NECA • BICSI
SUMMIT 2023

The Intersection of Cybersecurity in OT/IoT/IT

And Why It Matters

NECA • BICSI
SUMMIT 2023

Agenda

- Who is CompTIA?
- Networking Overview
- What is OT/IoT/IT?
- OT & Cybersecurity
- OT Threats Examples
- OT Product Origination
- Who is Responsible?
- Practical next steps

CompTIA

The IT Industry
Trade Association

Jeff Parker
Global Business Development
jparker@comptia.org
317 385 8599

Ron Culler
VP, Cyber Learning Officer

CompTIA

The IT Industry
Trade Association

Who We Are

CompTIA is a global not-for-profit IT Trade Association and the voice of the industry.

Our Mission

Advance the IT Industry

Who We Serve

Tech Professionals, Tech Adjacent Workers, Tech Businesses, Tech Educators, and anyone interested in Tech Careers or a vibrant Tech industry

- Research
- Philanthropy
- Education & Certification

NECA • BICSI
SUMMIT 2023

Networking Overview

Networking - 101

- Simply put it’s how devices connect to one another, it can be over copper cabling, or fiber optics for common ethernet, wireless technologies like Wi-Fi, cellular (3G to 5G), Zwave, Zigbee, or LoRaWAN

- Your homes, your businesses, and your customers all have networks, and they are almost always connected to each other because of the Internet (the biggest network of them all)

- Common terminologies:
  - VLAN – a virtual network. Multiple VLANs can exist on a single physical device or across multiple devices.
  - PoE – Power over Ethernet – The ability to supply power to devices over copper networks without having to run AC power to them.

Networking – The Digital Handshake

- Secure connection between a computer or a network and a device.
- Required for a device and a computer or network to send secure protocols or information back and forth.
- Ensures both “participants” know the rules on working together.
- Various types of handshakes: some are very simple others are complex (i.e. three-way handshake).
- Types: TLS & SSL

Networking – Common Vulnerabilities

- Improperly Installed Hardware or Software
- Operating systems or firmware that have not been updated
- Misused hardware or software
- Poor or a complete lack of physical security
- Insecure passwords
- Design flaws in a device's operating system or in the network

This Photo by Unknown Author is licensed under CC BY-SA

What is OT, IoT & IT?

What is IT, IoT, and OT?

The National Institute of Standards and Technology (and IEEE) defines IT, IOT, and OT as follows:

IT – Information Technology

The use of hardware, software, services, and supporting infrastructure to manage and deliver information using voice, data, and video.

IoT – Internet of Things

Connecting any device with an on/off switch to the Internet and/or other devices (i.e. cellphones, watches, thermostats, jet engines, oil rig drills).

OT – Operational Technology

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

The Where and What of OT

Where can I encounter OT?

- Manufacturing
- Energy Distribution
- Transportation
- Building Management Systems
- Process Plants
- Warehouse Management Systems
- Physical Security Systems

The Where and What of OT

What are typical OT Components?

- Control Systems and Devices
- Human Machine Interfaces (HMIs) and Engineering Workstations
- Sensors, Motors/Drives, and Actuators
- Batch Managers, Data Historians

What's in a name?

OT can be referred to as SCADA, Distributed Control Systems, Industrial Control Systems, Manufacturing Network, and Process Control

What are the Differences Between OT and IT?

	Information Technology (IT)	Operational Technology (OT)
Equipment Lifecycle	Three (3) to Five (5) Years	Five (5) to Thirty (30) Plus
Reboot Ability	Easy to reboot with backups for critical systems	Complex, requiring significant planning to reboot
Updates/Maintenance	Regular updates with a defined process	Complicated, requires special maintenance times, often with a vendor
Hardware	Standard, Plug & Play	Proprietary, can require custom integration
Location	Corporate/Business Offices	Industrial locations (mixed environments)
Primary Focus	Security, Reliability, Integrity	Safety, Availability

Specific OT Device Examples

- PoE Lighting
- Fire Control Systems
- Wind Turbines
- Solar Arrays
- Any Building Automation and Control
  - Air Systems
  - Control Panels
  - Thermostats
  - Sensors

NECA • BICSI
SUMMIT 2023

OT and Cybersecurity

Why is OT Cybersecurity Important?

Compromise of these systems can lead to:

- Death, Injury, or Sickness
- Environmental releases
- Equipment damage
- Production loss / service interruption
- Off-spec / dangerous product
- Loss of trade secrets

Specific OT Cyber Risks

1. Malware and Ransomware Attack
2. Denial of Service Attacks
3. Insider Threats
4. Supply Chain Attacks
5. Lack of Security Updates and Patches
6. Human Error

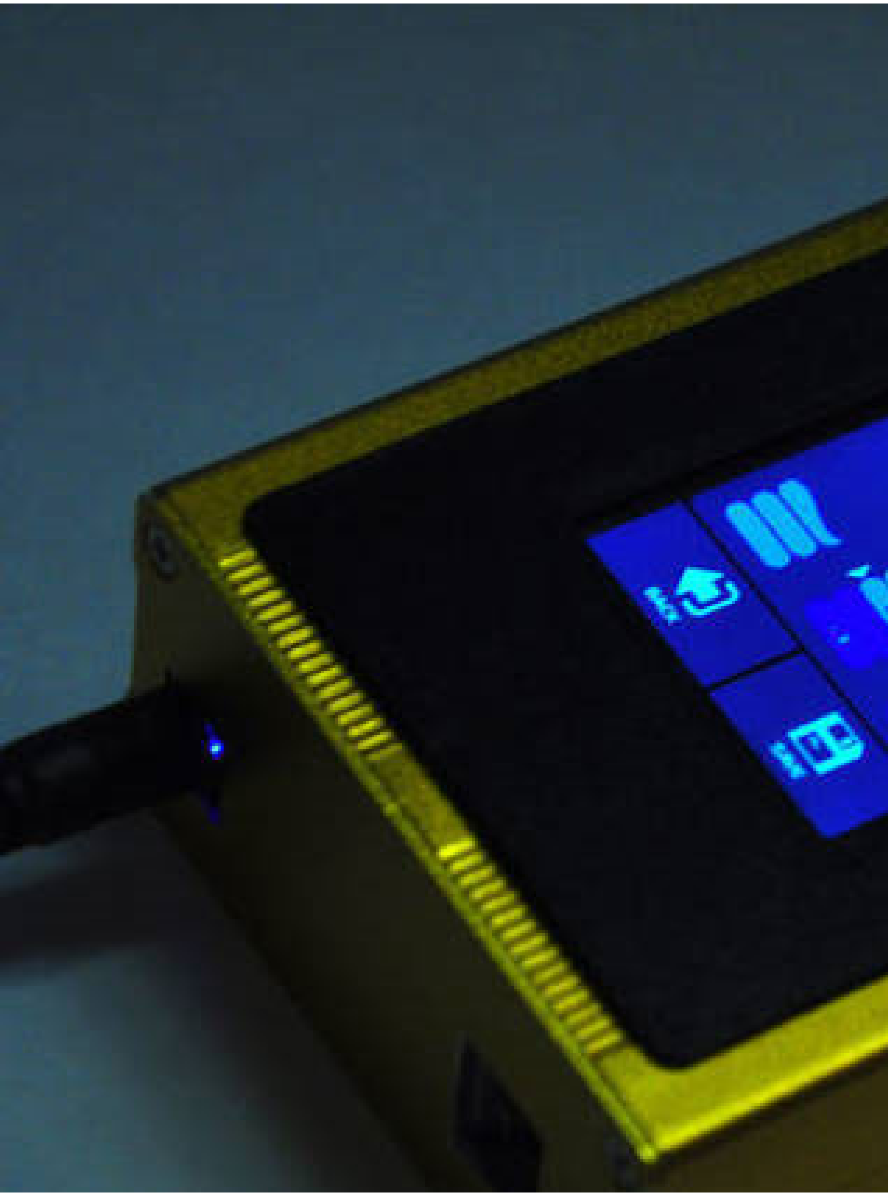
NECA • BICSI
SUMMIT 2023

OT Threat Examples

Attack Vulnerabilities – OT Network Switching

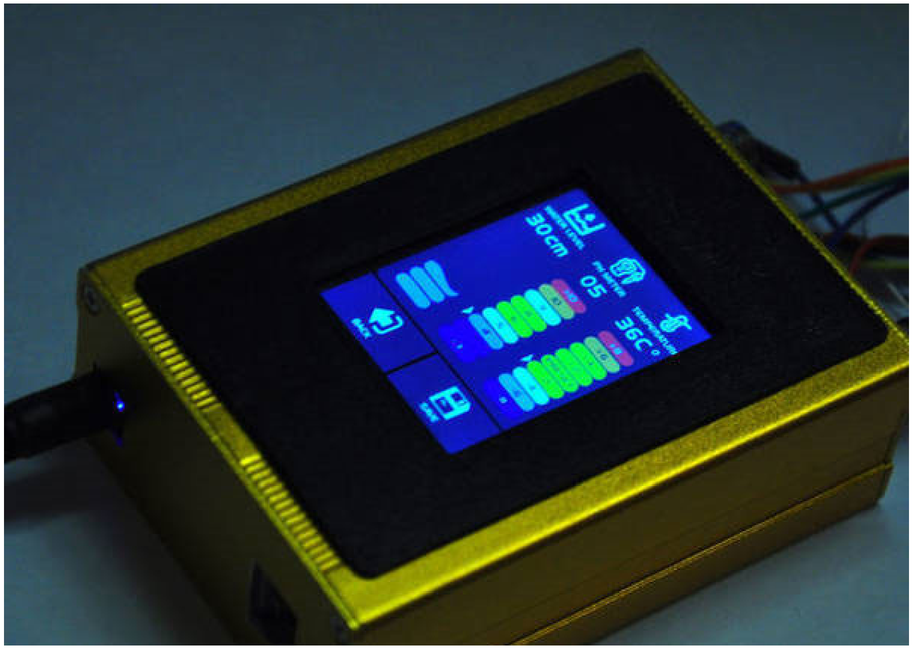
- Ethernet OT networks are ubiquitous today
- Older OT networks are like serial-based networks
- Ethernet switch is the linchpin of an OT network
- Two types: Unmanaged and Managed Switches

- Unmanaged Switches are a risk:
  - Open ports = security risk
  - Cannot manage data traffic
- Unmanaged Switches are a risk
  - High Security
  - Manages Traffic
  - Managed Services Opportunity



Does Anyone Know What This Is?

Threat Example – Fish Tank Thermometer



This Photo by Unknown Author is licensed under CC BY-NC-ND

- According to a 2018 Business Insider Report:
  - Attackers entered a casino's network via network connected device
  - Once in the network, attackers accessed a high roller database
  - The data was pulled through the device
  - This type of attack is called a Pivot or Pivoting

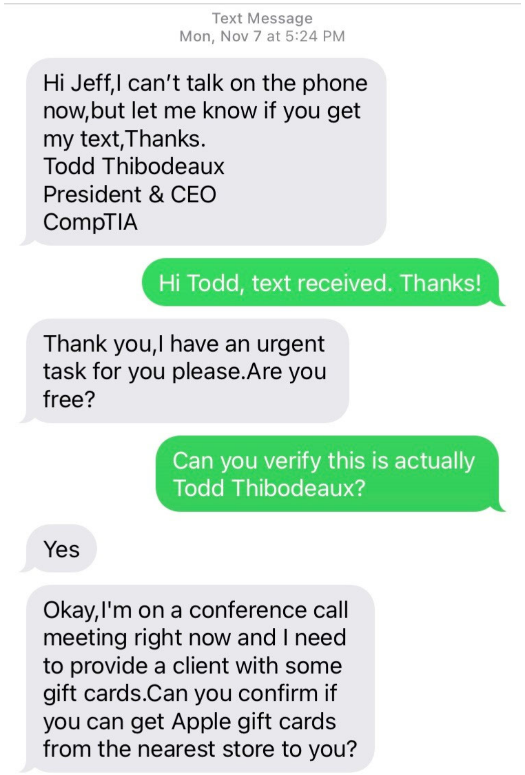
Threat Example – Wind Turbine

- $20 Handheld Computer – Raspberry Pi
- Intercepted Control Messages – Remote
- Turbine Stopped Turning
- Potentially Damaged or Destroyed Components
- Man in the Middle Attack

Threat Example – HVAC

- Nov 2013 – Well Known Retail Chain
- New Install by a HVAC Sub-Contractor & Service Provider
- Stolen employee credentials from the Sub-Contractor Allowed Access
- Malware Planted
- Over 40 million credit & debit card numbers stolen

Threat Example - Phishing



Text Message
Mon, Nov 7 at 5:24 PM

Hi Jeff,I can't talk on the phone now,but let me know if you get my text,Thanks.
Todd Thibodeaux
President & CEO
CompTIA

Hi Todd, text received. Thanks!

Thank you,I have an urgent task for you please.Are you free?

Can you verify this is actually Todd Thibodeaux?

Yes

Okay,I'm on a conference call meeting right now and I need to provide a client with some gift cards.Can you confirm if you can get Apple gift cards from the nearest store to you?

Threat Example - Phishing

- 80-90% of cyber attacks
- Attackers use email, phone or text to entice individuals to provide personal or sensitive information
- Attackers pose as legitimate representatives
- Point of phishing is to gain trust and create urgency

Threat Example – NUIT

NUIT = Near Ultrasound Inaudible Trojan*

- Silent attack through and against voice assistant power devices
- Uses near ultrasound waves to send malicious commands
- Can be inserted into online Videos, Websites, or played during a video call
- Malicious commands take less than 1 second to send
- Command examples:
  - “Unlock the front door”
  - “Disable the alarm”
  - “Go to this malicious site”

* https://www.bleepingcomputer.com/news/security/inaudible-ultrasound-attack-can-stealthily-control-your-phone-smart-speaker/

NECA • BICSI
SUMMIT 2023

OT Product Origination

Be Aware – Origination of Products & Services

- OT devices or parts can be manufactured in non-US countries, then assembled in the US
- Marked as “Made in USA”
- Examples: Fire Control, Video Cameras, Network Switches, etc
- These devices can and some do have Open Network Ports
    - Security Risk
    - “Listening” in
    - Can send information back to foreign governments
- Services, Applications, and Sites (ie Tik-Tok, social media)

NECA • BICSI
SUMMIT 2023

Who is Responsible for Cyber Attacks?

Who is Responsible?
(Or Who Can Be Held Accountable?)

1. The Hacker

2. Generally speaking
   - Data owners will be held responsible for data security (DPP-GDPR)
   - US/State/Local Governments also bear responsibility

3. Third parties can be held accountable if clear evidence of negligence is shown
   - For example, installing a device with an unmanaged switch or with an open port

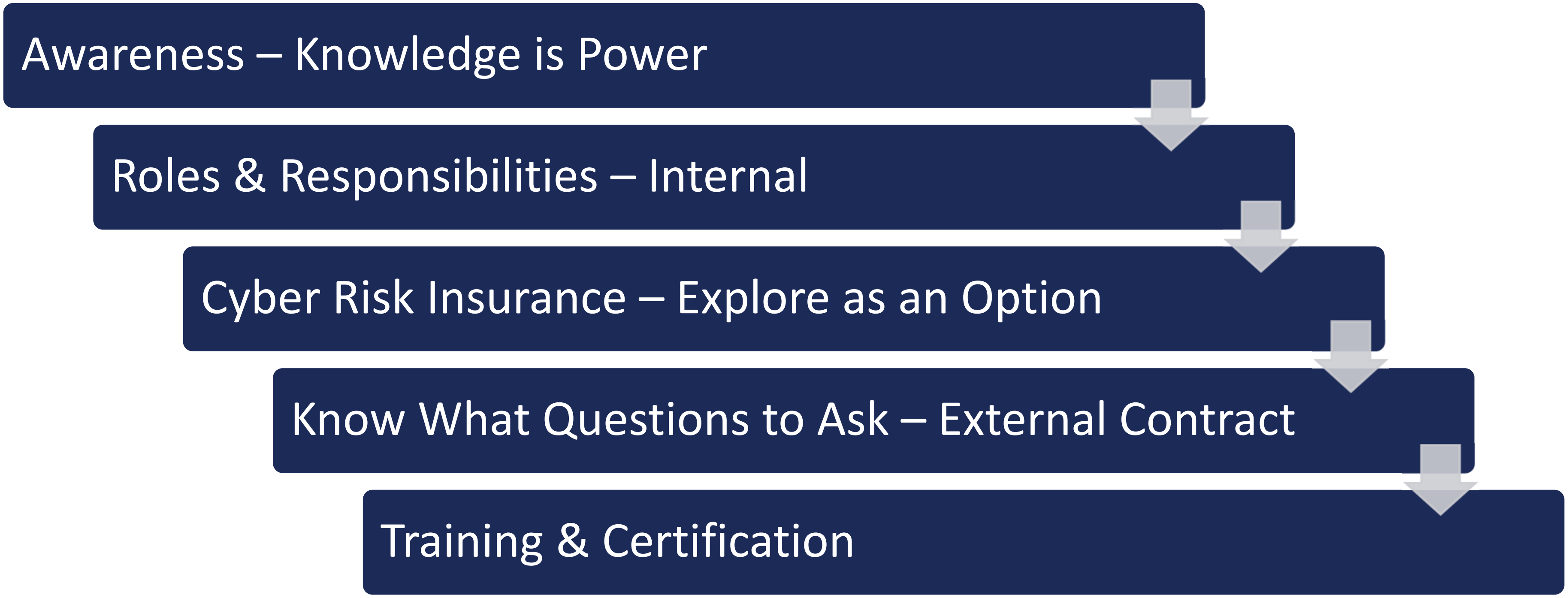
4. Additional Reading:

https://www.csoonline.com/article/3691769/new-vulnerabilities-found-in-industrial-control-systems-of-major-vendors.html

NECA • BICSI
SUMMIT 2023

What Can We Do Now?

Five Things To Do Now



Awareness – Knowledge is Power

Roles & Responsibilities – Internal

Cyber Risk Insurance – Explore as an Option

Know What Questions to Ask – External Contract

Training & Certification

Q & A