Risk Management in the Energy Sector: Evolving Cybersecurity Risks & Strategies

The University of Oklahoma
COLLEGE OF LAW

Joseph R. Dancy
Director, The University of Oklahoma College of Law
Oil and Gas, Natural Resources, and Energy Center (ONE C)

OKC SPEE – September 28, 2017

National Association of Corporate Directors

2014 NACD Cyber-Risk Oversight Study:

1. Increasing number of cyberattacks
2. Cyberattack complexity has grown dramatically
3. Cost to address cyber issues escalating quickly
4. Sophisticated attacks will almost always breach the target

HOUSTON ★ CHRONICLE

Sunday, March 5, 2017 | HoustonChronicle.com and Chron.com | Vol. 116, No. 143 | $4.00 ★★ Chance of storms: High 70, Low 65

SpaceX sends a message to NASA

Private company pushes limits with moonshot plan

By Mike Tolson and Kevin Diaz

In the world according to Elon Musk, haste doesn't make waste — it makes sense. Want to go to the moon? Just do it.

While NASA slowly assembles its big new moonbound rocket and the capsule that will place astronauts on top of it, Musk and his company, SpaceX, announced last week that they have received down payments for the voyage of a lifetime — a weeklong trip in 2018 that will take a pair of paying customers tantalizingly close to the dusty lunar surface.

In other words, a company that did not exist at the turn of the century was going to beat the agency that created space travel back to the spot of its greatest triumph. By years.

Some will dismiss the private moonshot as a stunt, a wild hare of an idea from the mind of a man obsessed with colonizing Mars. If Musk is crazy, it may be more like a fox than a hare. There's a new president in town with a preference for the private sector, and patience is not his MO.

NASA continues on A11

Sensors may settle oil, quake debate

By David Hunn and Lydia Depillis

The state of Texas wants to stick a seismometer on Terry Hill's ranch, right next to his deer blind.

Hill, a fourth-generation Texan born and raised in this Rio Grande outpost outside Del Rio, understands the significance. He receives a few thousand dollars in oil and gas royalties a year, yet the findings of the earthquake sensor could dramatically alter the industry that helps pay his bills.

"I don't know what this is, or what it's gonna do," said Hill, 66, "but I hope it will be helpful."

Hill is among the landowners allowing the state

CHRONICLE EXCLUSIVE

HACKED

Ken Ellis / Houston Chronicle

Energy industry an alluring target for sophisticated cyberattacks

By Collin Eaton

A Coast Guard cutter glides along the waters of the Sabine-Neches waterway, conducting sweeps for unprotected wireless signals that hackers could use to gain access to oil, gas and petrochemical facilities.

Four massive refineries sit along the 79-mile channel that cuts through this stretch of Gulf Coast. It's one of the largest concentration of refineries, pipelines, chemical plants and natural gas terminals in the United States — and an alluring target for espionage, disruption or worse.

"There are actors that are scanning for these vulnerable systems and taking advantage of those weaknesses when they find them," said Marty Edwards, director of U.S. Homeland Security's Cyber Emergency Response Team for industrial systems.

As national attention focuses on Russian cyberattacks aimed at influencing the last presidential election, oil and gas companies face increasingly sophisticated hackers seeking to steal trade secrets and manipulate industrial sensors and operations.

Nowhere is the threat more consequential than in Houston and Southeast Texas, where the world's most celebrated names in energy produce, refine and transport fossil fuels, including Exxon Mobil, Royal Dutch Shell and Phillips 66.

The operation aboard the Coast Guard cutter, a joint effort with Houston Police last April, was one of the first of its kind in the U.S. to focus on cyberattacks by sea.

The U.S. Department of Homeland Security, responsible for protecting the nation from cybercrime, received reports of more than 350 incidents at energy companies between 2011 and 2015. In most cases, a hacker infiltrated or tried to infiltrate the control systems of energy firms. During that period, the agency identified nearly 900 security vulnerabilities within U.S. energy companies, more than any other industry.

The vastness of oil and gas operations makes it difficult to secure. Thousands of interconnected sensors and automated controls that run oil and gas facilities remain rife with weak spots.

PART ONE

The massive network of U.S. energy pipelines, refineries and fuel terminals is increasingly vulnerable to the dangers of cyberattacks.

NEXT SUNDAY

PART TWO

Infiltrating oil and gas facilities is too easy – professional hackers describe how it's done.

Trump: Obama tapped his calls

Explosive claims made on Twitter with no evidence

By Michael D. Shear and Michael S. Schmidt
NEW YORK TIMES

WEST PALM BEACH, Fla. — President Donald Trump on Saturday accused former President Barack Obama of tapping his phones at Trump Tower the month before the election, taking to Twitter to call his predecessor a "bad (or sick) guy."

Without offering any evidence or providing the source of his information, Trump fired off a series of Twitter messages claiming that Obama "had my 'wires tapped.'" He likened the supposed tapping to "Nixon/Watergate" and "McCarthyism."

A spokesman for Obama said any suggestion that the former president had ordered such surveillance was "simply false."

Trump's aides declined to clarify whether the president's explosive allegations were based on briefings from intelligence or law enforcement officials — which could mean that Trump was revealing previously unknown details about an investigation — or on something else, like a news report.

His decision to lend the power of his office to such a charged claim against his predecessor — without offering any initial proof — was remarkable, even for a leader who has repeatedly shown himself willing to make assertions that are false or based on dubious sources.

It would have been difficult for federal agents, working within the law, to obtain a wiretap order to target Trump's phone conversations. It would have

Obama continues on A13

Inside

» *Trump says he may shelve plans to cooperate with Russia against ISIS.* **Page A2**
» *Lisa Falkenberg writes the ruthless deportation of Jose Escobar is not what Trump promised.* **Page A3**
» *President has few options on North Korea.* **Page A27**

NOTE TO READERS

Delays in the delivery of newspapers on Satur-

Source: National Association of Corporate Directors, Houston Chronicle

Major Risks to Capital and the Energy Venture

Established Risks:

- Pricing Risk
- Technology Risk
- Regulatory Risk

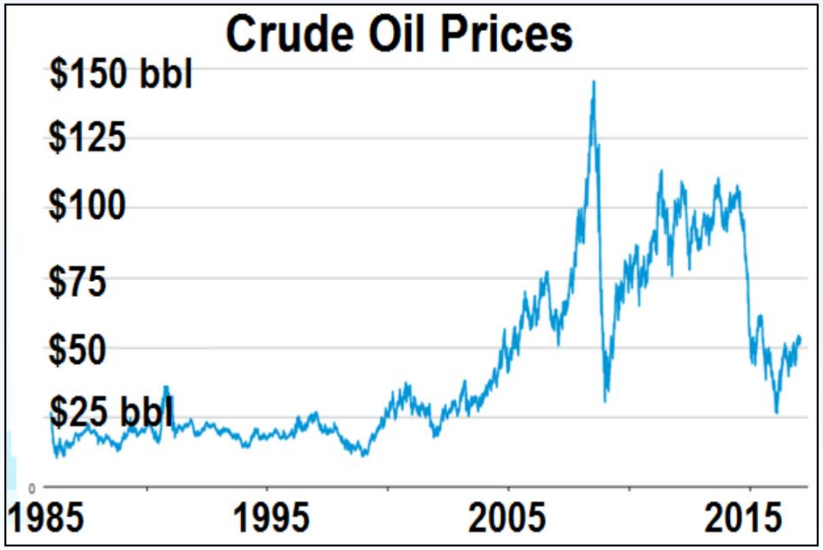
Developing Risks:

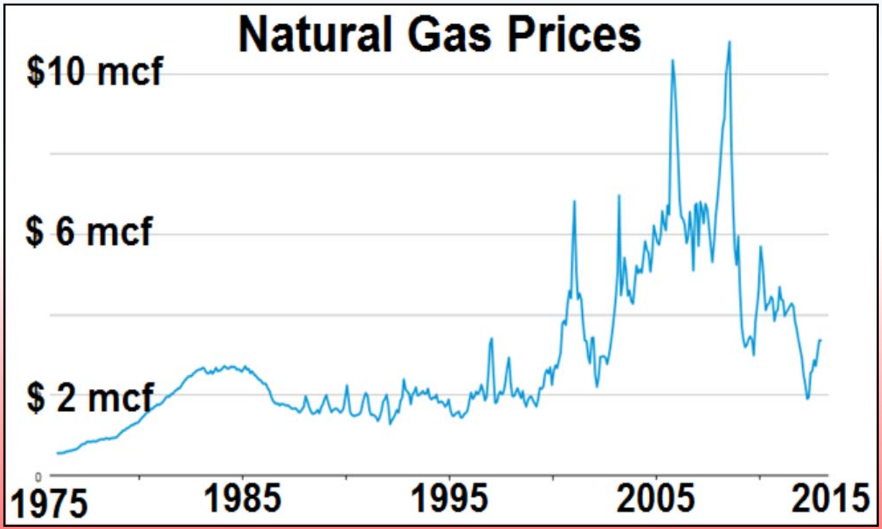
- Cybersecurity
- Data Breach
- Ransomware

The Attorney, Energy Executive or Investor must manage – or at least be able to evaluate – the major sector risks

Prices are Cyclical and Volatile

- Global Oil Demand Growth is Relentless
- Demand is Inelastic Short Term
- Geopolitical Issues Abound
- But Firms can Hedge to Reduce Risks

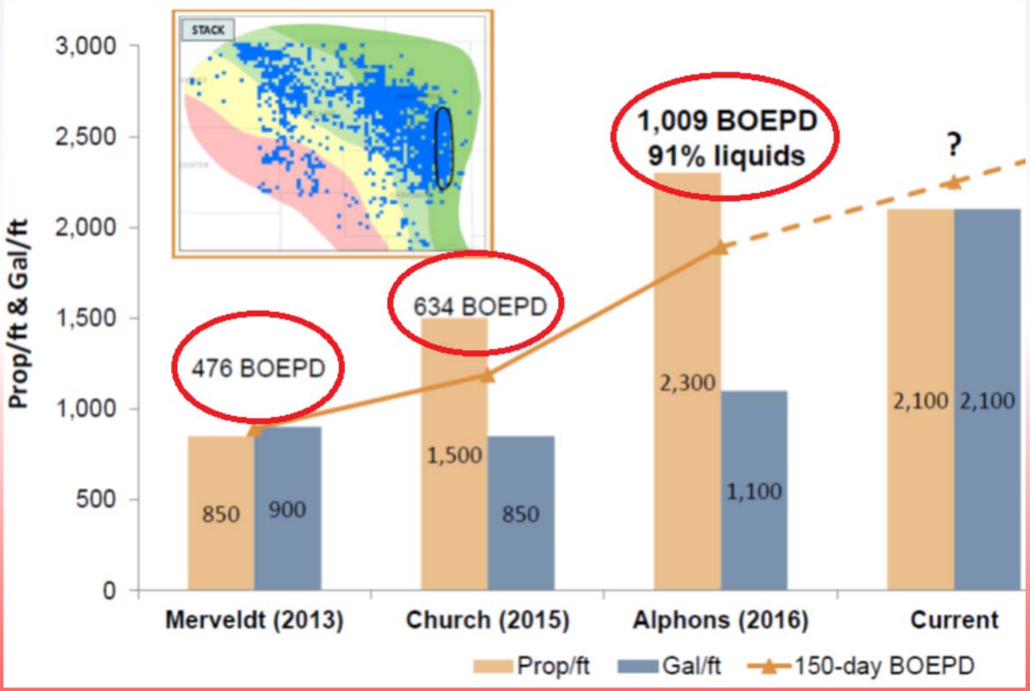


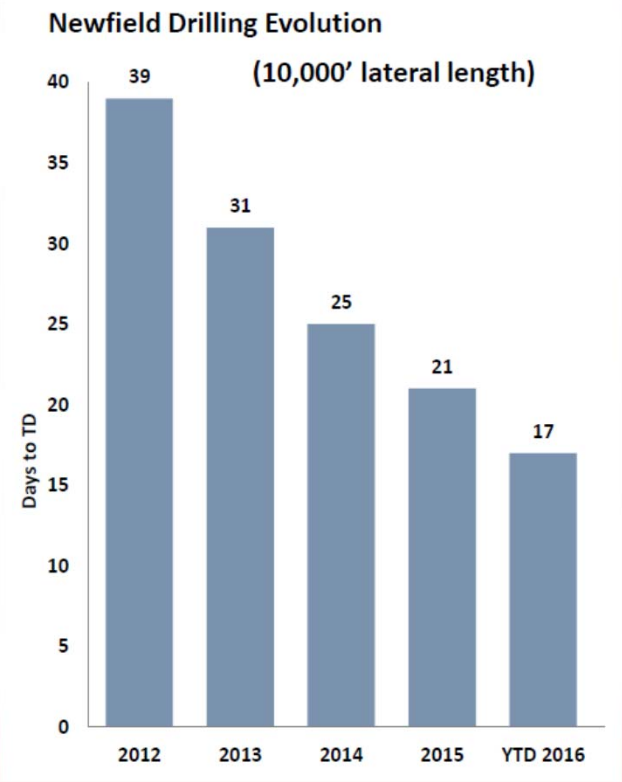


Source: U.S. Energy Information Administration

Technology Risks

Well costs are decreasing while technology relentlessly evolves - increasing efficiencies and economic returns

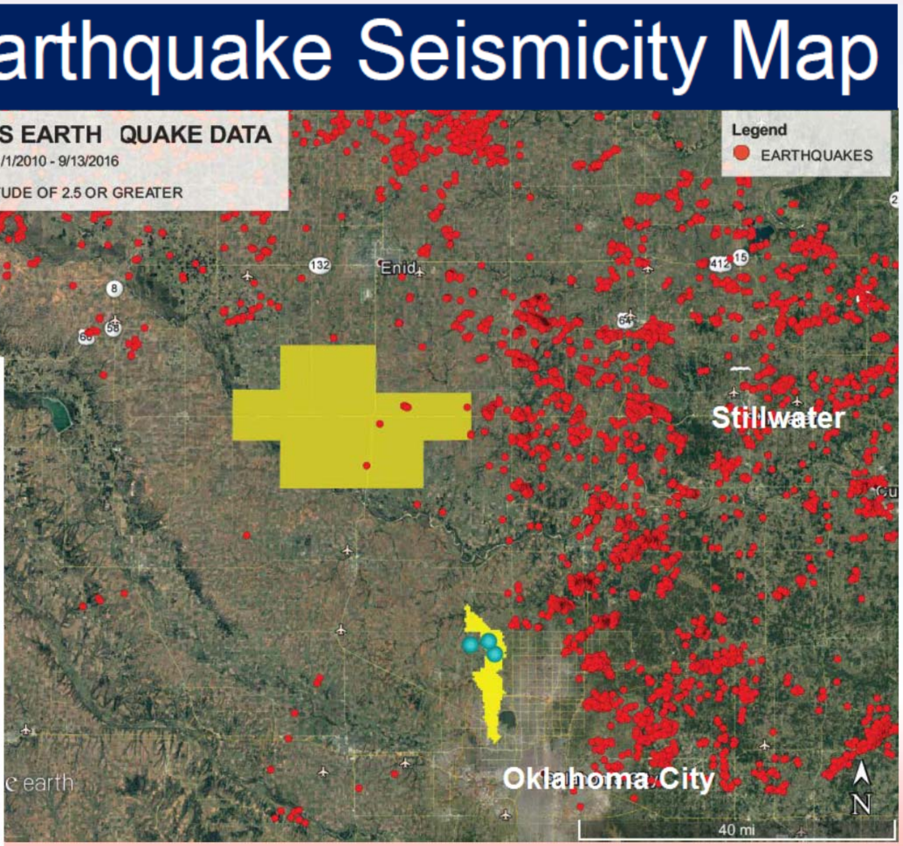


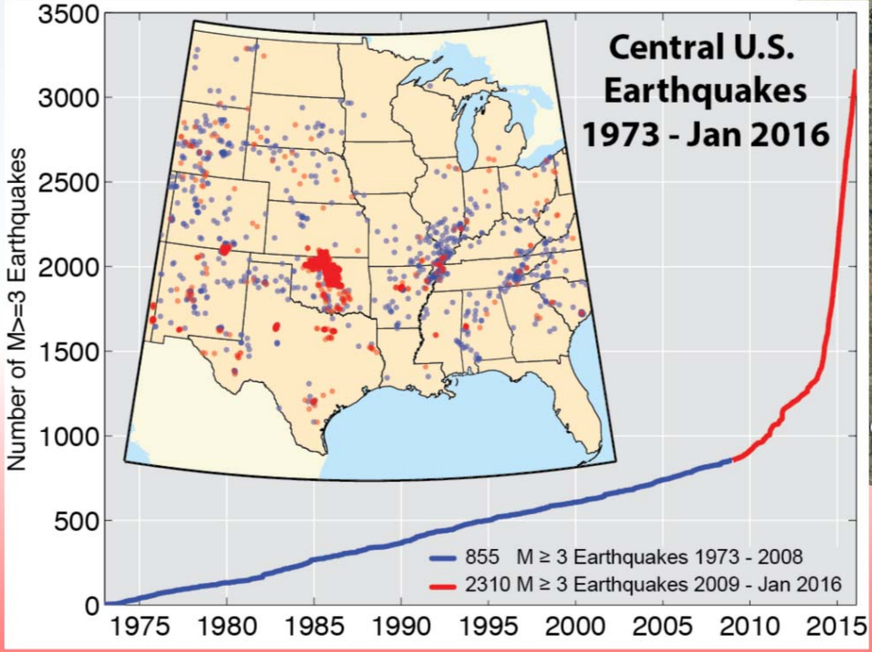


Source: Newfield Exploration Corporate Presentation

Regulatory Risks

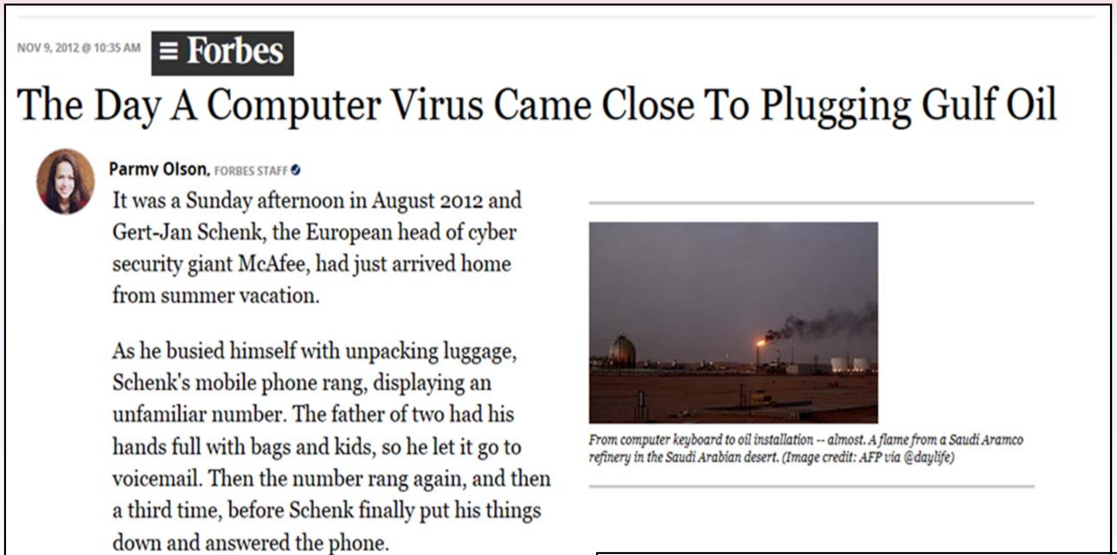
- Induced Seismic Events
- Spacing/Pooling Issues
- Water Use & Quality


Earthquake Seismicity Map
USGS EARTH QUAKE DATA
FROM 1/1/2010 - 9/13/2016
MAGNITUDE OF 2.5 OR GREATER
Legend
● EARTHQUAKES
Enid
Stillwater
Oklahoma City
N
40 mi



Sources: University of California Berkeley; Gastar Exploration Inc. Corporate Presentation

Evolving Risks: Cybersecurity & Data Breach



NOV 9, 2012 @ 10:35 AM ≡ Forbes

The Day A Computer Virus Came Close To Plugging Gulf Oil

Parmy Olson, FORBES STAFF

It was a Sunday afternoon in August 2012 and Gert-Jan Schenk, the European head of cyber security giant McAfee, had just arrived home from summer vacation.

As he busied himself with unpacking luggage, Schenk's mobile phone rang, displaying an unfamiliar number. The father of two had his hands full with bags and kids, so he let it go to voicemail. Then the number rang again, and then a third time, before Schenk finally put his things down and answered the phone.

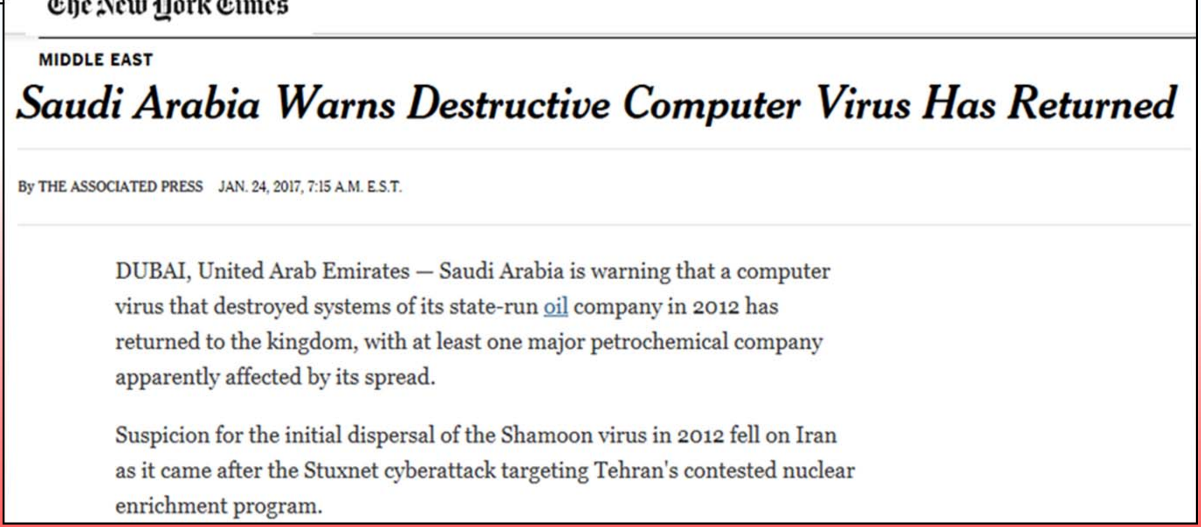
From computer keyboard to oil installation -- almost. A flame from a Saudi Aramco refinery in the Saudi Arabian desert. (Image credit: AFP via @daylife)

Virus shut down office system:

35,000 computers infected
1,000 servers infected
50,000 hard drives replaced

Impact lasted for months

Saudi Arabia produces 9.5 million barrels of oil per day – 10% of global supply!



The New York Times

MIDDLE EAST

Saudi Arabia Warns Destructive Computer Virus Has Returned

By THE ASSOCIATED PRESS JAN. 24, 2017, 7:15 A.M. E.S.T.

DUBAI, United Arab Emirates — Saudi Arabia is warning that a computer virus that destroyed systems of its state-run oil company in 2012 has returned to the kingdom, with at least one major petrochemical company apparently affected by its spread.

Suspicion for the initial dispersal of the Shamoon virus in 2012 fell on Iran as it came after the Stuxnet cyberattack targeting Tehran's contested nuclear enrichment program.

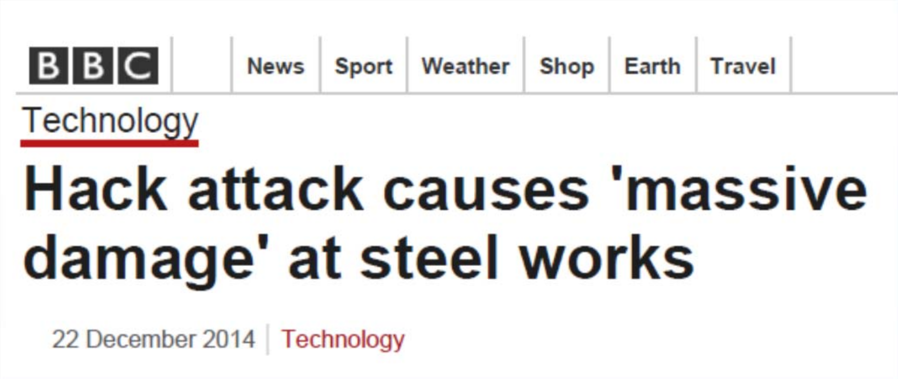
Sources: Forbes, New York Times

Operating System Breach

An attack on an operating system can have catastrophic consequences

Difficult to quantify cyber risk:

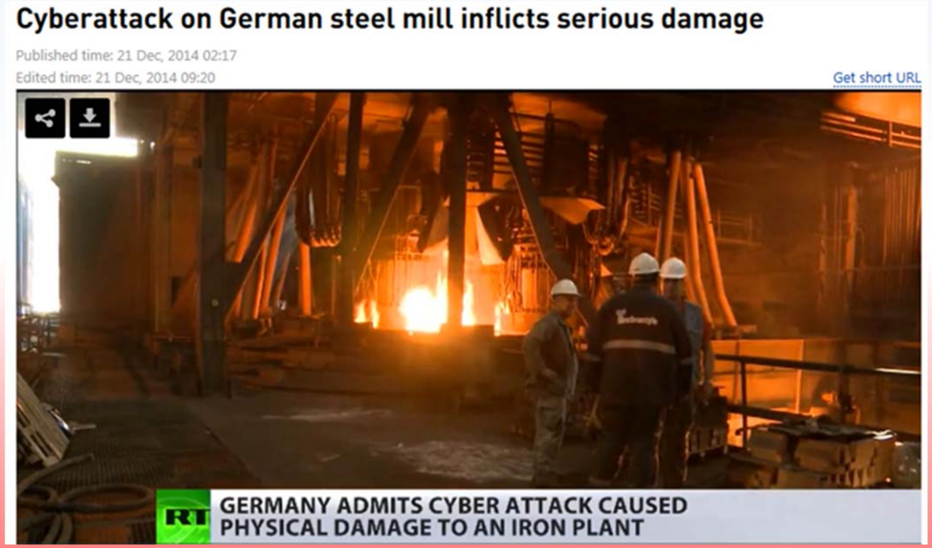
- Corporate victims generally do not disclose
- U.S. Department of Homeland Security generally does not disclose
- Other state and federal agencies generally don't disclose



Technology

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology



Cyberattack on German steel mill inflicts serious damage

Published time: 21 Dec, 2014 02:17

Edited time: 21 Dec, 2014 09:20

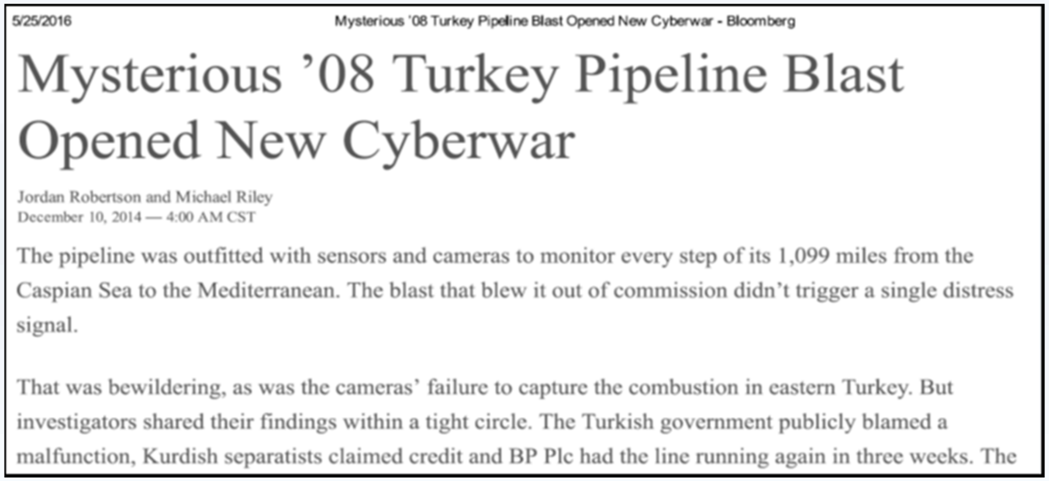
Get short URL
RT
GERMANY ADMITS CYBER ATTACK CAUSED
PHYSICAL DAMAGE TO AN IRON PLANT

Sources: BBC, RT, K&L Gates

Pipeline System Cyber Breach

Baku Tbilisi Ceyhan (BTC) 1,100 mile pipeline:

- Security cameras disabled
- Data monitoring and control system disabled
- 30,000 barrels of oil spilled
- $1 billion in lost revenue
- 2008 blast - first reported as cyber breach in 2014 by Bloomberg News



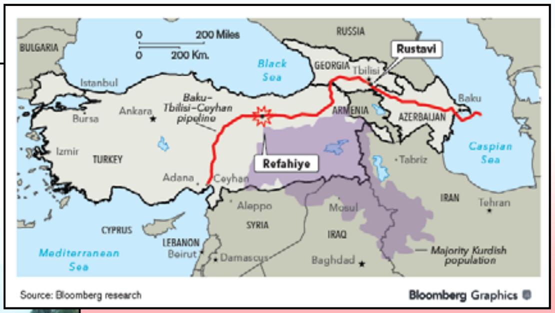
5/25/2016 Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar - Bloomberg

Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar

Jordan Robertson and Michael Riley
December 10, 2014 — 4:00 AM CST

The pipeline was outfitted with sensors and cameras to monitor every step of its 1,099 miles from the Caspian Sea to the Mediterranean. The blast that blew it out of commission didn't trigger a single distress signal.

That was bewildering, as was the cameras' failure to capture the combustion in eastern Turkey. But investigators shared their findings within a tight circle. The Turkish government publicly blamed a malfunction, Kurdish separatists claimed credit and BP Plc had the line running again in three weeks. The



Source: Bloomberg research

Bloomberg Graphics

Source: Bloomberg

General Cyber Regulatory Environment

Difficult subject matter for regulators:

- Rapidly evolving nature of cyber threats
- Industry specific threats, general rules can be too broad
- Time needed to propose rules / take comments
- Lack of ability to quickly revise obsolete rules
- Difficulty sculpting rules that are effective rule yet flexible enough to apply in different operating environments

Some of the regulators have adopted industry specific rules and regulations, but many require “reasonable procedures” versus specific standards

Source: K&L Gates

Energy Sector Cyber Environment

Regulatory Structure is of Recent Origin and Evolving Due to the Recent Nature of the Threat

- Most regulators require “reasonable” plans to prevent Cyber issues
- The appropriate “standard of care” is evolving as are “best practices”
- TSA suggests “best practices” that can be adopted by pipelines
- NIST “Cybersecurity Framework” identifies best practices by industry that can be adopted and utilized
- Non-specific guidelines provide for more flexibility in meeting cybersecurity goals

What are “reasonable procedures” to address the cyber threat?

Sources: NIST, TSA, DOT

Cybersecurity Risk Assessment

Risk = Threat x Consequences x Vulnerability

Dr. Frederick Chang, Director
Darwin Deason Institute for Cyber Security
Southern Methodist University

Degree of "Threat" difficult to quantify but:

- 82% of energy firms reported increased attacks in last year
- 53% of energy firms claimed increase in attacks was substantial
- The threat is dynamic in nature

"Consequences" of breach will vary with facilities but:

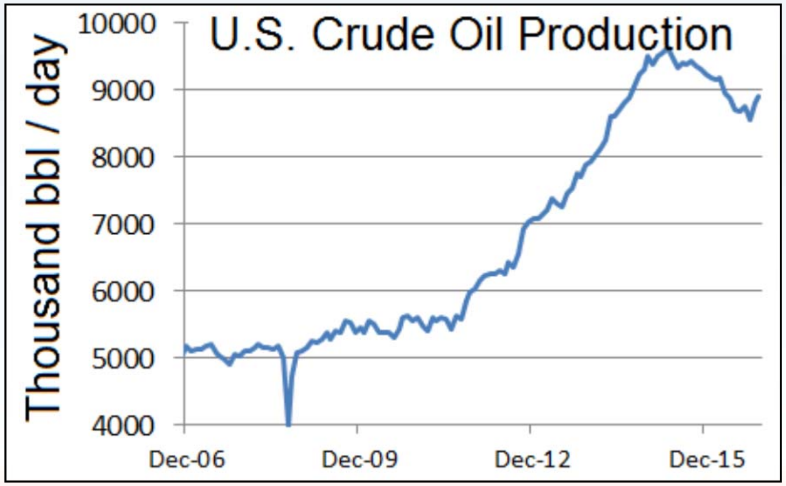
- Energy sector generally has higher consequence events
- Widespread and concentrated harm across economic sectors
- Asymmetrical harm possible

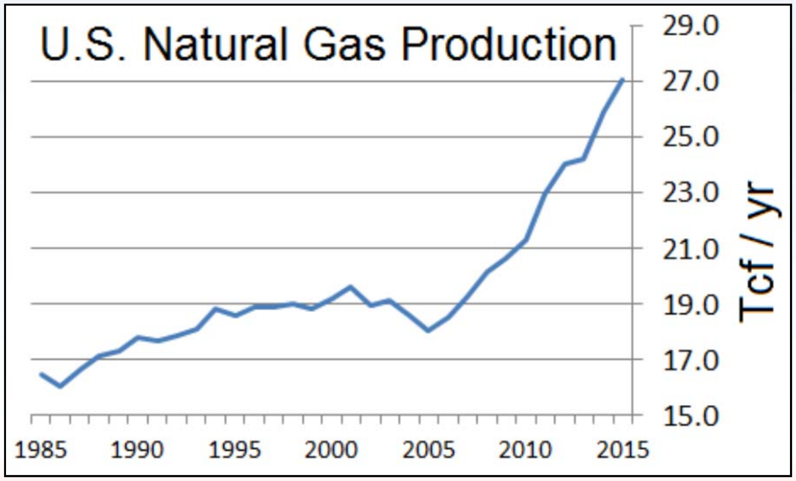
Source: SMU, Insurance Business Magazine, K&L Gates

Risk = Threat x Consequences x Vulnerability

Dr. Frederick Chang, Director
Darwin Deason Institute for Cyber Security
Southern Methodist University

"Vulnerability" component:





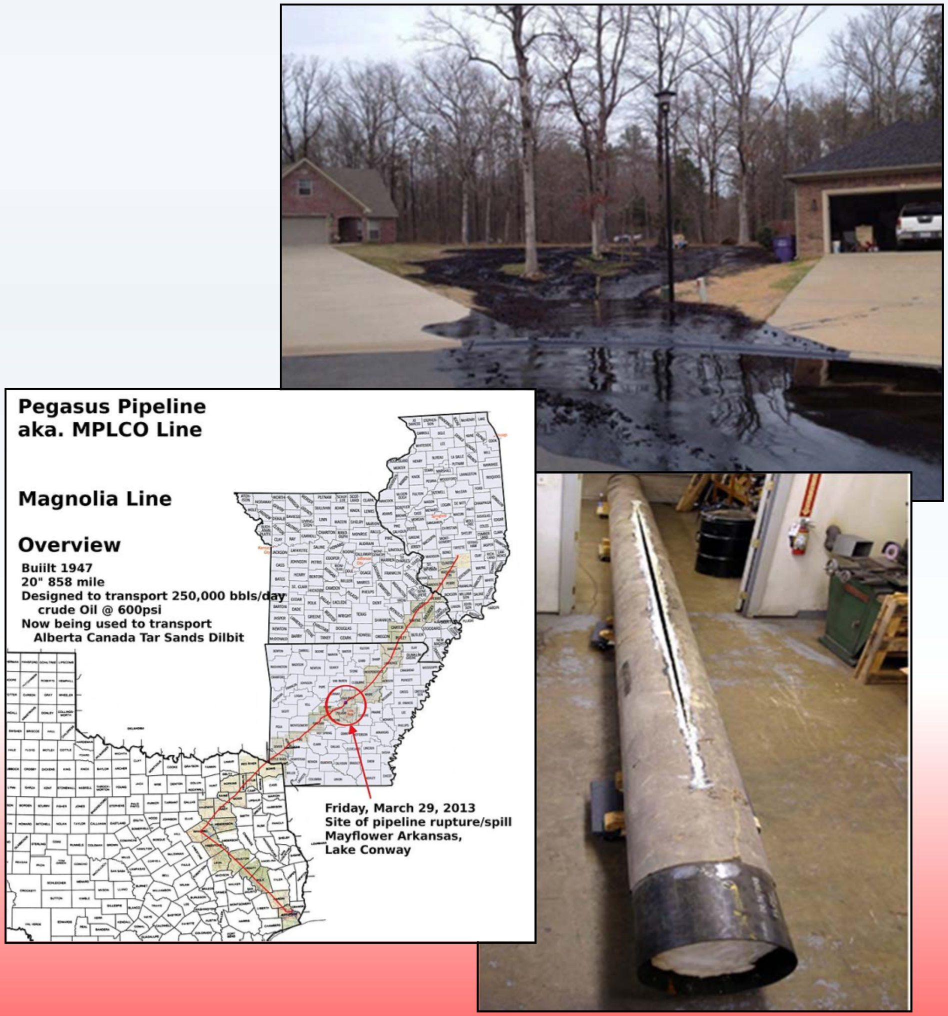
More Crude Oil and Natural Gas Being Transported Domestically

Source: U.S. Energy Information Administration

Our Liquids Pipeline System is Dated

Pipeline Hazardous Materials Safety Administration (PHMSA) studies:

- Corrosion, low frequency weld issues
- Roughly one-quarter of hazardous liquids pipeline pre-1970 era
- Cost $50 billion to replace
- Preventative testing not very effective
- Leak detection systems problematic



Pegasus Pipeline
aka. MPLCO Line

Magnolia Line

Overview

Buiilt 1947
20" 858 mile
Designed to transport 250,000 bbls/day
crude Oil @ 600psi
Now being used to transport
Alberta Canada Tar Sands Dilbit

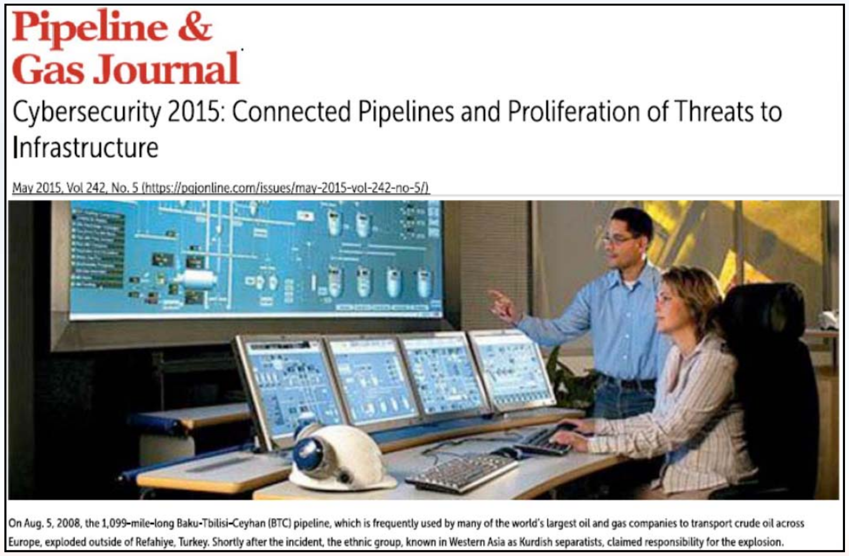
Friday, March 29, 2013
Site of pipeline rupture/spill
Mayflower Arkansas,
Lake Conway

Source: PHMSA, U.S. Department of Transportation

SCADA or ICS Data & Control Systems

“Supervisory Control and Data Acquisition” (SCADA) /
“Industrial Control Systems” (ICS)

- Collects operational data real time
- Controls system, pressure, valves, etc.
- Recent studies:
  - SCADA systems “extremely vulnerable”
  - “Alarming level” of SCADA cybersecurity threats
  - Systems can be out of date



Pipeline & Gas Journal

Cybersecurity 2015: Connected Pipelines and Proliferation of Threats to Infrastructure

May 2015, Vol 242, No. 5 (https://pgjonline.com/issues/may-2015-vol-242-no-5/)

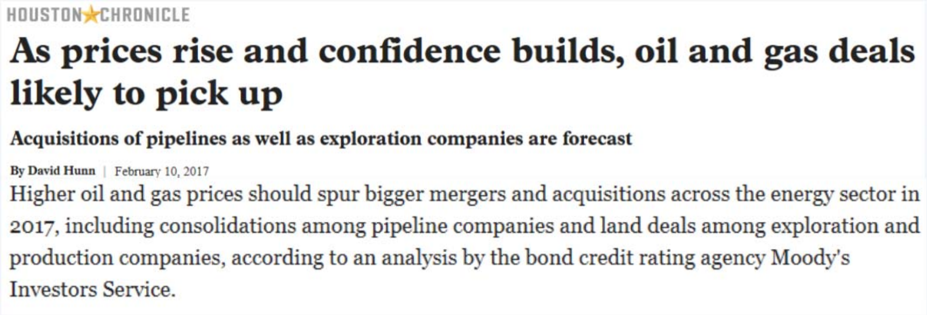
On Aug. 5, 2008, the 1,099-mile-long Baku-Tbilisi-Ceyhan (BTC) pipeline, which is frequently used by many of the world's largest oil and gas companies to transport crude oil across Europe, exploded outside of Refahiye, Turkey. Shortly after the incident, the ethnic group, known in Western Asia as Kurdish separatists, claimed responsibility for the explosion.

Source: Pipeline & Gas Journal

Third Party Contractor Risks

Risk of data leak / deal disclosure due to cyber breach

- M & A activity increasing
- Property sales and transactions increasing
- Requires:
  - Title opinions
  - Title curative
  - Due diligence
  - Financing
  - Partner agreements
  - Regulatory approval



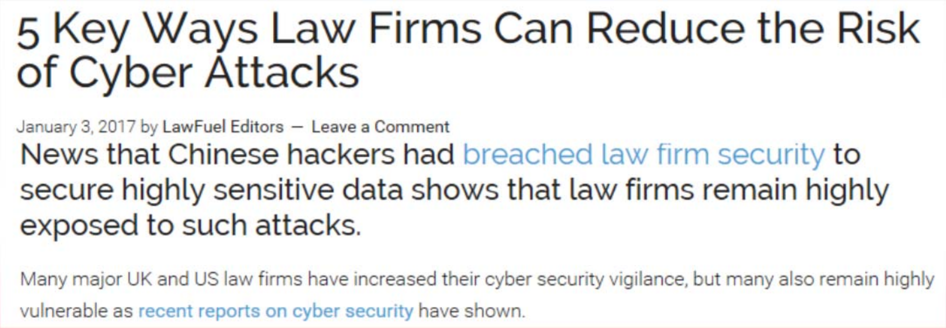
HOUSTON★CHRONICLE

As prices rise and confidence builds, oil and gas deals likely to pick up

Acquisitions of pipelines as well as exploration companies are forecast

By David Hunn | February 10, 2017

Higher oil and gas prices should spur bigger mergers and acquisitions across the energy sector in 2017, including consolidations among pipeline companies and land deals among exploration and production companies, according to an analysis by the bond credit rating agency Moody's Investors Service.

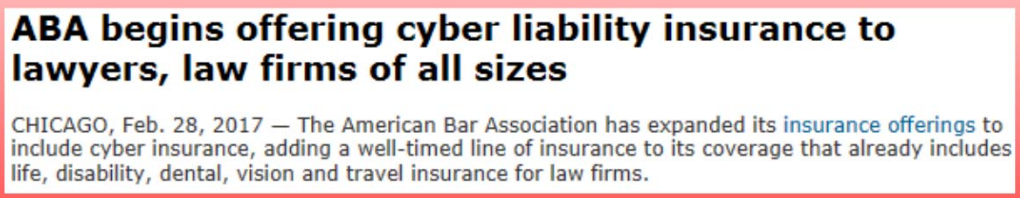


5 Key Ways Law Firms Can Reduce the Risk of Cyber Attacks

January 3, 2017 by LawFuel Editors — Leave a Comment

News that Chinese hackers had breached law firm security to secure highly sensitive data shows that law firms remain highly exposed to such attacks.

Many major UK and US law firms have increased their cyber security vigilance, but many also remain highly vulnerable as recent reports on cyber security have shown.



ABA begins offering cyber liability insurance to lawyers, law firms of all sizes

CHICAGO, Feb. 28, 2017 — The American Bar Association has expanded its insurance offerings to include cyber insurance, adding a well-timed line of insurance to its coverage that already includes life, disability, dental, vision and travel insurance for law firms.

Source: Houston Chronicle, ABA, LawFuel

Scorecard: Energy Sector Risk Assessment

Cyber Risk = Threat x Consequences x Vulnerability

Threat	Consequences	Vulnerability
Substantial and increasing	Substantial	Substantial

≡ Forbes

NOV 4, 2015 @ 12:05 PM

The Biggest Cybersecurity Threat: The Energy Sector

Michael Krancer, CONTRIBUTOR

I cover the world of energy and policy.

It's cyber attacks on the energy space, not the consumer credit space, that could cripple the United States — or any country — as well as bring about a collapse of order and society that most of us associate with apocalyptical scenarios.

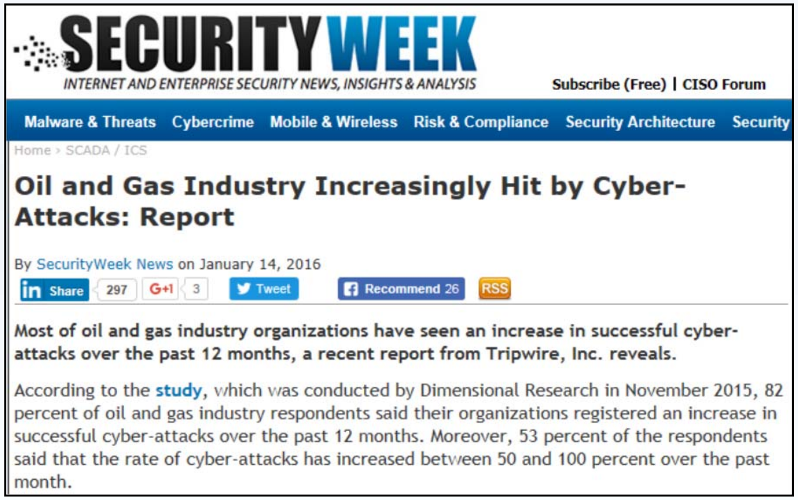
Michael Krancer, Forbes

Source: Forbes

Common Law Liability for Cyber Breach

Evolving issues:

- Foreseeability
- Negligence
- Negligence per se
- Duty of reasonable care

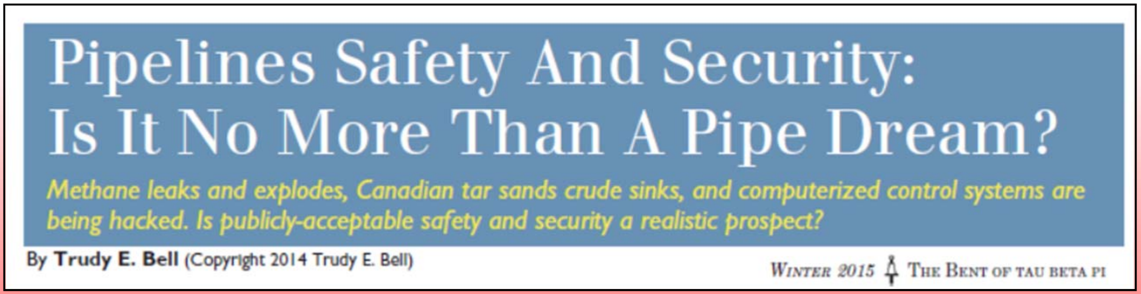


Oil and Gas Industry Increasingly Hit by Cyber-Attacks: Report

By SecurityWeek News on January 14, 2016

Most of oil and gas industry organizations have seen an increase in successful cyber-attacks over the past 12 months, a recent report from Tripwire, Inc. reveals.

According to the study, which was conducted by Dimensional Research in November 2015, 82 percent of oil and gas industry respondents said their organizations registered an increase in successful cyber-attacks over the past 12 months. Moreover, 53 percent of the respondents said that the rate of cyber-attacks has increased between 50 and 100 percent over the past month.



Pipelines Safety And Security: Is It No More Than A Pipe Dream?

Methane leaks and explodes, Canadian tar sands crude sinks, and computerized control systems are being hacked. Is publicly-acceptable safety and security a realistic prospect?

By **Trudy E. Bell** (Copyright 2014 Trudy E. Bell)

WINTER 2015 THE BENT OF TAU BETA PI

Source: Security Week, The Bent of Tau Beta Pi

Addressing Cyber Risks

“Reasonable procedures” an entity could focus on:

- Possible infection pathways and firewalls
- System access policies
- Employee and contractor training
- Subdivide networks to limit damage
- Identify chokepoints to cut off infection
- Periodically assess security
- Data encryption and retention policies
- Software patches & antivirus software
- Disaster / recovery protocols

Rely on experts to advise on a prudent course of action

Source: SMU, NACD, Pipeline & Gas Journal

Cybersecurity Strategy Suggestions

1. Designate IT expert responsible and provide resources
2. IT expert provides training to employees and contractors
3. IT expert restricts access / adopts company wide rules
4. CEO reports to board quarterly on cyber issues
5. Separate office / operational / web servers
6. If serious breach occurs, board of directors informed

Source: NACD, SMU

Concluding Thoughts

- Cyber threats are a growing issue
- Threats quickly evolve and morph
- The issue is global in nature
- Difficult to regulate
- Damage can be asymmetrical
- Prudent entities will address the threat

Contact Information

Joseph R. Dancy

Executive Director, The University of Oklahoma College of Law
Oil and Gas, Natural Resources, and Energy Center (ONE C)

(405) 325-4699

The University *of* Oklahoma
COLLEGE OF LAW