services intended to protect assets depending in any way on ICT platforms. New security models that address the convergence of operational technology (OT) and information technology (IT) seem to be the key. Yet oil & gas companies continue to rely on compliance with outdated policies and guidance. IT, OT, networking and physical security still act as islands, thus exposing weaknesses to potential attackers.

2.4.1 IT Technology.

Since each industry has a different understanding and definition of terms, at oil and gas business IT can be defined as a widely part because of the amount of Terabytes of data that they already have.

For that reason, this part must have tools and solutions to defend and protect IT infrastructure and systems. IT assesses data such as those stored on servers, or sent by emails and stored on mobile devices and even information backed up on USB memory sticks.

Cyber-attacks in IT have different targets: data bases, mobiles, iPads, Cloud, wi-fi, usb devices, radio control systems…

The next list presents an example of companies and solutions to intercept attacks:

a) Symantec – '*Symantec Enterprise Vault*' has already been used in the oil and gas business at ENPPI
b) Fire Eye – A key product '*Network Threat Prevention Platform*' was used by the Energy Ministry of Saudi Arabia in 2011. It is based on detection and prevention of numerous attacks.
c) Palantir – '*Palantir Cyber'* provides enterprises with the unified view necessary to correlate incidents of cyber-attacks across data sources and monitor cyber threats in real time.
d) Splunk – '*Splunk software'* bases their use in investigation and incident response, complex correlation, proactive alerting and auto-remediation.
e) Fidelis – '*XPS, Resolution1 endpoint'* solutions help to detect, investigate and stop advanced attacker at every stage of the attack lifecycle.

f) INDRA -- ‘COMSec’ provides secure voice communications and data in commercial mobile devices over wireless

2.4.2 OT Technology.

On the other hand, Operational technology (OT) covers another important part of the company technology such as the sensors, SCADA systems, software and other controls that operate the pipelines, power plants, and transmission and distribution grids

The following list provides an example of how companies and solutions intercept attacks in OT:

1) MICROSOFT -- ‘*Microsoft Upstream Reference Architecture’* Case Study: Chevron, PEMEX.
2) MOTOROLA -- It secures operations control, uncompromising security for the radio network, complete security services.
3) CISCO -- ‘*Cisco Secure Ops’* Solution .Case Study: Company that Produces 3M+ barrels of oil and natural gas daily and with more than 90,000 employees.
4) IBM -- ‘*Internet Security System’* offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection.
5) N-DIMENSION -- ‘*N-Sentinel’,* cloud-based managed security services that maintain continuous vigilance in the detection of cyber threats and vulnerabilities, helping critical energy infrastructures take time action in protecting their networks, data and assets from risks.
6) INDRA -- ‘i-CSOC’, cybersecurity operations center offers service lines of MSSP, Labs, Cyberintelligence, CSIRT, Training and Cloud.

3. REGULATION

3.1 European Regulation

The beginning of the Cybersecurity policy in the European Union (EU) is in the joint communication of the Council and the Commission COM (2000) 890. Afterwards, different communications, documents and also norms of the corresponding institutions, have been issued in order to establish a common policy and regulation about cybersecurity.

On 23th of November 2011 in Budapest was signed the Convention on Cybercrime, Treaty No.185. Until now it is the most universal document about cybercrime. It is the only cyber treaty that aims at harmonizing universal rules of national criminal law and criminal prosecution of crimes related to Internet. It has been confirmed by USA and 23 European countries.

In relation to protection against cyberattacks, the EU has published several documents, like the COM (2006) 251 "Strategy for a secure information society" and the COM (2010) 245 “European Digital Agenda”.

The EU also has focused on the protection of Critical infrastructures. The EU has developed the European Programme for Critical Infrastructure Protection (EPCIP). These critical infrastructures are the assets, facilities, systems, networks or processes that are essential for the security and the functioning of a society and economy.

Among others, the oil & gas sector, and specifically the gas production, transport and distribution as well as oil products production, transport and distribution facilities, are considered critical infrastructures. Based on EPCIP, each European country regulates the operations and fixes the requirements for operators of these infrastructures.

It should be noted the obligation of designing a cybersecurity plan that fulfills the standard security requirements, and the obligation of notifying when a cyberattack occurs to the nationals Computer Emergency Response Team (CERT). [8]

Nowadays, the two most recent and important documents are the Cibersecurity Strategy of the European Union of 2013, JOIN(2013) 1, and the Directive for Network and Information Security (NIS).

3.1.1 Cibersecurity Strategy of the European Union

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

- Achieving cyber resilience.
- Drastically reducing cybercrime.
- Developing a cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP).
- Develop the industrial and technological resources for cybersecurity.
- Establish a coherent international cyberspace policy for the European Union and promote core EU values.

3.1.2 Directive for Network and Information Security (NIS).

The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by:

- Increasing the cybersecurity capabilities in the Member States
- Enhancing cooperation on cybersecurity among the Member States
- Ensuring a high level of risk management practices in key sectors (such as energy, transport, banking and health).

Once adopted and implemented, the NIS Directive will benefit citizens, as well as government and businesses, who will be able to rely on more secure digital networks and infrastructure to provide their essential services at home and across borders. [9]

3.2 European agencies.

The two main agencies of cibersecuriy in Europe are the European Union Agency for Network and Information Security (ENISA) and the European Cybercrime Centre (EC3)

ENISA was set up in 2004 and is the EU's response to the cybersecurity issues of the European Union. ENISA was set up to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security problems. In order to achieve this goal, ENISA is a Centre of Expertise in Network and Information Security and is stimulating the cooperation between the public and private sectors. As such, the Agency is a 'pace-setter'. [10]

The European Cybercrime Centre (EC3) was created in 2013 as part of Europol. The EC3 was set up to strengthen the law enforcement response to cybercrime in the European Union (EU) and to help protect European citizens, businesses and governments. Its establishment was a priority under the EU Internal Security Strategy.[11]

3.3 USA regulation

Recently Enacted Legislation:

- P.L. 114-113, Cybersecurity Act of 2015, signed into law December 18, 2015. Promotes and encourages the private sector and the US government to rapidly and responsibly exchange cyber threat information.
- P.L. 113-274, Cybersecurity Enhancement Act of 2014, signed into law December 18, 2014. Provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.
- P.L. 113-282, National Cybersecurity Protection Act of 2014, signed into law December 18, 2014. Codifies an existing operations center for cybersecurity.
- P.L. 113-246, Cybersecurity Workforce Assessment Act, signed into law December 18, 2014. Directs the Secretary of Homeland Security, within 180 days and annually thereafter for three years, to conduct an assessment of the cybersecurity workforce of the Department of Homeland Security (DHS)

3.4 USA agencies

USA has a solid structure to watch the national cybersecurity:

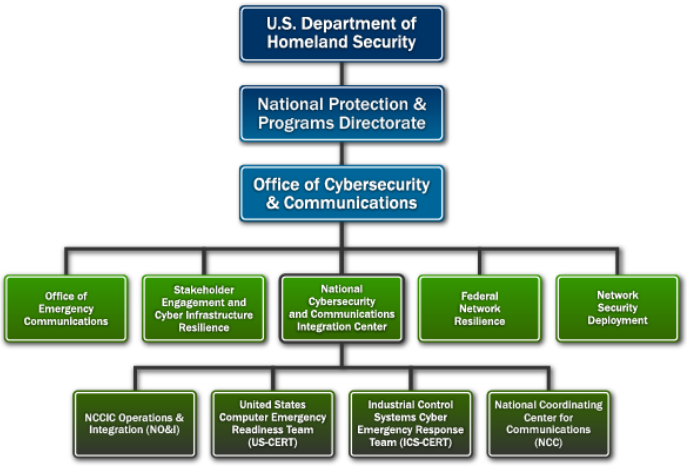

Illustration 5 USA structure of national cybersecurity. *Source: USA Cert Gov website*

The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. [12]

It should be pointed the Department of Homeland Security, who is the responsible for protecting the Nation's critical infrastructure from physical and cyber threats. Cyberspace enables businesses and government to operate, facilitates emergency preparedness communications, and enables critical control systems processes. Protecting these systems is essential to the resilience and reliability of the Nation's critical infrastructure and key resources and to our economic and national security. As it was mentioned before, certain Oil & Gas infrastructures are considered critical and are under the cybersecurity regulation.[13]

4. FUTURE TRENDS

4.1 Cyber-attacks

According to the recent activities and incidents in terms of cyber-attacks, there are two main areas in which they will evolve in the next years: extortion and hacktivist.

Online Extortion

Instead mastering the technical aspects of the operation, online threats will evolve to master the psychology behind each scheme.

In the last 10 years, cyber extortionists made use of different tools:

- **Ransomware** is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. The ransomware tricks online users to make them fall for their tactics. This was done by exploiting one's fears to coerce victims into paying the ransom.
- The rogue/fake AV trap was set up to target those who feared computer infection. Earlier variants of ransomware locked screens of users, tricking them into paying to regain access.
- Crypto-ransomware, cybercriminals aimed for the most valuable part of one's system, the data.

Using these techniques, cyber extortionists will treat with damage the reputation of the entire enterprise or any of their employees. Reputation is everything, and threats that can ruin a business' reputation will prove to be effective and—more importantly— lucrative.

Another point is the use new social engineering lures. There will be a significant increase in tricks that use new social engineering lures. Using advanced ploys, the employees will be persuaded to transfer money to a cybercriminal-controlled account. These malicious schemes will be based on the knowledge of ongoing business activities and intercepting the communications between business partners, like the tactics used in the past by the cybercriminals behind the cyberattacks like Cuckoo Miner (active campaign against financial and banking institutions) or Predator Pain (malware use to steal information from victims' computers)

Hacktivists

Data breaches will be used to systematically destroy hacktivists' targets. In the next years, we will see more hacktivists going the route of "destructive" attacks by going for data that can potentially damage their target's integrity.

In the past, the hacktivist used default tactics like web defacement and DDoS attacks to ruin targets. However, the recent success of high-impact breaches, driven by a common goal of exposing incriminating information like questionable corporate practices, classified messages, and suspicious transactions will drive cybercriminals to add data breach methods to their arsenal of tactics.

4.2 Regulatory trends.

Cybersecurity regulation will become a global movement. Governments and authorities will work together in order to act faster and give a rapid response to cyberattacks.

Cooperation and partnership among cybersecurity agencies will be key factor to struggle against cybercrime, as occurred in the combat against SIMDA in April 2015. SIMDA is the family of password-stealing trojans can give a malicious hacker backdoor access and control to the computers. They can then steal your passwords and gather information about the computer. It was necessary the common effort of different agencies and companies as INTERPOL or Microsoft, to takedown SIMDA.

The Internet hasn't had a solid regulation but, in the next years, will see a significant change in the attitude of governments and regulators that will suppose a strong regulation. Governments will be more active in protecting the Internet and safeguarding its users.

4.3 Future business investments

According to the security company Trend Micro, in the next years companies will reinforce their structure focusing on cybersecurity. Enterprises will finally realize the need for a job designation that focuses solely on ensuring the integrity of data within and outside the enterprise. Whether the company creates a separate Data Protection Officer (DPO), Chief Risk Officer (CRO) or includes this among the tasks of the Chief Information Security Officer (CISO) depends on company size, budget and other factors, but the set of responsibilities will be the same.

The iron cage put up by the EU Data Protection directive will mandate a high standard of protection on data and the role of the DPO/CISO will be vital in ensuring the integrity of data and compliance with rules and regulations of countries where company data is stored. DPOs and CISOs must be experts in data protection and data security regulations and must know how these should be effectively implemented.

Awareness around data protection will pave the way to a significant shift in the enterprise mindset and strategy against cyber-attacks. We will see more enterprises taking on the role of the 'hunter' instead of the 'hunted', in that they will begin to make use of threat intelligence and next-generation security solutions with custom defense to detect intrusions earlier. [14]

4.4 How should companies protect themselves?

It is globally estimated that cyber-attacks against oil and gas infrastructure will cost owners $1.87 billion by 2018 [3]

Application of international safety standards such as ISO 27001 standards will provide guidelines on which it will be possible to build a secure enterprise.

1. **Know your critical assets** – Identify your organization's business objectives and high-value assets, then lead risk assessments to find any vulnerability.

2. **Protect your IT, radio network and OT environments** – Establish defenses to block intruders before they reach your critical business assets, and educate your employees to recognize and avoid phishing attacks.

3. **Detect potential threats before they occur** – Use the right tools to get a comprehensive view of your security environment and monitor potential threats both externally and internally.

4. **Respond and recover** – With the speed and intelligence of many of today's cyber-attacks, cyber breaches may still occur, even in the most secure infrastructure. Having a contingency plan in place can help you respond immediately if a breach should occur.

5. **Build a culture of Security** – Cybersecurity practices are reflexive and excepted among all energy sector stakeholders.

In order to protect oil and gas operations, engineers and network designers must identify new cybersecurity measures. The following measures are designated to reduce cyber-security risk:

Table 4 Measures to Reduce Cybersecurity Risk

#S1	#S2	#S3	#S4	#S5
•Adopting a framework.	• Defining the organization, roles, activities and responsibilities of cybersecurity.	•Making an inventory and classification systems from the point of view of cybersecurity.	•Analyzing and managing the risk. • Defining an incident management procedure.	•Including cybersecurity requirements in any project from the beginning.

#S6	#S7	#S8	#S9	#S10	#S11
•Raising awareness and creating culture related to cyber-security.	• Implementing perimeter defense systems..	•Forecasting cybersecurity audits.	•Monitoring and correlating events systems	•Collaborating actively in forums and specialized working groups in order to create a culture of security.	•Including cybersecurity requirements in any project from the beginning.

4.5 Vision and Barriers

By 2020, resilient energy delivery systems were designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions.[15]

• Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures.

• Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures.

• Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations.

• Threat, vulnerability, incident, and mitigated information sharing is insufficient among government and industry.

• Weak business case for cybersecurity investment by industry

• Regulatory uncertainty in energy sector cybersecurity

5. CONCLUSIONS

After the analysis of the current situation of cybersecurity and their influence in Oil&Gas industry, there arise different conclusions: the low companies concern about cybersecurity, the future stronger regulation and the real threat of cyberattacks and the cyberterrorism.

First of all, despite that cybercrime is a real threat, Oil & Gas companies are not concerned enough. The investment on that area are not very significant because is an inversion that doesn't have an economic return. It's an inversion to prevent against hypothetic cyberattacks and companies don't carry it out. Furthermore, cyberattacks are not usually published, so there is no clear and reliable information about how probably a cyberattack is.

In the same way, companies should invest money and time in a *cyberculture* Building this formation in their employees they ensure prevention, anticipation and quickly intervention in order to make certain in a future attack. This culture must be integrated with governments focusing in the same common idea and trying to extend in all population.

On the other hand, it's important to take into account the regulation tendency. There is a clear tendency of increase and develop deeper the regulation about cybersecurity; especially for critical sectors. Without any doubt, Oil&Gas is a strategic sector for every country so earlier will have a specific regulation for this kind of companies. The regulation will request of how companies protect their data, the customer and user information and how they protect their system against cyberattacks. Governments will set the cybersecurity requirements for the companies that operate in their countries. Besides the IT systems and their cybersecurity of the shall be carefully audited by governmental agencies. In conclusion, a strong investment in cybersecurity will be unavoidable.

Also it's remarkable the threat of cyberterrorism. A cyberattack can produce a complete shutdown of an entire company that implies huge economic losses. Moreover, IT system control the security of several infrastructures as pipelines or refineries, a bad intentioned use of these tools can provoke material damage or even cost human life.

6. REFERENCES

1. Top business risk 2015 ,ALLIANZ 2015
2. US ICS-CERT (Industrial Control Systems Cyber Emergency Response Team).2014
3. PwC. “The Global State of Information Security Survey 2015”
4. Energy News. Enrique Martin GMV ,2014
5. Cyber-attacks: Effects on UK Companies. Oxford Economics July 2014
6. RIS*: Repository of Industrial Security Incidents, 2011*
7. Oil & Gas iQ , 2014
8. Computer emergency response team (CERT-EU) 2015
9. European Commission ‘EU Strategies’ Dec 2015
10. European Union Agency for Network and Information security (ENISA) 2015 (website)
11. Europol ‘The European Cybercrime Centre (EC3)’ 2013
12. United States Computer Emergency Readiness Team (US-CERT) 2016
13. Homeland security ‘Office of Cybersecurity and Communications’ October 27, 2015
14. Trend Micro. ‘The Fine Line. 2016 Trend Micro Security Predictions’, 2015
15. U.S DOE ‘Roadmap to achieve Energy Delivery Systems Cybersecurity’, 2014