Utilities & Energy Infrastructure: In the Crosshairs of Cyber Terrorists

Brig Gen Charly Shugg, USAF, Retired
Partner | Chief Operating Officer
Sylint Group, Incorporated

The Question of the Day

How did we come up with the company name **"Sylint"** and what does it mean?

- Sylint (si-lent): from the Greek variant "**Syl**-" meaning "together" and the suffix "-**int**" comes from the variant meaning "information", usually associated with secret information regarding the enemy or about hostile activities, or "**int**elligence"

Sylint Group, Inc

Incident Response, Cyber Security, Digital Data Forensics (SRQ 1999)

- Clients - Fortune 500, Gov’t, Public, Private, High Profile, LEO
- 1 of 16 Companies Accredited by National Security Agency (NSA) and NSCAP for Cyber Incident Response Assistance (CIRA)
- 1 of 11 Companies Authorized to Investigate Card Breaches (PCI) in USA for VISA, MasterCard, AMEX: PCI Forensic Investigators (PFI)
- NSA, DoD/Air Force – Intelligence Centric Methodologies
- DHS Industrial Control System (ICS) Joint Working Group Member

What is Your Position?

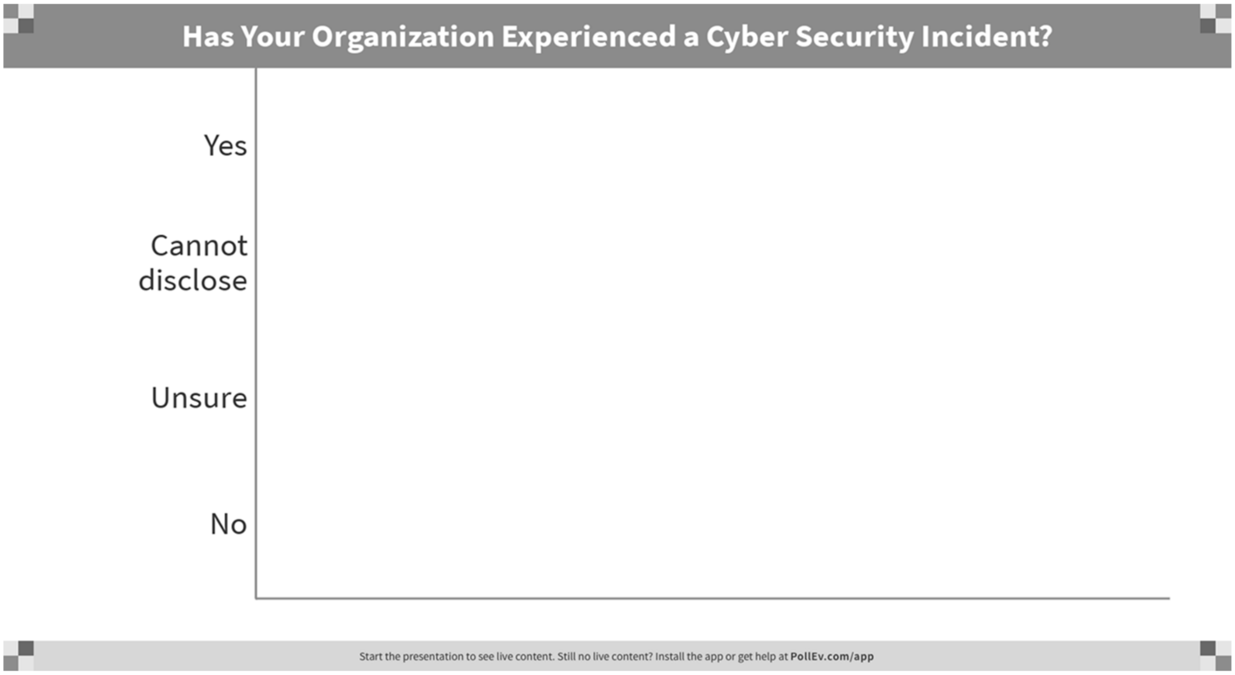
Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

Oil & Gas Industry “Big Picture”

Your Kingdom

You

Threats /
Enterprise Risk

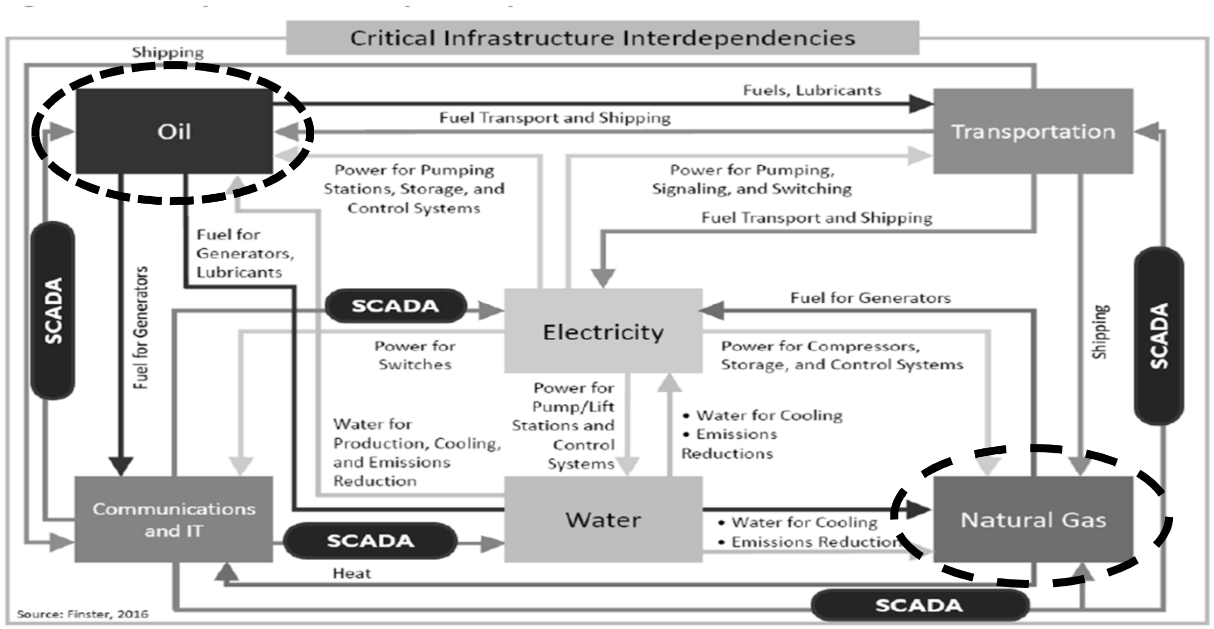


Has Your Organization Experienced a Cyber Security Incident?

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

Why Gas & Oil Industry?

- National Critical Infrastructure with Multiple Interdependencies


Critical Infrastructure Interdependencies
Shipping
Oil
Fuels, Lubricants
Fuel Transport and Shipping
Transportation
Power for Pumping Stations, Storage, and Control Systems
Power for Pumping, Signaling, and Switching
Fuel Transport and Shipping
SCADA
Fuel for Generators
Fuel for Generators, Lubricants
SCADA
Electricity
Fuel for Generators
Power for Switches
Power for Compressors, Storage, and Control Systems
Shipping
SCADA
Power for Pump/Lift Stations and Control Systems
Water for Production, Cooling, and Emissions Reduction
• Water for Cooling
• Emissions Reductions
Communications and IT
SCADA
Water
• Water for Cooling
• Emissions Reduction
Natural Gas
Heat
SCADA

Source: Finster, 2016

Why Gas & Oil Industry?

- National Critical Infrastructure & Interdependencies
- High Net Worth Industry – Economic Effect
- Extensive Geographic Network
- Volatile Product (Huge Bomb)

Does Your Organization Discuss the Possibility of a Devastating Attack/Impact?

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

Who is the Potential Threat?

Threat Capability and Intention Evolution…

Nation States

Organized Crime

Activists

Terrorists

Terrorist Objectives

Terrorist groups commits *__acts of violence__** *to:*

- Produce wide spread fear
- Attract the attention of the media
- Create doubt that the government can provide for and protect its citizens
- Extort money
- Satisfy vengeance

* ***Maximize Death and Destruction***

Conventional Terrorist Tactics

Prepositioned Bombs & Suicide Bombs

Terrorist Issues:

- Material Preparations Detected & Thwarted
- Reconnaissance Preparations Detected & Thwarted
- Attrition Rate of Suicide Bomber Volunteers
- Post Attack Detection (Eye witness, video, forensics, etc.) & Capture

Risk Reduction Solution:

- Physical Security for Physical Attack

Good News: We Eventually Track Down The Attacker

Emerging Terrorist Tactics – Cyber Attack

Turn "Physical" Critical Infrastructure into Lethal Bomb

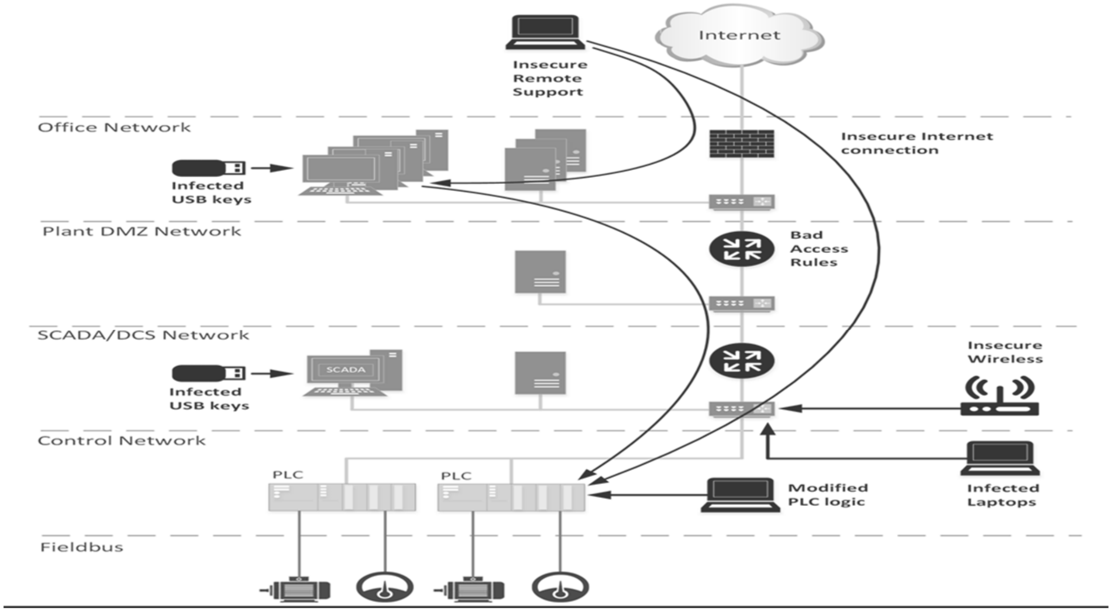
Terrorist Issues:

- ~~Material Preparations Detected & Thwarted~~ No Longer a Factor
- ~~Reconnaissance Preparations Detected & Thwarted~~ No Longer a Factor
- ~~Attrition Rate of Suicide Bomber Volunteers~~ No Longer a Factor
- ~~Post Attack Detection (Eye witness, video, forensics, etc.) & Capture~~ No Longer a Factor

Risk Reduction Solution:

- Cyber Security for Physical Attack

Bad News: We Probably Will Never Track Down The Attacker



Historical OT Attacks

"CrashOverride" (also called "Industroyer")

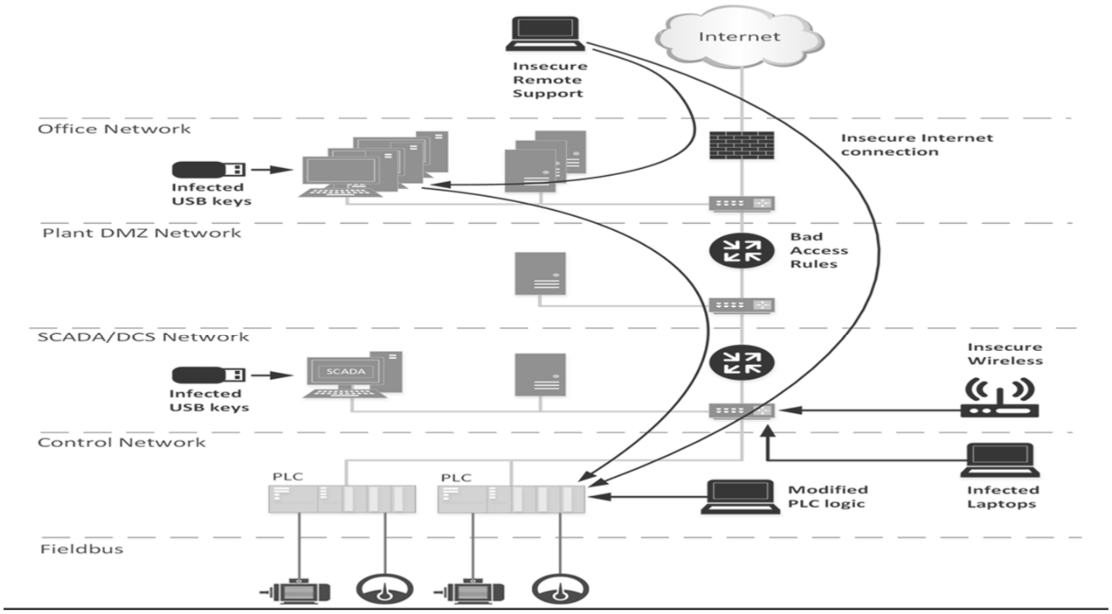
- Targets ICS ***<u>but not against vulnerabilities and exploits</u>***
- *Leveraged legitimate grid operations against itself - Ukrainian* power grid
  - Infects Windows machines, automatically maps out control systems and locates target equipment
  - Sends network logs to understand how unique control systems function over time

"Triton"

- Threat knowledgeable of IT/OT operations and able to navigate network
- Exploited previously unknown vulnerability in Schneider's Triconex safety system firmware
  - Attack occurred against Middle Eastern Oil Company.
  - Attributed to a sophisticated nation state cyber effort

Your Role

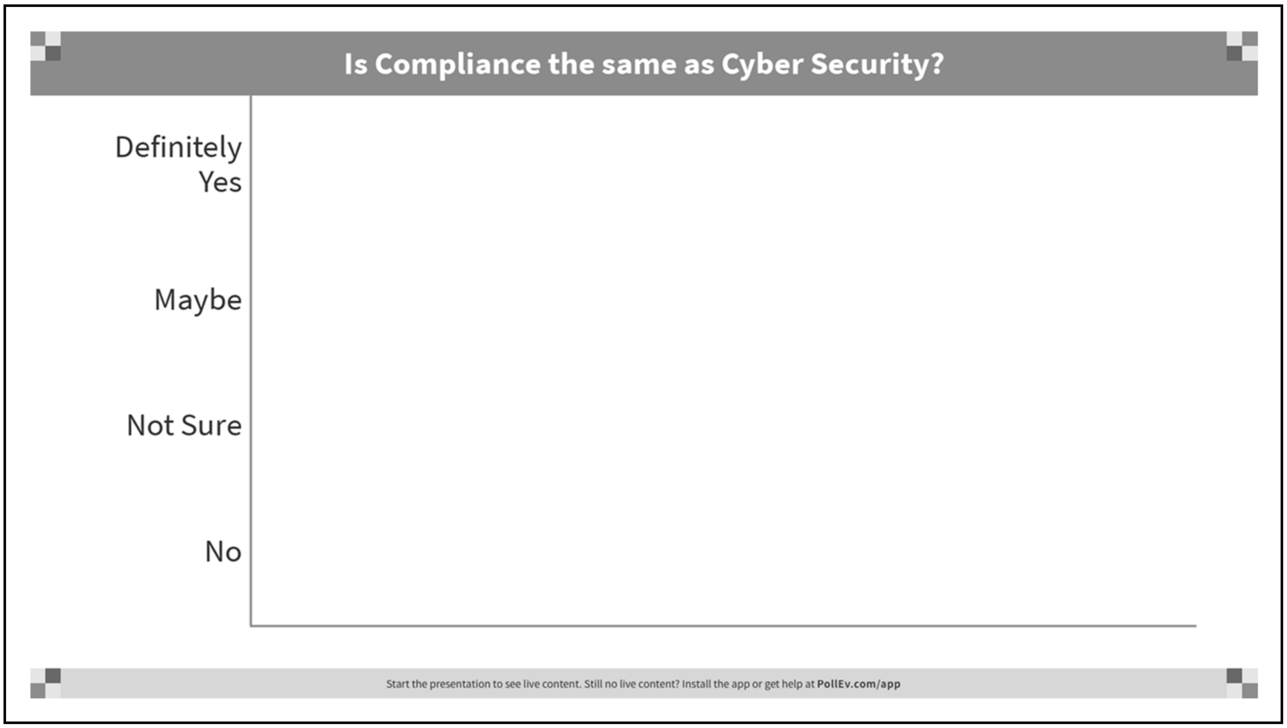
Understand the IT/OT interaction and potential vulnerabilities/impact



Your Role

Understand the IT/OT interaction and potential vulnerabilities/impact

Understand the difference between “Compliance” vs “Security”



Is Compliance the same as Cyber Security?

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

Compliance vs Security

Requirement for “Protection”…Network Firewall

Compliance vs Security

Requirement for “securing assets”…encrypting Data

Compliance vs Security

Requirement for "monitoring critical assets"…Collect and Analyze Network Security Logs

Your Role

Understand the IT/OT interaction and potential vulnerabilities/impact

Understand the difference between "Compliance" vs "Security"

Convince Senior Management of Preparation Benefits in Cyber Risk Management

Ask the Right Questions

Who is responsible for cyber security risk (Enterprise/IT/Convergence between IT & OT)?

What are the cyber security's reportable Key Performance Indicators (KPIs) for ICS/SCADA?

How is overall cyber risk posture (to include ICS) communicated to senior executives and board of directors?

Are we doing it "right" from the start…and maintain the highest standards of service and safety?

Contact Information

Sylint

Charly Shugg
Partner | Chief Operating Officer
cshugg@usinfosec.com

Sylint Group
Sarasota, Florida
941-951-6015
www.sylint.com