



CLYDE & Co

Cyber Threats to Pipeline Safety:
Vulnerabilities and Evolving
Standards of Care

Joseph A. Walsh II
Destinee N. Finnin
Clyde & Co US LLP

Pipeline Cybersecurity

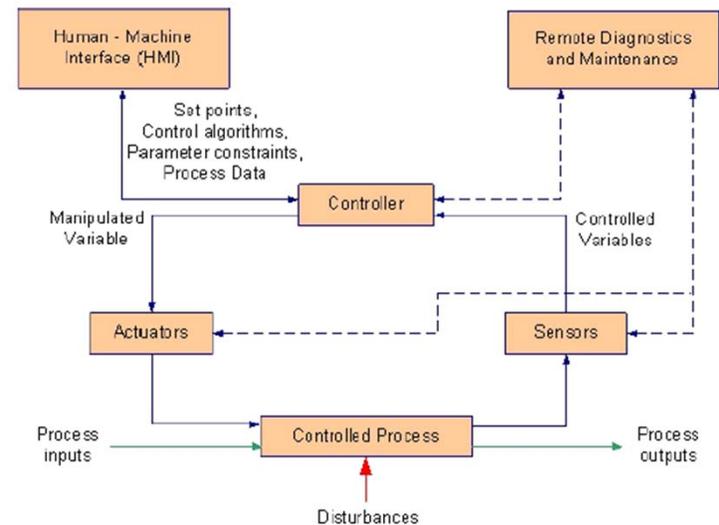
- **Types of Disruptions**
- **Standards of Care**
- **Risks and Liabilities**
- **Insurance Implications**



Photo Source:
www.icscybersecurityevent.com

Industrial Control Systems (ICS) Generally:

- **Command and control networks and systems designed to support industrial processes**
- **Encompasses several types of control systems:**
 - Supervisory Control and Data Acquisition Systems (SCADA)
 - Distributed Control Systems (DCS)
 - Programmable Logic Controllers (PLC)
- **Allow remote command and control**
 - Economic and Ease of Use Benefits
 - Security Vulnerabilities
- **Isolated \leftrightarrow Highly Interconnected**



Cyber Threats to Industrial Control Systems:

-Malicious Attacks

- Intentional/Targeted Criminal Cyber Attacks
- Advanced Persistent Attacks (APT)

-Accidental Introductions/Migrations from IT Systems

- Laptops
- Websites
- E-mails
- USB Drives
- External Computers

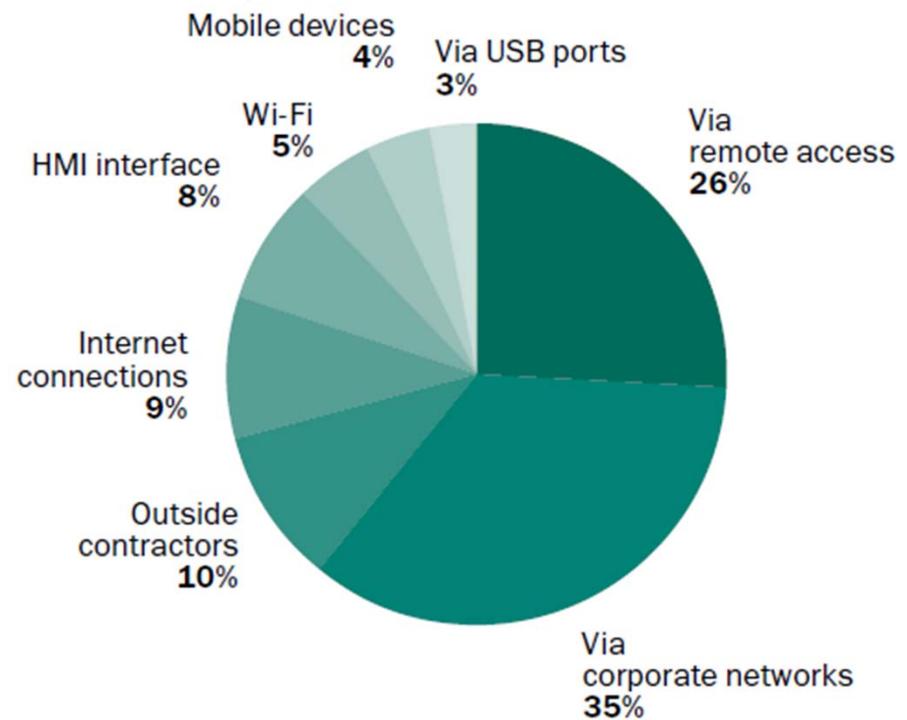


Figure: Sources of Malicious Code in Industrial Systems

Photo & Data Source: Kaspersky

Broad Range of Targets for Cyber Attacks



Photo Credit: Americanbanker.com

-**Retailers**: Target, Pizza Hut, & The Home Depot

-**Entertainment Industry**: Sony Pictures

-**Financial Institutions**: JP Morgan Chase & Co.

-**Maritime Industry**: Hyundai Merchant Marine, Various Port Authorities, Oil Rigs

-**Heavy Industry**: Large Plants

-**Public Utilities**: Water & Power

Case Study: Baku-Tbilisi-Ceyhan (BTC) Pipeline (Turkey 2008)

-1,099 mile pipeline carrying crude oil from the Caspian Sea

-Main Weapon: A Keyboard

-Circumvented all sensors and security mechanisms

-Western Reactions:

- Watershed Event
- Re-wrote the History of “Cyberwar”

- New Methods for Terrorists, International Rivals, and Political Enemies alike

- “One of Most Secure Pipelines in the World”



Photo Source: Bloomberg Technology

Case Study: Stuxnet (Iran 2010)

-Complex Malware

-Viewed as Transition from Stealing Information to Physical Destruction

-Target: Iranian Nuclear Program

-Altered Code Controlling Programmable Logic Controllers (PLCs)

-Two-Prong Approach:

- Part 1: Increase Centrifuge Pressure and Damage the Devices/Process
- Part 2: Record and Play-Back Normal Operations



Photo source: CNBC.com

Additional Examples

-April 2012: Malware Attack on Control System of Kharg Island in Iran

-August 2012: Shamoon Virus Attack on Control Systems of Saudi Oil Supplier

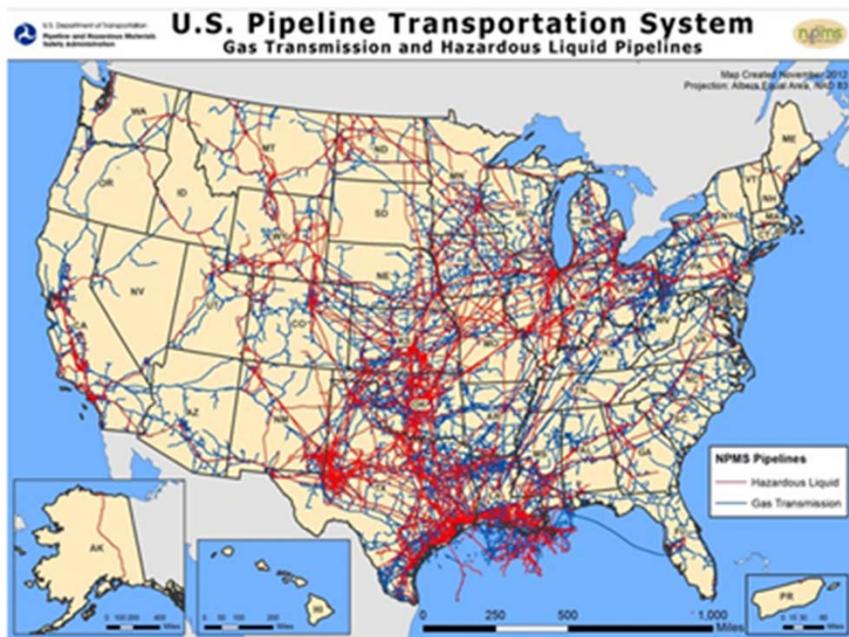
-January 2015: German Steel Mill Blast Furnace Control System Attack

-December 2015: Ukraine Power Companies SCADA Attack



Photo Source: American Security Project

U.S. is No Exception



Source: USDOT Pipeline and Hazardous Materials Safety Administration

Photo Source: tripwire.com

- Over 2.5 million miles of pipeline vulnerable to attack

- Oil
- Gas
- Other Hazardous Substances

- Vulnerabilities:

- A single pipeline has thousands of sensors, valves, pumps, and controllers which can be targeted
- Pipeline Facilities are Typically Unstaffed
- Similar ICS Systems Across Industries

-Deliberate Attacks:

- No successful attacks have been confirmed to date
- Several Attempts

Methodologies/Points of Entry

- Removable Media (USBs)
- External Computers/Devices
- Other Industry Computers
- Remote Access
- Internet Connections
- Corporate Networks
- Security Cameras
- Spear Phishing Emails
- Network Scanning
- Waterholing
- However, in a Majority of Incidents, the Access Points are Unknown



Pipeline Cybersecurity as a Safety Issue

Informational → Physical Threat

- Safety of:

- People
- Environment
- Property



Photo Source: Enerdynamics

- Risks:

- Ruptures
- Explosions
- Fires
- Releases/Spills

Pipeline Cybersecurity as a Financial and Operational Issue

- **Malware attacks account for approximately 35% of incidents in industrial networks**

- **Operational Issues:**

- Delays
- Shutdowns
- Hardware Failure due to Blocked Operations
- Lost Time, Productivity, and Growth

- **Financial Implications:**

- Up to \$3 trillion in losses across all industries

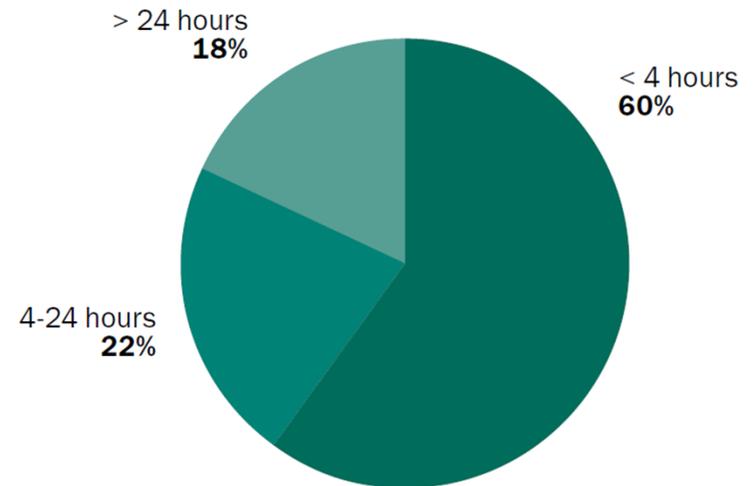
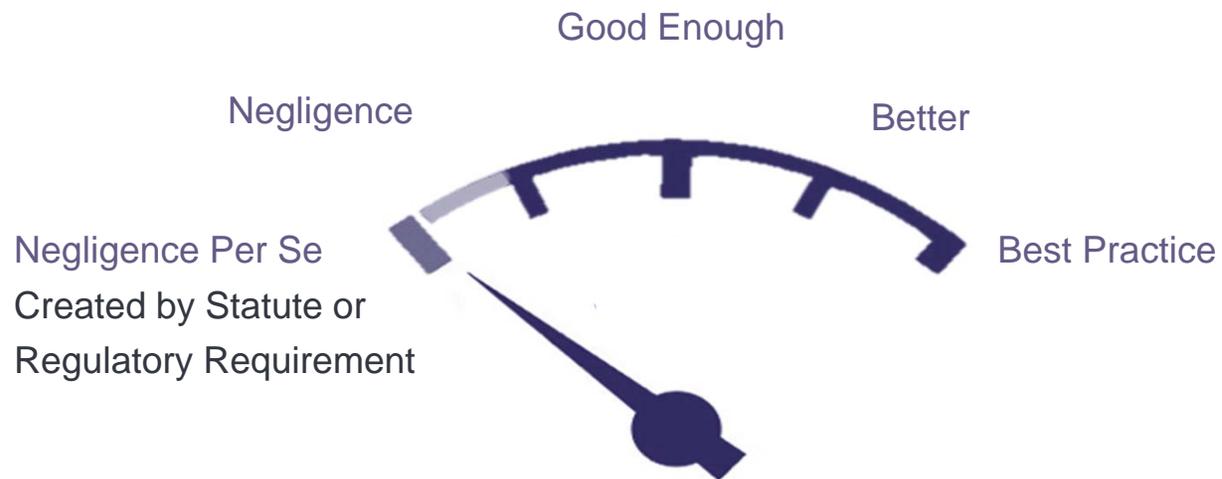


Figure: Industrial Process Downtime due to Malware Incidents

Photo & Data Source: Kaspersky

What is the Standard of Care?



National Institute of Standards and Technology (NIST)

- **Executive Order (EO) 13636 Improving Critical Infrastructure**
- **Cybersecurity Framework (CSF)**
 - Guidance- Not “One Size Fits All”
 - “Voluntary, industry-led cybersecurity standards and best practices”
 - Aids in Prioritizing and Maximizing Investments
 - Provides a Common Language
- **Industry Feedback and Next Steps**
 - Minor Modifications/Clarifications
 - Self-Assessment Criteria
 - Continued Outreach



**National Institute of
Standards and Technology**
U.S. Department of Commerce

Photo Source: nist.gov

Supporting Agencies/Programs

-Transportation Security Administration (TSA)

- Pipeline Security Guidelines
- Supports the NIST Cybersecurity Framework
- Cybersecurity Toolkit
- Voluntary Assessment Program with Federal Energy Regulatory Commission
- Works in Conjunction with the **Pipeline and Hazardous Materials Safety Administration (PHMSA)**

-Department of Homeland Security (DHS)

- Critical Infrastructure Cyber Community C³ Voluntary Program
- Chemical Facility Anti-Terrorism Standards (CFATS)



Photo Sources: forbes.com

Supporting Agencies/Programs (continued)

-United States Department of Energy

- Energy Sector Cybersecurity Framework Implementation Guidance

-Securities and Exchange Commission's Division of Corporation Finance

- Voluntary Disclosure Guidance



Potential Tort Liability: Failure to Meet “Standard of Care”



Photo Sources: e-discoveryteam.com,
www.wyndhamworldwide.com , & blog.caspio.com

Notable Case Law

- *T.J. Hooper*, 60 F.2d 737 (2d Cir. 1932)
- *Byrne v. Avery Ctr. for Obstetrics & Gynecology*, 314 Conn. 433 (Conn. 2014)
- *FTC v. Wyndham*, 799 F.3d 236 (3d Cir. 2015)

Consider the Possibility of “Borrowed” Standards of Care

- Regulatory Agencies’ “Guidance”
- State Laws
- Parallel Industry Standards
- Insurance Requirements

Potential Criminal Liability

Responsible Corporate Officer Doctrine

- Personal Liability- Both Civil and Criminal
- Liability Based on Position Alone for Violations of Public Welfare Statutes
- Area To Watch for Potential Expansion of Liability



Photo Source: www.forbes.com

Potential Limitations on Liability



Photo Source: www.ssousa.com

- Support Antiterrorism by Fostering Effective Technologies Act of 2002

- DHS Certification of Security Program
- Affords Liability Protections involving:
 - Jurisdiction
 - Defenses
 - Damages

- Potential Government Incentives

- Intended to Promote Compliance with the Framework
- Likely Not a Viable Limitation Mechanism

Insurance Coverage:

- Cyber Risks Typically Excluded from Traditional Commercial General Liability Policies
- Separate Cyber-Insurance Policies
 - Provide the most comprehensive coverage
- Supports and Furthers Best Practices
- Funding for Major Losses with Fair Risk Distribution



Photo Source: Forbes.com

Summary:

- Pipeline Cybersecurity is a rapidly growing area.
- These continuing developments, recently promulgated standards, as well as “borrowed” standards are evolving into a new standard of care.
- These changes have important implications with respect to liability and insurance coverage.



Photo Source:
www.icscopybersecurityevent.com

Questions?

360+

Partners

1800+

Legal professionals
worldwide

3000+

Total Staff

45

Offices across 6
continents

Clyde & Co US LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary. No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co US LLP.
© Clyde & Co US LLP 2016