Convegno Sezione Automazione ANIMP

SISTEMI DI AUTOMAZIONE: NUOVE SFIDE E OPPORTUNITA’

6 ottobre 2016
c/o Auditorium Maire Tecnimont (Milano)
Cybersecurity for the Oil & Gas industry: Risk & Opportunity
Roberto Minicucci – Senior IT Risk manager
GE Oil & Gas

- Why do we need this now?
- Cybersecurity standards landscape
- Elements of an effective Security Program
- Secure Supply Chain
- Examples & Discussion

Convegno Sezione Automazione ANIMP, Milano – 6 ottobre 2016
Why do we need this now?

Aramco says cyber attack was aimed at production

“For the first time, the agency recommended that manufacturers submit security plans to ward off cyber attacks when seeking FDA approval for their products.”

WSJ – June 2013

Customers, & competitors increasing focus on product cybersecurity

Device makers urged to bolster cybersecurity

“Saudi Arabian oil company, Aramco, said on Sunday that a cyber attack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia.”


Growing pattern of incidents

Regulators & Standards pressure

SEC asks AIG, Hartford Fin’, Eastman Chem., among others, to report cyber risks

GEHC Cranberry incident discovered; later reported to 28 government authorities

Customers, & competitors increasing focus on product cybersecurity

companies to include “material” cyber-risks in 10-K

incident discovered; later reported to 28 government authorities

FTC Internet of Things workshop focused on device/network security

DoD cyber-report requirement in DFARs for contractors with critical technical information

Italian data protection authorities orders GEHC to discontinue some automated collections

Customers, & competitors increasing focus on product cybersecurity

Aramco says cyber attack was aimed at production

Device makers urged to bolster cybersecurity

Growing pattern of incidents

Regulators & Standards pressure

SEC asks AIG, Hartford Fin’, Eastman Chem., among others, to report cyber risks

GEHC Cranberry incident discovered; later reported to 28 government authorities

Customers, & competitors increasing focus on product cybersecurity

companies to include “material” cyber-risks in 10-K

incident discovered; later reported to 28 government authorities

FTC Internet of Things workshop focused on device/network security

DoD cyber-report requirement in DFARs for contractors with critical technical information

Italian data protection authorities orders GEHC to discontinue some automated collections
ICS vulnerabilities trend*

*From Recorded Future Inc.
Cybersecurity Standards Landscape

STANDARDS MEAN:

- Consistent products and processes
- Industry needs are met
- Cost-effective solutions

ISO 27000 series
Focus on information security standards (IT)

NIST CSF
Overarching guidelines

NIST 800-53
Security controls

ISA/IEC 62443 suite
Cyber Security for Industrial Automation in the Energy sector

WIB M2784
Focus on vendors and providers

ISA99
Focus on industrial automation and control users

NERC-CIP
Electricity distribution/transportation

IADC DCS
Drilling Control Systems

DNV-OS-D202
Offshore Automation, Safety and Telecomm. systems

IADN (Japan)

FSTEC #31 (Russia)

IACS security (Qatar)

CPNI (UK)

CIGR (France)

NAMUR, VDI (Germany)

OLF (Norway)

ONC-C2M2
DHS & DOE

AGA 12
Crypto protection of SCADA comm.

API 1164 (US)
Pipeline SCADA security

NEMA (US)
National Electric manufacturers

ONG-C2M2
Pipeline SCADA security

Convegno Sezione Automazione ANIMP, Milano – 6 ottobre 2016
Elements of a Security Program

People

Process

Technology
SECURE DEVELOPMENT LIFECYCLE: Process

**Goals:**
- Incorporate Security Requirements into Product Development
- Establish Security practices and gate checks to ensure Commissioning and Maintenance/Upgrade still deliver a secure product
O&G | Supplier security key drivers

Supply Chain Risk mgt program ... a response to multiple inputs across GE O&G

<table>
<thead>
<tr>
<th>Comply with Standards</th>
<th>Meeting customer demands</th>
<th>Manage Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant industry standards</td>
<td>Example customers:</td>
<td>Risk management goals</td>
</tr>
<tr>
<td>• IEC 62443-2-4</td>
<td>• Shell</td>
<td>• Prove due diligence</td>
</tr>
<tr>
<td>• ISO27036</td>
<td>• Chevron</td>
<td>• Increased controllership</td>
</tr>
<tr>
<td>• DHS Proc. Language</td>
<td>• etc.</td>
<td>• Effective incident response plan</td>
</tr>
<tr>
<td>• ISO 21827 -SSE-CMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• API 1164</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ONG-C2M2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NIST SP800-161</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ internal standards/policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aligning to industry standards for compliance and competitiveness</td>
<td>Adhering to customer demands to sustain business</td>
<td>Output/benefits of risk mgmt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inject security into supply chain risk management processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increase supply chain maturity level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reduce risk exposure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Drive security awareness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable informed business decisions</td>
</tr>
</tbody>
</table>

Customer requirements:
• Current product inventory
• Completed risk assessment
• Reference architecture
• Back up and restore processes
• Achilles (or similar) certifications
• Etc.

Example customers:
• Shell
• Chevron
• etc.

Convegno Sezione Automazione ANIMP, Milano – 6 ottobre 2016
(In)security impact within the supply chain

The supply chain incorporates multiple tiers of suppliers

Tier 1 supplier → Tier 2 supplier → System integrator

Tier 1 supplier → Tier 2 supplier → Service provider

Potential break downs within supply chain
- Counterfeit software
- Viruses
- IP theft
- Poor security practices
- Backdoor threats

Potential impact to final product
- Counterfeit components
- Reduced reliability
- Uncontrolled variations
- Backdoor threats
- Poor performance

40% of the data-security breaches experienced by organizations arise from attacks on their suppliers (ISF research, 2013)
**Next steps / road to closure**

- Training sessions for Sourcing global teams
- Host supplier workshops to provide guidance
- Incorporate security into sourcing processes
- + pilot of cutting edge blockchain technology

**Initiative outcome**

- Identified 229+ critical components & 50+ suppliers
- Defined 39 basic requirements covering product & process
- Leveraged EXISTING Sourcing process
### Customer ICS security policy

<table>
<thead>
<tr>
<th>Sections 1 - 3:</th>
<th>General sections – Scope, Signature page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 4:</td>
<td>Management Leadership, Commitment and Accountability</td>
</tr>
<tr>
<td>Section 5:</td>
<td>Risk Assessment and Management</td>
</tr>
<tr>
<td>Section 6:</td>
<td>Project Management, Facilities Design and Construction</td>
</tr>
<tr>
<td>Section 7:</td>
<td>Information Availability and Protection</td>
</tr>
<tr>
<td>Section 8:</td>
<td>Personnel and Training</td>
</tr>
<tr>
<td>Section 9:</td>
<td>Operation and Maintenance</td>
</tr>
<tr>
<td>Section 10:</td>
<td>Management of Change</td>
</tr>
<tr>
<td>Section 11:</td>
<td>Third Party Services</td>
</tr>
<tr>
<td>Section 12:</td>
<td>Incident Investigation and Analysis</td>
</tr>
<tr>
<td>Section 13:</td>
<td>Community Awareness and Emergency Preparedness</td>
</tr>
<tr>
<td>Section 14:</td>
<td>Assessment and Improvement</td>
</tr>
<tr>
<td>Section 15:</td>
<td>Control System Networks</td>
</tr>
<tr>
<td>Section 16:</td>
<td>Operating Systems</td>
</tr>
</tbody>
</table>

- Complies with the State of <....> National ICS Security Standards

**Reference:**
ISA99/IEC 62443

Convegno Sezione Automazione ANIMP, Milano – 6 ottobre 2016
Vendor and Third Party ICS Security Related Initiatives

- External and Remote Connections - ICS External and Remote Connection Best Practices - purpose of this document is to define the best practices for connecting to the Industrial Control Systems Environment (ICSE) either remotely or externally.

- Project Management System Security Requirements and Specifications
  - provide ICS vendors guidance in designing, implementing, and delivering a secure ICS system that meets the minimum security requirements for ICS systems.
  - describes the minimum expected security and controls equipment, attributes, and related deliverables for new control and equipment management systems.
Some Key Vendor Requirements

- Participation of ICS Security team in design, implementation and acceptance process
- Inclusion of system security technical specifications in procurement language
- External and remote connectivity design shall have elements of 2FA, encryption, detection, logging, etc.
- Technical security specifications – minimum security hardening, network logical and physical segregation design
- Management and protection of information – handling and management of client information
- Secure practices during SAT, FAT, etc. – user ID management, removable media management, use of portable devices, etc.
Grazie per la cortese attenzione