Keeping the Lights On

Fundamentals of Industrial Control Risks, Vulnerabilities, Mitigating Controls, and Regulatory Compliance

© Copyright 2014 Netsecuris Inc. All rights reserved
Learning Goals

- Understanding definition of industrial controls
- Understanding differences between traditional IT networks vs. industrial control networks
- Understanding risks and mitigating controls associated with industrial controls
- Understanding regulatory compliance and service resilience
What is Industrial Control?
Industrial Control Defined

- A system that controls a process
- Industrial Control System – traditionally a general term defining several types of control systems used in industrial production
  - Distributed Control System (DCS)
  - Supervisory Control and Data Acquisition System (SCADA)
  - Remote Terminal Units (RTU)
  - Programmable Logic Controllers (PLC)
Why learn about this topic?

- Industrial controls are pervasive!
  - Utilities
  - Factories
  - Automobiles
  - Military
  - Data Centers
  - Appliances

- Industrial controls are being networked like traditional IT networks.
Industrial Controls that might Surprise You

- Environmental controls in your data center
- Missiles launched by the military
- Assembly line controller in a factory
- SCADA systems at utilities
- Gasoline pumps at a convenience store
T-shirt Question

Can you name an industrial control or application I have not already mentioned?
National Critical Infrastructures

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems
Get Involved

- Join a Cyber Security or Physical Security Working Group in your Sector.
  - https://www.dhs.gov/critical-infrastructure-sectors

- Join an Information Sharing Analysis Center (ISAC) in your industry.
  - http://www.isaccouncil.org/memberisacs.html
  - http://itlaw.wikia.com/wiki/Information_Sharing_and_Analysis_Center
What’s important in the industrial space

- Life Safety is foremost.
- Reliability is a close second.
- Integrity and Availability is primary.
- Confidentiality is secondary or not important at all.
What can happen

- Cyber Security failures have the potential to cause physical consequences.
- Cyber Security issues can arise out of supply chain relationships.
- Human decisions can cause devastating consequences.
- Productivity can be affected.
Cyber Security Implication – Physical Consequences

- Electric Power Blackouts
  - September 2007 cyber attack in Brazil
  - 2003 Northeast blackout
  - 1999 Southern Brazil blackout
  - 1965 Northeast blackout
- 1979 Three Mile Island Nuclear Plant Accident
- 2000 Maroochy Shire cyber event
- 2007 Aurora Generator Test
- 2009 Stuxnet
- 2010 San Bruno natural gas pipeline explosion

© Copyright 2014 Netsecuris Inc. All rights reserved
Look what happens when ...
Supply Chain Cybersecurity

- Google’s headquarters in Sydney, Australia was breached due to building management vendor.

- Researchers discovered that they could breach the circuit breakers of a Sochi Olympic arena through their HVAC supplier.

- Watering hole attack on a major oil company’s network

- Major retailer breach due to relationship with HVAC vendor.
What makes an Industrial Control System fragile?

- COTS
  - Microsoft Windows
- Use of specialized communications protocols
  - Modbus
  - DNP3 (Distributed Network Protocol)
  - OPC (Open Platform Communications formerly known as OLE for Process Control)
- Manufacturers deviating from RFC
- Poor software design
Survey of Specialized Communications Protocols
Modbus

- Open protocol standard
- Moves raw bits or words without placing many restrictions on vendors.

- TCP/IP packet may look perfectly normal but the Modbus frame could crafted to carry malicious code.
DNP3

- An Open Standard
- Designed to be reliable but not secure.

- Header may look perfectly normal but the data payload could crafted to carry malicious code.
- No authentication mechanism in basic DNP3.
  - Secure DNP3
OPC

- Based on the OLE, COM, and DCOM technologies developed by Microsoft.
- Any vulnerabilities in these technologies is carried into this protocol.
- OPC is firewall unfriendly because OPC servers dynamically assign TCP ports.
- DCOM and RPC are extremely complicated protocols that can be translated into attack surfaces for malicious actors.
- OPC is complicated to setup so some vendors leave exposures in their products.
IT Cyber Security vs. OT Cyber Security
# IT Cyber Security vs. OT Cyber Security - Performance Requirements

<table>
<thead>
<tr>
<th>IT Systems</th>
<th>OT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Non-realtime transactions typically</td>
<td>• Real-time or near real-time transactions</td>
</tr>
<tr>
<td>• High throughput required</td>
<td>• Low to Medium to High throughput</td>
</tr>
<tr>
<td>• High delay or jitter may be acceptable</td>
<td>• High latency or jitter is not acceptable</td>
</tr>
</tbody>
</table>

Source: Derived from the NIST 800-82 Standard
## IT Cyber Security vs. OT Cyber Security - Availability Requirements

<table>
<thead>
<tr>
<th>IT Systems</th>
<th>OT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Rebooting acceptable but typically with change management process followed.</td>
<td>• Rebooting typically not acceptable unless planned.</td>
</tr>
</tbody>
</table>

Source: Derived from the NIST 800-82 Standard
### IT Cyber Security vs. OT Cyber Security - Risk Management Requirements

<table>
<thead>
<tr>
<th>IT Systems</th>
<th>OT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data confidentiality and integrity are most important.</td>
<td>• Life safety followed by process protection is most important.</td>
</tr>
<tr>
<td>• Fault tolerance is less important.</td>
<td>• Fault tolerance is essential.</td>
</tr>
<tr>
<td>• Major risk is delay of business operations</td>
<td>• Major risk is regulatory non-compliance, environmental impacts, and loss of life, equipment or production</td>
</tr>
</tbody>
</table>

Source: Derived from the NIST 800-82 Standard
## IT Cyber Security vs. OT Cyber Security - Change Management Requirements

<table>
<thead>
<tr>
<th>IT Systems</th>
<th>OT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Software changes are applied in a timely manner in the presence of good security policy and procedures</td>
<td>• Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of ICS is maintained</td>
</tr>
</tbody>
</table>

Source: Derived from the NIST 800-82 Standard
## IT Cyber Security vs. OT Cyber Security - Unintended Consequences Requirements

<table>
<thead>
<tr>
<th>IT Systems</th>
<th>OT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security solutions are designed for typical IT systems</td>
<td>• Security solutions must be tested offline on test ICS to ensure they don’t compromise the operation of production ICS</td>
</tr>
</tbody>
</table>

Source: Derived from the NIST 800-82 Standard
Regulatory Compliance Survey
Regulatory Compliance - Electric

- North American Electric Reliability Corporation (NERC)
  - Transmission and Generation
  - Critical Infrastructure Protection (CIP) v3
    - Requirements CIP-002 to CIP-009
    - CIP-003 Security Management Controls
    - CIP-005 Electronic Security Perimeter(s)
    - CIP-007 Systems Security Management
  - CIP v5 is approved and is in effect April 2016 for all High and Medium Assets and April 2017 for Low Assets.
Regulatory Compliance – Oil and Natural Gas

- US Department of Transportation in conjunction with US Department of Homeland Security’s Transportation Security Administration (TSA)
  - TSA wrote the “Pipeline Security Guidelines” and published in April 2011.
    - Section 7 Cyber Asset Security Measures
      - Baseline Cyber Security Measures
      - Enhanced Cyber Security Measures
  - TSA performs audits and reports results to US DOT.
  - US DOT enforces regulation and levies fines.
Federal Energy Regulatory Commission (FERC) has jurisdictional authority, granted by Congress, over non-public hydroelectric dams and facilities.

- Provides cyber security guidelines
- Cannot levy fines but can stop a company from selling electricity produced by the hydroelectric facility
Regulatory Compliance - Chemical

  - Risk-Based Performance Standards (RBPS)
    - RBPS8 covers cyber security requirements.
    - RBPS address to primary risks.
      - Sabotage
      - Diversion
  - Heavy fines
    - Divulging information about a CFATS tiered facility
    - Divulging information about Security Plans and Procedures
    - Not meeting RBPS requirements
Avoid Cyber Security Misconceptions

- Avoid the Air Gap Myth
- “We have a firewall!”
- “We’re just a small company, we’re not a target”
Shodan

- An industrial control system and network search engine
- http://www.shodanhq.com/
Netsecuris


- Contact Information
  - Leonard Jacobs, MBA, CISSP
  - President/CEO
  - sales@netsecuris.com
  - 952-641-1421

© Copyright 2014 Netsecuris Inc. All rights reserved
Questions and Answers

Thank you