DIGITAL OILFIELD AND THE CYBER RISKS IN THE EVERYDAY WORK. MANAGING OILFIELD DATA IN A MORE UNSECURE WORLD

1. Robert Kosova,
Faculty of IT, UAMD, Durrës, ALBANIA
2. Irakli Prifti,
Faculty of Geology and Mining, Polytechnic University, Tirana, Albania
3. Teuta Thanasi,
Faculty of IT, UAMD Durrës, ALBANIA
4. Elda Cina,
Faculty of IT, UAMD Durrës, ALBANIA

Abstract:

Industrial organizations operating in the oil and gas sector face greatest challenges today including the pressing need to find and exploit new energy supplies, greater regulatory pressures, new work requirements and the demands of a growing data management. At the same time, oil companies face a serious and growing risk from cyber-attacks, malicious software, and other threats against their IT infrastructure, scientific and production data and intellectual property.

Extracting value from the computers or networks of unsuspecting oil companies and government agencies has become a big business and a very profitable one. No oil company or agency can ignore network security today; it is the source of systematic risk that threatens long-term health, stability and profitability of any oil company. Cyber security is and must be part of any corporate strategy for managing risk and compliance. Cyber security risk management is becoming a high-level responsibility for any board of executives and one of the most difficult tasks to deal with.

From the history of hacking and cyber attacking there are plenty of conclusions and results such as:

It is not difficult at all to hack data from a oil company.

More than 90% of successful breaches required only the most basic techniques to do. Only 3% of breaches were impossible or unavoidable without difficult or expensive actions. Outsiders were responsible for most network breaches.

85% of breaches took a lot of time to be discovered; the average time for discovering one is five to six months.

96% of successful breaches could have been avoided or prevented if the victim (oil company) had put in place simple or intermediate controls.

75% of network attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.

One study found that most of antivirus software missed as much of 95% of malware in the first few days after its introduction.

Another study on internet and network security found that 25% of malware is not detected by current antimalware or software techniques.

In this paper we will look at how oil and gas organizations can measurably improve their security posture – not only by deploying sophisticated technologies or strategies, but mostly and instead by simply following the basics of common-sense and effective cyber security.

Keywords: oilfield, data, security, cyber risk, hacking, management.
JEL Classification: 0320

Introduction

The oil and gas industry needs and relies on information and communications technology (ICT) to meet its business goal and in everyday work. The industry knows that to manage future oil and gas developments and the effective production of existing reserves, it will be essential to integrate and connect business processes, peoples, geographies and organizations.

These environments, which define the connected oilfield, must be designed around a "human network"; in other words, the environment must connect all stakeholders and partners, such as field staff, technical experts, and knowledge workers, if they are to function effectively.

The Society of Petroleum Engineers commented in a recent position paper: "Over the next decade the way in which we understand our reservoirs, identify development options, manage and optimize our wells, facilities, and associated production will all change radically. Logically this leads to…a substantial impact on the people working on these fields. "

With change comes the promise of significant rewards to those who have made the investment in business transformation based on information and communication technology. Ultimately, connecting oilfield assets and stakeholders with real-time and right-time information will facilitate distributed problem solving and decision making and enhance effective management.

The consequential improvement in recovery rates, together with better cost management and improved health, safety, and environmental performance, will help the industry continue to meet the ongoing hydrocarbon needs of the world's energy consumers. The connected oilfield is about new ways of working.

What Is the Connected Oilfield?

While the oil and gas industry focuses a great deal of activity on "digitization of the oilfield, " little effort has been expended on the role of the intelligent network as the platform for connecting decision makers with oilfield assets. The connected oilfield is about "integrating operations"—using IT to change work processes for better decision making, to manage and control equipment and processes remotely and to move functions and personnel onshore.

Having a network is not sufficient; it must be an intelligent network that truly can act as a central nervous system, connecting every individual and every function in the organization while permitting collaboration and data sharing with the greater oil and gas ecosystem.

This means that time zones and geographical distance are no longer barriers. It delivers true "demand and respond" capabilities, which allow oil and gas companies to manage workflows across geographies, enhance collaborative environments, and monitor and manage fixed and mobile assets at the right time, in the right place, with the right resources.

The intelligent network will facilitate the seamless integration of data, information, and work processes. It creates a virtual environment where effective communication and collaboration among experts can occur, regardless of where the experts are physically located or to which organizations they belong.

An intelligent network means the connected oilfield knows no internal, limiting boundaries, and delivers information that will result in the improved recovery of hydrocarbons, more efficient oilfield operations, and increased productivity.

At the most basic level, the ability to recalibrate a pressure gauge remotely imparts data that can be shared and incorporated in the decision making process in a matter of minutes—instead of hours, days, or weeks.

The intelligent network provides for the human element. In the exploration and production business, critical decisions are based on the assembly and consolidation of knowledge as it is interpreted by technical professionals—knowledge workers who need help visualizing potential solutions and outcomes.

Oil and gas is one of the few truly global industries—particularly exploration and

production. It is also one of the most knowledge-intensive industries. It relies on professional workers to make and implement key value decisions.

Business needs and pressures, coupled with rapid advances in ICT capabilities, are promulgating a digital evolution—indeed, a revolution. Understanding and using connectivity and connectedness between assets, workers, and all stakeholders is a critical requirement. Digital oilfield helps achieving:

Production Increase:

- Real-time interaction between involved activities and disciplines. For example, engineers
- monitoring oilfield wells can contact the field if they discover matters requiring action.
- Use of dynamic simulation in connection with production and process analyses.
- Use of analysis tools in critical work processes, where the tools extract and present available information from operating data (both historic and near-real-time data).
- The use of interaction rooms to support work processes between land and sea, and between
- operator and supplier (the measure also includes drilling, operations, and maintenance). Production issues can be solved earlier through prompt involvement of support functions and experts who can quickly implement the right measure.
- In some cases, work can be performed from such rooms that would otherwise have necessitated travelling to the installations.
- Continuous control/support from specialists—from both the organization and its suppliers—on a 24-hour basis.

Reserve Increase:

- Consistent production and reservoir data (including seismic data)
- Accurate reservoir models for optimal localization of wells
- Smart wells, and real-time reservoir monitoring and management

Reduced Operating and Maintenance Costs:

- Condition- and campaign-based maintenance
- Transferral of administrative, surveillance, management, and reviewing activities onshore
- Reduced usage of experts offshore
- Onshore remote control
- Increased instrumentation and automation, and improved efficiency for monitoring and analysis
- New ways of supporting the fields by centralizing tasks, coordinating across fields, and specializing service supplies to a larger degree.

Reduced Drilling Costs:

- Fewer sidetracks with more accurate drilling
- Real-time optimization of path and drilling processes
- Reduced need for sending out specialists and service personnel
- Improvement in ultimate (hydrocarbon) recovery: 1-7 percent
- Production acceleration: 1-6 percent
- Reduction in downtime: 1-4 percent
- Improvement in operating efficiency: 3-25 percent
- Drilling cost reduction: 5-15 percent

As oil and gas companies engage in their digital oilfield studies and pilots, and as they look to connect and integrate all the disparate data and communication flows, they find they have a single common need: connectivity, defined as the ability to integrate data and information seamlessly with workflows, processes, and people in a “borderless” manner across legacy systems, organizations, and country borders.

Cost Reduction:

The energy industry is cyclical, driven by expectations of the current and future price of oil and gas. Prices are driven by basic supply and demand, created by world macroeconomics. When oil prices are high, the industry invests in skills and capabilities (usually at the peak).

When the price of gas and oil is low, the industry stops investing. Unfortunately, the timing is never quite right, leading to cyclical volatility in capacity and in the price of materials and services. The result is that the oil and gas industry is often painfully short of capacity and skilled workers just when they are most needed.

Connecting the Oilfield:

The oil and gas business is about acquiring and managing assets. It's about making value decisions, such as where to drill next and how best to maximize production. It's about linking, coordinating, and ultimately scaling the organization, gaining access to the right skills and resources. And all this must be accomplished safely, with high regard for the health of employees and local inhabitants, as well as for environmental issues.

Distributed Decision Making:

A connected oilfield is by definition a "virtualized" in which decision making is a distributed function. Peer-to-peer exchanges—individuals distributed around the oilfield itself and around the world, communicating digitally— are the everyday transactions of the connected oilfield. In this widely distributed environment, which relies not only on the availability of information, but also on the expertise of individuals to correctly interpret it, tools like remote visualization and Unified Communications are indispensable.

Network security and managing:

The goals of network security are as follows:

- Protect confidentiality
- Maintain integrity
- Ensure availability
- With this in mind, it is imperative that all networks be protected from threats and vulnerabilities for a business to achieve its fullest potential. Typically, these threats are persistent because of vulnerabilities, which can arise from the following:
- Misconfigured hardware or software
- Poor network design
- Inherent technology weaknesses
- End-user carelessness
- Intentional end-user acts (that is, disgruntled employees)

This study provides an overview of essential network security concepts, common vulnerabilities, threats, attacks, and vulnerability analysis.

Open Access

An open security model is the easiest to implement, as shown in Fig 1. Few security measures are implemented in this design. Administrators configure existing hardware and software basic security capabilities. Firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs), and other measures that incur additional costs are typically not implemented. Simple passwords and server security become the foundation of this model. If encryption is used, it is implemented by individual users or on servers.

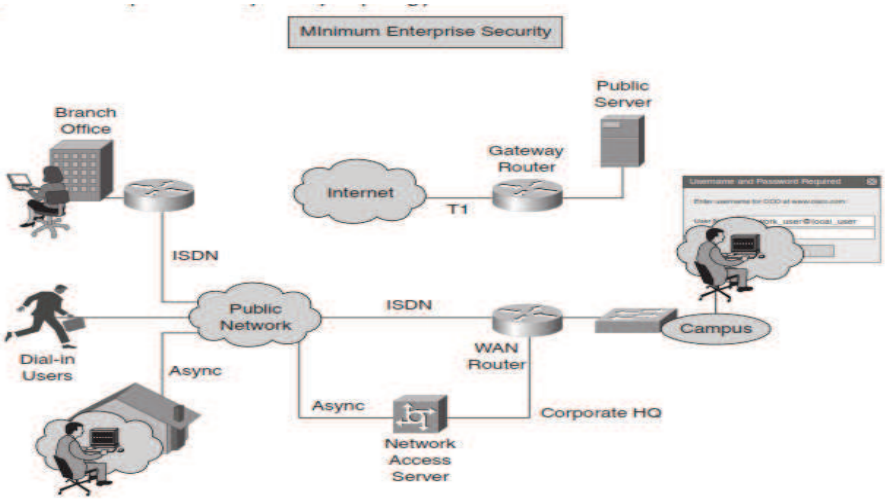

Fig 1. Minimum security.

Closed Access

A closed security model is most difficult to implement. All available security measures are implemented in this design. Administrators configure existing hardware and software for maximum-security capabilities in addition to deploying more costly hardware and software solutions such as firewalls, VPNs, IDSs and identity servers as shown in Fig 2.

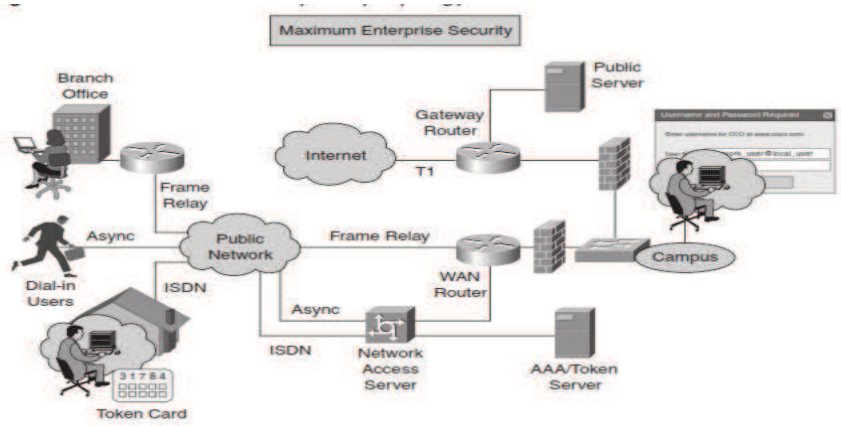

Fig 2. Maximum security.

When discussing network security, the three common terms used are as follows:

Vulnerability—A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.

Threats—The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

Attacks—The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops.

The sections that follow discuss vulnerabilities, threats, and attacks in further detail.

Vulnerabilities

Vulnerabilities in network security can be summed up as the “soft spots” that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

- Technology weaknesses
- Configuration weaknesses
- Security policy weaknesses

Access Attacks

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. Access attacks can consist of the following:

- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle attacks
- Social engineering
- Phishing

Network Analysis and tools.

Many industry best practices, tools, guides, and training are available to help secure network devices. These include tools from Cisco, such as Auto Secure and Cisco Output Interpreter, and from numerous web resources.

The Cisco AutoSecure feature is enabled from a Cisco IOS Security command-line interface (CLI) command. AutoSecure enables rapid implementation of security policies and procedures to ensure secure networking services. It enables a “one-touch” device lockdown process, simplifying the security configuration of a router and hardening the router configuration. This feature simplifies the security process, thus lowering barriers to the deployment of critical security functionality.

Knoppix STD

Knoppix Security Tools Distribution (STD) is a Linux LiveCD distribution that contains many valuable security tools. The LiveCD is a bootable CD-ROM that contains the Linux operating system, along with software applications, that can be run from memory without installation on the hard drive. After the LiveCD is ejected from the CD-ROM drive, the system can be rebooted to return to the original operating system. Knoppix STD contains many useful features, such as the following:

- Encryption tools
- Forensics tools
- Firewall tools
- Intrusion detection tools
- Network utilities
- Password tools
- Packet sniffers
- Vulnerability assessment tools

Microsoft Baseline Security Analyzer

You can use the Microsoft Baseline Security Analyzer (MBSA) to scan hosts running Windows 2000, Windows XP, and Windows Server 2003 operating systems to determine potential security risks. MBSA scans for common system misconfigurations and missing security updates. MBSA includes both a graphical interface and a CLI that can perform local or remote scans. After a system scan, the MBSA provides a report outlining potential vulnerabilities and the steps required to correct them. This tool is available as a free download from Microsoft.

Conclusions and Recommendations:

- The digital oil field (DOF) concept is helping oil and gas companies drive offshore innovation and optimisation. Now that data analysis and wireless technologies are readily available to the industry, companies must ask themselves how they can make the most of the new information age.
- (DOF) is very useful everyday managing and leverages existing information technology and data with minimal IT overhead. As a result, implementation cost is reduced while creating additional value and returns on legacy systems and IT investments, including information systems and data management.

(DOF) is about unifying disparate oil field processes into a more easily digestible stream of information, making it easier to get the big picture on an operation and thus optimise productivity in real-time, while minimising the industry's labour-intensive, hard-copy hassles.

- **(**DOF) provides a decision-support framework that bridges the gap between strategic and operational decisions, enabling optimal business results and value.
- (DOF) boosts net present value by improving exploration and production asset management, reducing cycle time, and optimizing decision-making for exploration and production opportunities.
- (DOF) facilitates collaboration and knowledge sharing across the petroleum enterprise, enabling organizations to harness collective expertise from a globally distributed work force, improve process efficiency and reduce cycle time for E&P work processes.
- The exponential growth of networking has led to increased security risks. Many of these risks are due to hacking, device vulnerabilities, and improper uses of network resources.
- Awareness of the various weaknesses and vulnerabilities is critical to the success of modern networks. Security professionals who can deploy secure networks are in high demand. The four primary threats to network security include unstructured threats, structured threats, external threats, and internal threats. To defend against threats, an understanding of the common methods of attack must be established, including reconnaissance, access, DoS, and malicious code.

References:

1. Marisé J. B. Mikulis. Digital Oil Field Technology Offers Valuable New Options For Optimizing Production. . The digital oil field, oil and gas investor. April 2004.
2. Reynold Decou. How El Paso Production Went Digital: . Tinvestor, april 2004.
3. Roberta Bigliani. Reducing Risk in Oil and Gas Operations: IDC Energy Insights May 2013.
4. David Joy. Digital Danger: How Do You Build An Effective Cyber Strategy For Oil & Gas?
5. David Gewirtz. 14 global cyber security challenges for 2013.
6. Justin Lowe. Enabling Digital Oilfields through effective cyber security: IDOC: .
   Security in Upstream Oil & Gas. The Microsoft Upstream Reference Architecture (June 2010).
7. *Darrell R. Pitzer (ExxonMobil Production Company) | Ana M. Girdner (ExxonMobil Production Company)*. Addressing and Managing Cyber Security Risks and Exposures in Process Control. SPE Intelligent Energy Conference & Exhibition, 1-3 April, Utrecht, The Netherlands. **DOI:** ***http: //dx. doi. org/10. 2118/167912-MS***. **ISBN:** ***978-1-61399-306-4***.
8. *The Promise and Challenges of Digital Oilfield Solutions: Lessons Learned from Global Implementations and Future Directions*. Sankaran, Sathish, Halliburton Digital & Consulting Solutions. Lugo, Jose T. , Landmark Halliburton. 122855-MS SPE Conference Paper – 2009.
9. Al-Issa, Ayman, ADMA-OPCO. *Protecting the Digital Oil Field from Emerging Cyber Threats*. 162304-MS SPE Conference Paper – 2012.