INDUSTRY 4.0
INDUSTRIAL INTERNET OF THINGS

Webinar will be promptly at
2 P.M. ET/11 A.M. PT

HOSTED BY
NATIONAL CYBERSECURITY ALLIANCE

SIGNATURE SPONSOR
TREND MICRO™
education

AFFILIATE SPONSOR
GENERALI GLOBAL ASSISTANCE
IDENTITY PROTECTION SERVICES
✓ Convening partners who recognize strength in the security collective

✓ Educating individuals & organizations on cybersecurity best practices

✓ Amplifying collective efforts to increase cybersecurity awareness

www.staysafeonline.org  @staysafeonline
Thanks to our National Sponsors

Signature Sponsor

TREND MICRO™

education

Affiliate Sponsor

GENERALI GLOBAL ASSISTANCE
IDENTITY PROTECTION SERVICES

This was an excellent webinar with good information for small businesses and tech support companies like us who provide advice on support and security to our customers. The information covered can be passed along to our customers so they are #CyberAware!

Over 6,000 webinar attendees

Over 5,000 workshop attendees

Over 15,000 subscribers
Today’s Speakers

**Intro to Industry 4.0**
- Mitchel Chang, VP of Corporate Social Responsibility & Education, Trend Micro

**Challenges & Best Practices**

**CISA’s ICS Strategic Initiative**
- Rachel Russo, Cybersecurity Strategist, Cybersecurity & Infrastructure Security Agency
Perspective on Industry 4.0 and IIoT

Mitchel Chang
November 10, 2020
Introduction of mechanical, production facilities supported by water and steam power

1st Industrial Revolution

Mass production fuels the 2nd industrial revolution with the help of electrical power

2nd Industrial Revolution

Combining IT and electronics allows for further automation of the production process

3rd Industrial Revolution

The connected enterprise leads to the 4th industrial revolution. Connecting production facilities with the internet of things

“smart factory”

4th Industrial Revolution

How long to reach 50 million users?

- Telephone: 75 yrs
- Email: 38 yrs
- Facebook: 2 yrs
- Twitter: 9 days
- Instagram: 13 yrs
- Web: 4 yrs
Industry 4.0/IoT and the Future, Our World in 30 Years

- 4.0 Factory enhancements
- Cyber-physical ICT Infrastructure
- Smart cities
- Connected offices
- Good health
- Home comforts

But a cautionary conclusion:

*It is exciting as how the IoT may change the world, but the path to such progress will be littered with various cybersecurity challenges*
Industrial Cyber Security Business and Technical Challenges and Some Best Practices

Richard Ku
Sr. VP Commercial IoT Security Biz and Market Development
Adaptive Cybersecurity Solution for protecting ICS/OT Environment
Important definitions

• Cyber Incident
  – Defacto IT definition
    • Connected to the Internet, running Windows, and data is maliciously being manipulated or stolen - All about privacy
  – NIST definition
    • Electronic communication between systems that affects Confidentiality, Integrity, or Availability
    • No mention of “malicious” or Safety

• Purdue Reference model
  – Not the OSI Model

• Other
  – OT, Insider, Damage,…
Control systems basics

- Sensors
- Control Valves
- Programmable Logic Controllers (PLC)
- Motor Controls
- Serial-to-Ethernet Converter
- Network Monitoring
- Human Machine Interfaces (HMI) and Operator Displays
- Internet
- ERP
- MES
- Data Warehouse
- Support Systems

I/O
- Meters
- Sensors
- Field Devices

Remote
- PLC
- IED
- RTU Controller

Comms
- Protocols
- Ethernet
- Serial
- Wireless

Master
- SCADA
  - Server
  - HMI
  - EMS
  - DCS

Control Center

Field Devices

Internet

© 2020 Trend Micro Inc.
Purdue Reference Model

Days to weeks
Hours to Days
Gateway to Internet
Minutes to hours
Seconds to minutes
Milliseconds to seconds
Continuous to few milliseconds
Threats to ICS environment
### ICS Cyber Threats: Industrial Attack Timeline & Impact

#### Impact from ICS Cyber Attacks

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Cause</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>Iran Stuxnet Centrifuges Attack</td>
<td>4 zero-day vulnerability with USB devices and network infected Siemens equipments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The centrifuges were out of control during operations, causing physical damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>German Steel mill attack</td>
<td>Accessed office network by APT attack, then obtain privilege of control and production system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Steel mill unusually shutdowns, and causes massive physical damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Ukraine Power Grid Attack</td>
<td>Used spear-phishing emails with BlackEnergy3 malware, and got employee login access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Over 42000 emails and personal training reports leak</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>Middle East Trisis Plant Attack</td>
<td>Trisis malware attacks factory SIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Plant trip</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>Taiwan TSMC</td>
<td>Ransomware Attack</td>
<td>$255 Millions cost in down-time 10000 Affected Machines</td>
</tr>
<tr>
<td></td>
<td>• File Encryption and Data Exfiltration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td>US Visser Precision</td>
<td>Targeted Ransomware Attack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cause and Impact</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Timeline

- **2010**
  - Stuxnet worm infects Iranian nuclear plant. 20% of centrifuges damaged

- **2014**
  - Stuxnet infects Iranian nuclear plant. 20% of centrifuges damaged
  - Industries and Black Energy infect Ukrainian Power Grid. Hundreds of thousands of civilians lose electricity
  - WannaCry shuts down production in Honda plant, causing a delay in the output of over 1000 vehicles

- **2015-2016**
  - TRISIS infects Saudi Arabian Petrochemical Plant, marking the first known malware to target industrial SIS

- **2017**
  - WannaCry
  - North Korean Lazarus group suspected of cyber attack against Indian KKNPP Nuclear Plant

- **2018**
  - LockerGoga infects Norsk Hydro network, shutting down production & costing the company over $75M
  - Rheinmetall’s automotive division infected with malware, affecting manufacturing. Losses at $4.5M per week

- **2019**
  - DoppelPaymer Targeted Attack, File Encryption & Data Exfiltration

- **2020**
  - Havex supply chain malware hits dozens of ICS targets across EU and USA
  - North Korean Lazarus group suspected of cyber attack against Indian KKNPP Nuclear Plant
Control system cyber incidents are real

- >1,250 incidents to date*
- Impacts ranged from significant discharges to significant equipment damage to major electric outages to deaths
  - >1,500 deaths to date
  - >$70 Billion in direct impacts
- Very few ICS-specific cyber security technologies, training, and policies
- >2 million ICS devices directly connected to the Internet (and counting)
  - Many are gateways
- Resilience and recovery need to be addressed
Recent control system cyber incidents

- July 23, 2020  CISA Alert AA20-205A
  - Hacking of PLC connected to Internet
- Executive Order 13920
  - Hardware implants in large transformers
- Counterfeit process sensors
- Shadow sensor network in pharma equipment
- Drinking water hack
  - Disgruntled ex-employee changes pump configurations
- Multiple ransomware attacks
Industry Business and Technical Challenges
Industry Business Challenges

Lack of Domain Knowledge

- Insufficient Cybersecurity Knowledges, Expertise and Countermeasures in OT

IT/OT Convergence

- Cyber Security Role and Responsibility between IT and OT are not clearly define

Legacy Liability

- Due to legacy liability which is preventing cybersecurity countermeasure deployment in SCADA, HMI, PLC and networking

Pursuit Productivity & Economic

- The principle of manufacture productivity, revenue and profile will override every cybersecurity practice and SOP

ROI, Regulations and Leadership Support
EVERYBODY KNOWS ABOUT CYBER SECURITY. THE CHALLENGE IS KNOWING HOW TO APPLY IT.
Risks to ICS and OT Environment
Evolution of Industry Risk

- Increased Automation
- Increased Connectivity
- Increased Complexity
- Increased attacker sophistication

\[ \text{Increased RISK} \]
Reducing Industry Risk

- Increased Visibility
- Increased Prevention
- Increased Detection
- Increased Response
- Increased Collaboration

= RISK Reduction
IT/OT Cybersecurity Strategy: 3 Key pillars

**People**
- Staff Training and Awareness on security
- Professional Skills and Qualifications
- Competent Resources

**Process**
- Governance, Policy and Framework
- Management Systems
- Best Practices
- IT/OT Audit

**Technology**
- Technologies need to be tested, verified and validated
- Technology deployment requires competent people, support processes and an overall plan
Industry Standards Provide Best Practices to Protect Industrial Control Systems

IEC 62443 is recommended for industrial control systems
Recommend OT/ICS Security Solutions
# Purposed Built ICS/OT Security Solutions

<table>
<thead>
<tr>
<th>Visibility on Asset, Protocols, Control Commands, and Threats</th>
<th>Provide Real-time Protection and Enforcement to Prevent Security breaches with mini over head</th>
<th>Secure the OT/ICS network to keep operation running, reliable and Safe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Protection at the Network, Endpoint, Server, Cloud and Virtualization environments</td>
<td>Adaptive solution to fit into existing IT/OT infrastructure and operation</td>
<td>Centralized management for distributed, multi-tier deployments and Integrate with SIEM/SOAR platforms</td>
</tr>
</tbody>
</table>
Recommend ICS Security Solutions - Defense in Depth

- Additional solutions
  - End-Point Security
  - Cloud/Virtualization Security
  - High-End Network/IPS Security
  - SandBoxing Security Solution
Key Takeaways...

- Cyber attacks on ICS/OT environment are real and can/will have significant impact to your business
- Cybersecurity is the foundation to any digital transformation
- Trend Micro and its Partners are equipped to help you securely transform your business
Who Are We?
About Trend Micro, Inc and TXOne Networks

• 30-year young, “Billion $ Security Software Pure-Play”
• Headquartered in Japan & Global Operations in US
• Tokyo Exchange Nikkei Index, Symbol 4704
• Security: #1 in APAC, #2 in EMEA & LAR, #3 in NA
• Over 6000+ Employees, 38 Business Units Globally
• Customers include 48 of top 50 global corp’s

A Joint venture company of Trend Micro Inc. and Moxa Inc.  
30 years+ Cybersecurity Threat Intelligent

30 years+ OT Network Expertise

500,000+ commercial customers
155+ Million Endpoints
➢ 1+ Million Servers
Thank you!

Questions

Richard Ku richard_ku@trendmicro.com
CISA’S ROLE IN INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY:
STRATEGIC INITIATIVE OVERVIEW
WHAT ARE CONTROL SYSTEMS?

The Nation’s critical infrastructure (CI) depends on industrial control systems (ICS) to manage complex operational processes.

ICS are machines that automate and help control physical operations. *Often referred to as Operational Technology (OT) vice Information Technology (IT).*

Traditional ICS were built as standalone systems. *Cybersecurity was not a priority.*

Technology advancements are creating rapid integration and convergence of IT and OT systems as well as proliferation of IoT devices. *Includes connectivity to unsecure open networks like the internet.*

These factors broaden exposure to cybersecurity attacks. *Unique risk factors and security constraints come into play in an ICS environment.*

Managing ICS risk requires specific IT and OT technical expertise.
HOW DO WE ADDRESS ICS THREATS?

A Three-Pronged Approach

1. **CISA ICS Strategy: Defend Today.**
   We continue to improve ICS cybersecurity products and services we currently provide our partners.

2. **CISA ICS Strategy: Secure Tomorrow.**
   We must begin to build *shared ICS security capabilities* through joint investments with the ICS community.

3. **Strategic and Operational Partnerships:**
   **Control Systems Interagency Working Group (CSIWG):**
   CSIWG addresses intractable, systemic issues that require the expertise, ideas, resources and commitment of the entire ICS community.
HOW DO WE ADDRESS ICS THREATS?

Defending ICS Today.
HOW DO WE ADDRESS ICS THREATS?

Securing ICS for the Future.

SECURING INDUSTRIAL CONTROL SYSTEMS:

A UNIFIED INITIATIVE

FY 2019-2023
Government at all levels not only works with industry to help secure private sector ICS, but government agencies also own and operate CI (e.g., water and electric utilities, dams, ships, military equipment, mass transit systems, etc.).
DEFENDING TODAY, SECURING TOMORROW

We require a new model that enlists the entire community to anticipate, prioritize, and proactively manage ICS risk.

1. Ask more of the ICS Community, deliver more to them.
2. Develop and use technology to mature collective ICS cyber defense.
3. Build “deep data” capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS cyber kill chain.
4. Enable informed and proactive security investments by understanding and anticipating ICS risk.
Pillar 1

Ask more of the ICS community, deliver more to them.

Problem Statement:
We have arm’s-length relationships with many ICS stakeholders and close partnerships with only certain key stakeholders.

Outcome:
We will reinvigorate and deepen our existing partnerships, while also expanding the scope of engagements with the broader ICS community.
Problem Statement:
ICS-focused cybersecurity technologies are underdeveloped and rely too heavily on manual processes and insulated, proprietary information exchange platforms.

Outcome:
We will develop and promote easily accessible, deployable, and inexpensive ICS tools and capabilities to help asset owners secure ICS against adversaries.
Pillar 3

Build “deep data” capabilities to analyze and deliver information that disrupts the ICS cyber kill chain.

Problem Statement:
We do not access enough ICS data streams, nor do we make optimal use of the data we already have.

Outcome:
We will diversify data partnerships, further define ICS data needs, and support efforts to increase the ingestion of additional data differentiated by source, type, and consequence to increase visibility into ICS threats and vulnerabilities.
Pillar 4

Enable informed, proactive security investments by understanding and anticipating ICS risk.

Problem Statement:
We do not do enough to understand and anticipate ICS cyber risk, so we are too often reactive.

Outcome:
We will improve our visibility into the risk landscape and use that knowledge to inform investments into proactive initiatives that move the ICS community ahead of the threat curve.
CISA helps customers defend ICS today through these capabilities...

**Assessments**
Operational resilience valuations

**Cyber Hunt**
Aid ICS partners with adversary presence search in absence of known threat

**Exercises**
Testing and readiness for ICS incidents

**Information Exchange**
Sharing of threat and best practice guidance with partners

**Partnerships and Engagement**
Collaborate and coordinate with ICS partners

**Products and Tools**
Access to hands-on tool for the ICS community

**Response**
Deploy expertise advanced to aid ICS and victims

**Strategic Risk Analysis**
Provide ICS risk information pertaining to National Critical Functions (NCFs)

**Technical Analysis**
ICS malware analysis support

**Training**
Technical and non-technical ICS instruction for all skill levels

**Vulnerability Coordination**
Coordinated, pull disclosure of ICS vulnerabilities mitigation recommendations
For more information, visit: www.cisa.gov/ics

Questions?
CISAICSStrategicInitiative
@cisa.dhs.gov

Click here for a copy of the CISA ICS Strategy
SECURING YOUR DATA IN THE CLOUD

December 8, 2020
2-3 P.M. EDT/11 A.M. PDT

GUEST SPEAKER:
William Malik
Vice President, infrastructure Strategies
Trend Micro

Register Here: https://staysafeonline.org/event/cloudsecurity/