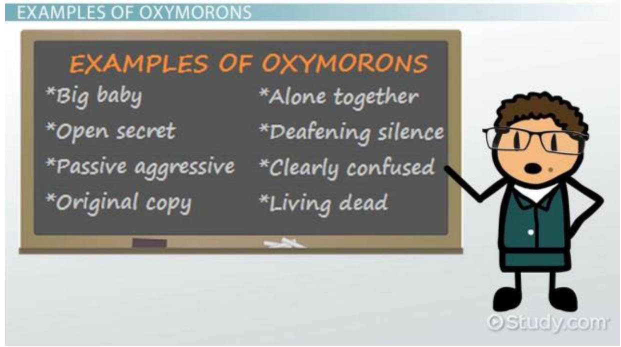
Critical Infrastructure Protection: Threats, Vulnerabilities, and Cybersecurity

Presenter Information

- Gordon W Skelton, PhD, CISSP, CISA, CEH, CRISC, Security+
- President, Security and Analytics, LLC, Ridgeland, MS
- Senior Member IEEE
- Member ISC(2), ASIS, ISA, ISIS, NCMS (The Society of Industrial Security Professionals)
- Research in cybersecurity as applied to Enterprise Networks and Industrial Control Systems

An Oxymoron – Cyber(?)Security

- No such thing as cyber security
- Just doing our best to stop known threats and to reduce attack vector
- Zero-day attacks are out there and coming to a computer near you
- Unprepared means that your are vulnerable



EXAMPLES OF OXYMORONS

EXAMPLES OF OXYMORONS

*Big baby	*Alone together
*Open secret	*Deafening silence
*Passive aggressive	*Clearly confused
*Original copy	*Living dead

©Study.com

WARNING – Cybersecurity is a BIG Topic

I can talk it about for days and will only scratch the surface

Hold on and great ready for a ride!!!

What is Critical Infrastructure?

Chemical Sector	Commercial Facilities Sector	Communications Sector
Critical Manufacturing Sector	Dams Sector	Defense Industrial Base Sector
Emergency Services Sector	Energy Sector	Financial Services Sector
Food and Agricultural Sector	Government Facilities Sector	Healthcare & Public Health Sector
Information Technology Sector	Nuclear Reactors, Material & Waste	Transportation Sector
	Water & Wastewater Systems	

https://www.dhs.gov/cisa/critical-infrastructure-sectors

What is the current state of Cyber Security?

- Attackers come from both the inside and outside of all organizations
- Most common means of attack – **email – phishing**
- Insider Threats account for nearly 75% of all security breach incidents
    - Those breaches are either intentional or unintentional
    - Includes clicking on malicious emails, visiting wrong websites
    - Inserting USB drives
    - Adding their smartphone to the corporate network
    - Just being stupid or not paying attention, not following policies

75%

Important Definitions

- SCADA – Supervisory Control and Data Acquisition
- ICS – Industrial Control System
- PLC – Programmable Logic Controller
- IoT – Internet of Things
- IIoT – Industrial Internet of Things

Traditional IT Sectors

- A number of the critical infrastructure sectors are traditional IT
- The integration of IT and OT, along with IoT and IIoT, are creating new opportunities for attackers
- The inclusion of mobile devices and IoT are creating new security issues for organizations
- Users want convenience and ease of use, so do attackers!!!

Why are we concerned?

- Changes to the industrial integration of enterprise networks (IT) and operating networks (OT)
- The “Shopfloor” is no longer isolated or “air gapped”
- Employing ethernet protocols in place of commonly used protocols
- Desire to incorporate data from manufacturing, production in decision-making,

  the use of “Big Data” for production analysis
- We are developing more sophisticated applications, often with AI, so are attackers

How Do They Get In?

- Misconfigured firewalls and other security devices
- Default usernames and passwords on devices
- Malware
- Use of authorized software / devices
- Employees not properly trained on cybersecurity
- Phishing attacks – employees click without thinking

Stop, Think Before Clicking!

How Do They Get In?

- Lack of physical security
- Failure to apply security patches
- Old operating systems – still have people using XP, Windows 7
- Social Engineering – "Hi, I'm your computer guy. What is your password?"
- Following you in – piggybacking
- Unlocked doors – just show up and walk in – "Glad to see you"

Common Components

Programmable Logic Controller (PLC)	Remote Terminal Unit (RTU)
Human Machine Interface (HMI)	Control Server
Master Terminal Unit (MTU)	Intelligent Electronic Device (IED)
Data Historian	Engineering Workstation
Sensors	Actuators
Switches / Hubs	Firewalls

Communications Protocols

- PROFINET – Process Field Net
- EtherNet/IP
- Common Industrial protocol (CIP)
- Ethernet
- Modbus and Modbus TCP/IP
- DNP3
- Common IT Protocols found in ICS – HTTP, FTP, Telnet, ARP, ICMP,

Profibus

PowerLink Ethernet

EtherCAT

Weaknesses of Communication Protocols

- No inherent security measures
- If using Ethernet, then traditional security issues exist – packet capture, injection of malicious attacks
- Identity theft
- Modification of messages
- Re-injection of traffic
- Eavesdropping, use of taps

Issues Surrounding Cybersecurity and ICS Protection

- Routine patching of operating systems is uncommon
- Limited memory and processing capabilities on PLCs
- Many of the communication protocols are hackable, containing inherent vulnerabilities
- Changes to programs – Ladder Programs – can be loaded directly to a PLC
- Lack of adequate training for technicians and engineering staff on cybersecurity
- Integration of IT and OT cybersecurity lacks proper understanding and focus

Examples of Non-traditional Systems That Can Benefit from a Cybersecurity Framework

- Advanced Metering Infrastructure
- Building Automation
- CCTV Surveillance Systems
- Digital Signage
- Electronic Security Systems
- Energy Management Systems
- Fire Alarm Systems
- Intrusion Detection Systems
- Public Safety / Land Mobile Radios
- There are many different systems that can benefit from NIST 800-52 rev. 2

Types of Threats

Replay attack on SCADA – data is captured from normal operations and replayed while attack is occurring thus preventing monitoring staff from being alerted by alarms

Malware on enterprise network is able to access OT network and ICS through integrated networks (IT / OT) – Stuxnet Virus

Physical Security Concerns

- Much of our critical infrastructure is stretched over unprotected miles
- Monitoring is at best weak
- Attackers can conduct surveillance without detection
- Destruction of one site might lead to a critical failure of infrastructure affecting 100,000s or Millions of individuals
- Can lead to events affecting human safety, environment, and the economy (EHS)

Botnet of IoT

- Mirai botnet attack – created by a group of teens used various unsecured Internet cameras to create a botnet
- https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Examining Your Own Systems

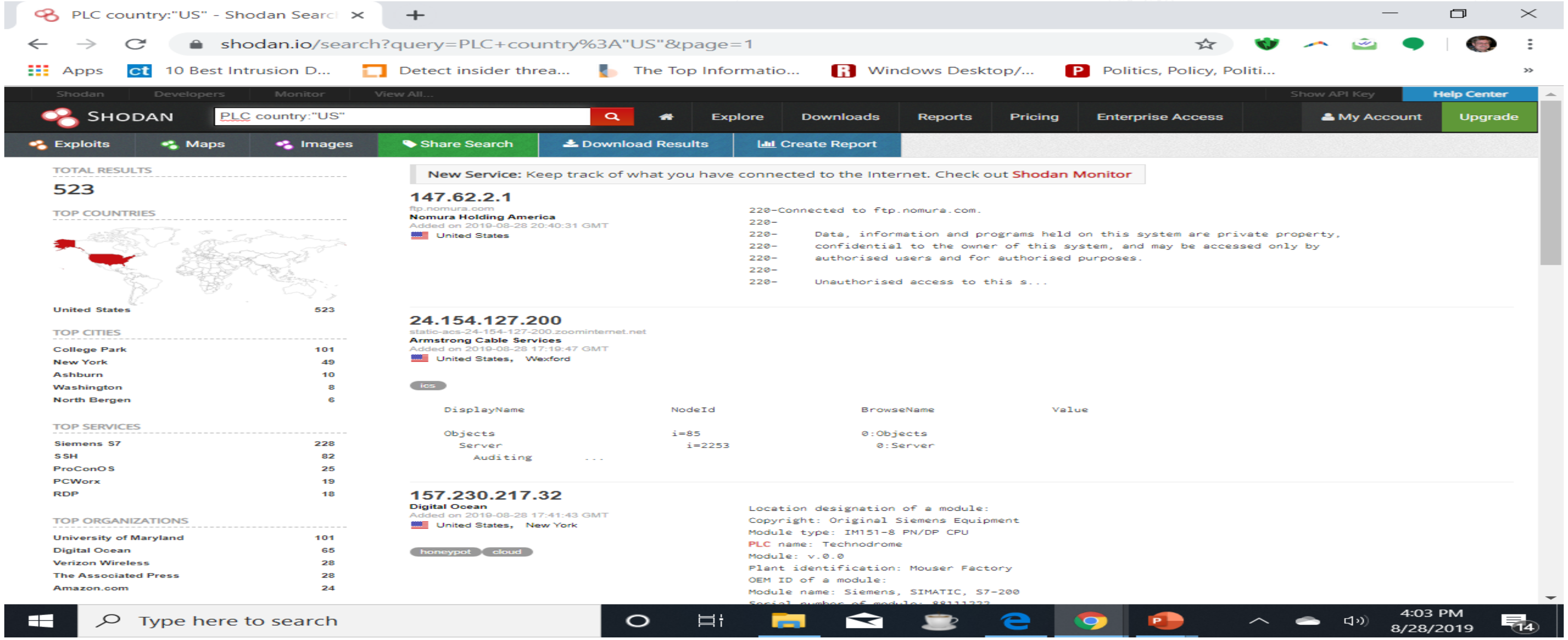
- Using Shodan https://www.shodan.io

or

- Censys.io https://www.censys.io

you can see if any of your industrial devices are available to individuals browsing the Internet

SHODAN Example



shodan.io/search?query=PLC+country%3A"US"&page=1

PLC country:"US"

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

523

TOP COUNTRIES

United States	523

TOP CITIES

College Park	101
New York	49
Ashburn	10
Washington	8
North Bergen	6

TOP SERVICES

Siemens S7	228
SSH	82
ProConOS	25
PCWorx	19
RDP	18

TOP ORGANIZATIONS

University of Maryland	101
Digital Ocean	65
Verizon Wireless	28
The Associated Press	28
Amazon.com	24

147.62.2.1
ftp.nomura.com
Nomura Holding America
Added on 2019-08-28 20:40:31 GMT
United States

```
220-Connected to ftp.nomura.com.
220-
220-      Data, information and programs held on this system are private property,
220-      confidential to the owner of this system, and may be accessed only by
220-      authorised users and for authorised purposes.
220-
220-      Unauthorised access to this s...
```

24.154.127.200
static-acs-24-154-127-200.zoominternet.net
Armstrong Cable Services
Added on 2019-08-28 17:19:47 GMT
United States, Wexford

ics

```
    DisplayName                NodeId              BrowseName             Value

    Objects                    i=85                0:Objects
      Server                     i=2253              0:Server
        Auditing         ...
```

157.230.217.32
Digital Ocean
Added on 2019-08-28 17:41:43 GMT
United States, New York

honeypot cloud

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

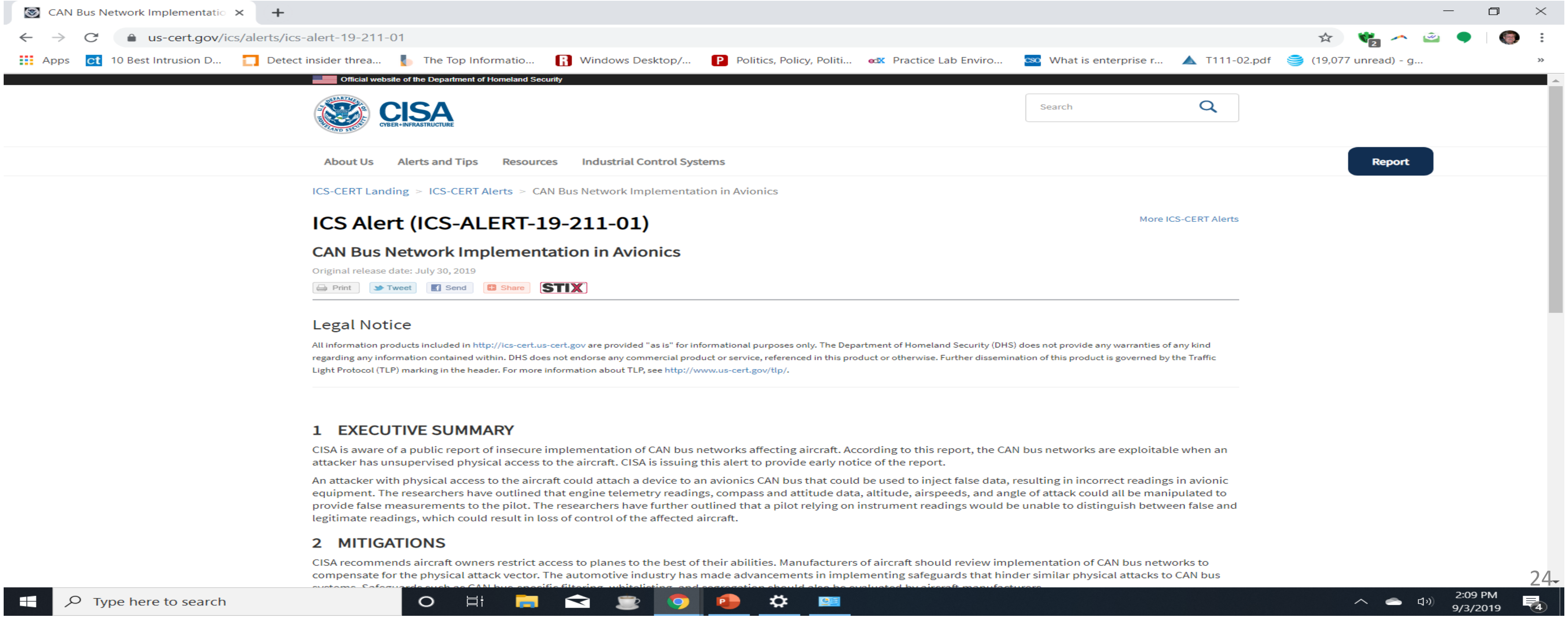
Threat Awareness

- Must be aware of the different types of attacks and how they may affect you
- Locate a good website that lists current threats and attacks and check it daily
- Search for your operating system (OS), equipment model, application software
- Make certain that you stay aware of types of attacks that affect your industry

Key Vulnerability Reference Sites

- Industrial Control Systems: Alerts, Advisories, Reports - https://www.us-cert.gov/ics Site used to report discovered vulnerabilities and aids in their mitigation
- Industrial Control Systems Cyber Emergency Response Team – https://isc-cert.us-cert.gov
- Industrial Control Systems Information Sharing and Analysis – http://isc-isac.org
- SCADAhacker.com – https://scadahacker.com/library

Example from CERT-ICS



ICS-CERT Landing > ICS-CERT Alerts > CAN Bus Network Implementation in Avionics

More ICS-CERT Alerts

ICS Alert (ICS-ALERT-19-211-01)

CAN Bus Network Implementation in Avionics

Original release date: July 30, 2019

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

1 EXECUTIVE SUMMARY

CISA is aware of a public report of insecure implementation of CAN bus networks affecting aircraft. According to this report, the CAN bus networks are exploitable when an attacker has unsupervised physical access to the aircraft. CISA is issuing this alert to provide early notice of the report.

An attacker with physical access to the aircraft could attach a device to an avionics CAN bus that could be used to inject false data, resulting in incorrect readings in avionic equipment. The researchers have outlined that engine telemetry readings, compass and attitude data, altitude, airspeeds, and angle of attack could all be manipulated to provide false measurements to the pilot. The researchers have further outlined that a pilot relying on instrument readings would be unable to distinguish between false and legitimate readings, which could result in loss of control of the affected aircraft.

2 MITIGATIONS

CISA recommends aircraft owners restrict access to planes to the best of their abilities. Manufacturers of aircraft should review implementation of CAN bus networks to compensate for the physical attack vector. The automotive industry has made advancements in implementing safeguards that hinder similar physical attacks to CAN bus systems. Safeguards such as CAN bus specific filtering, whitelisting, and segregation should also be evaluated by aircraft manufacturers.

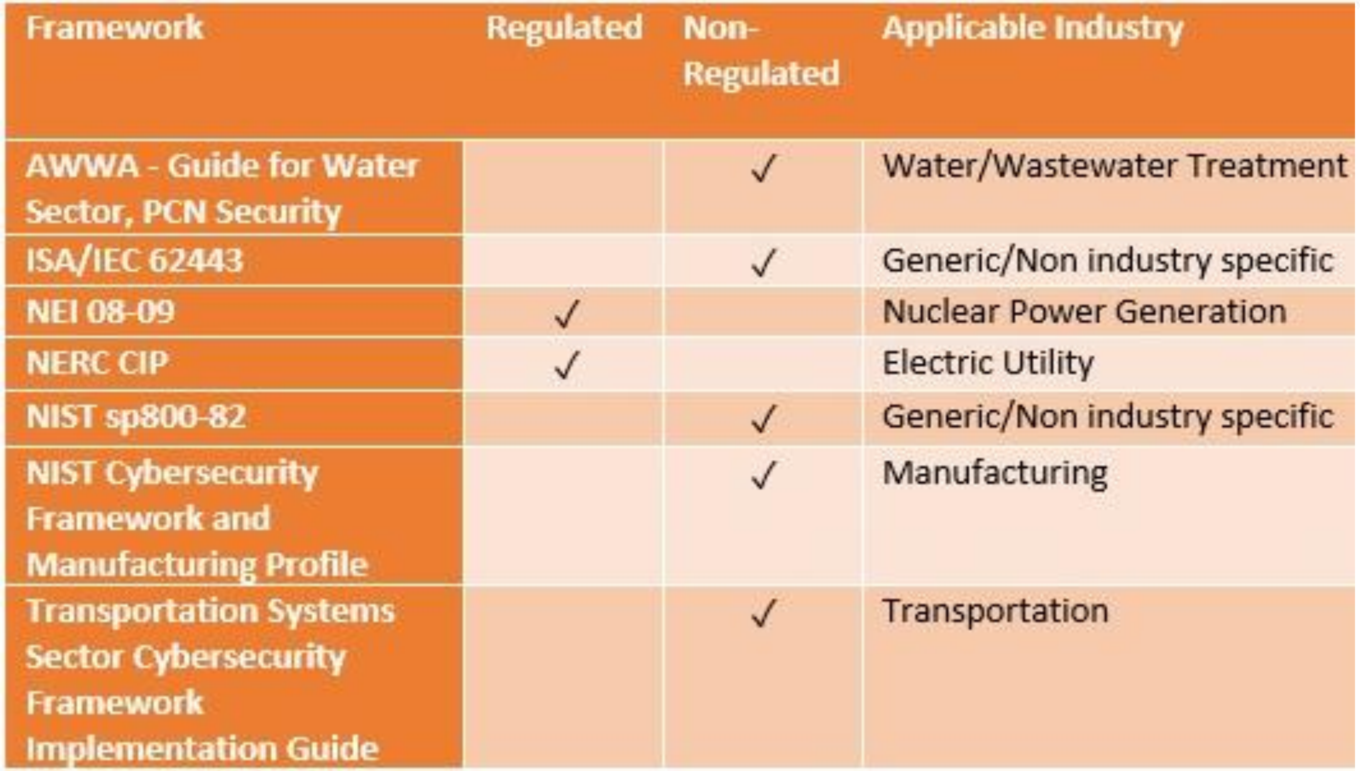
Helpful Reference Site for ICS Security Concerns

- https://www.trendmicro.com/us/iot-security/

Cybersecurity – Policies and Procedures

- Locate a good standard and modify to meet your needs
- 1st get support of executive leadership
- Develop an overall cybersecurity policy for the organization
- Develop specific policies and procedures for such things as Internet usage, email usage, data usage and security
- Make certain everyone has received a copy, actually read, understands, and follows the policies

Standards and Frameworks

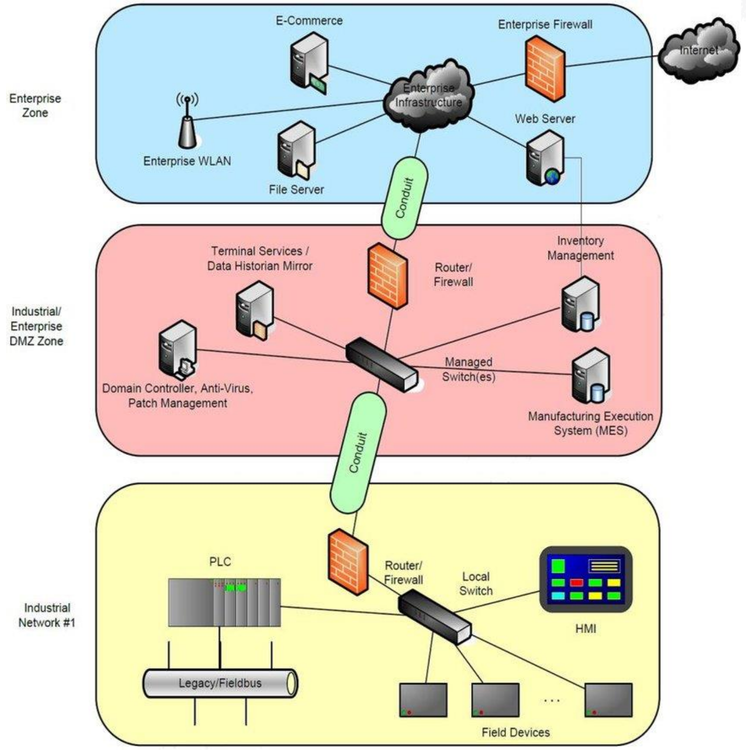


Framework	Regulated	Non-Regulated	Applicable Industry
AWWA - Guide for Water Sector, PCN Security		✓	Water/Wastewater Treatment
ISA/IEC 62443		✓	Generic/Non industry specific
NEI 08-09	✓		Nuclear Power Generation
NERC CIP	✓		Electric Utility
NIST sp800-82		✓	Generic/Non industry specific
NIST Cybersecurity Framework and Manufacturing Profile		✓	Manufacturing
Transportation Systems Sector Cybersecurity Framework Implementation Guide		✓	Transportation

ISA 62443 – Zones and Conduits

- Supports Segmentation of Networks
  - Zone – grouping of logical or physical assets with common security requirements based on criticality and consequence
  - Conduit – specific type of zone that groups communications between zones

ISA 62443 – Example



Zone model of Industrial Control Systems (source: ISA/IEC 62443)

DoD Framework Example

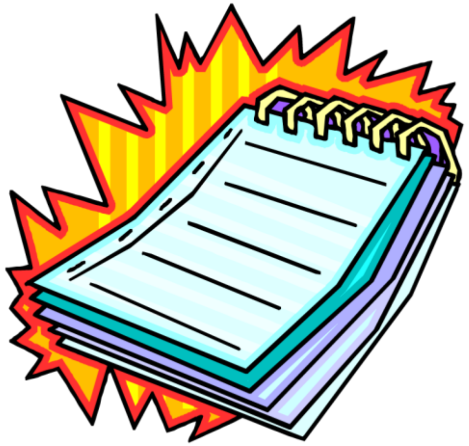
ia-policychart-30-Oct-19-DoDIN.pdf

What To Do?

- Constant vigilance
- Ongoing training of all personnel on data security
- Continuous update of all controls
- Monitor your networks, local hosts, and network servers
- Investigate the use of the cloud for data storage

What To Do?

- Change the default username, password on all hardware (if possible)
- Implement a password policy – longer, more complex, passphrases
- Investigate multi-factor authentication
- Encrypt your data both at rest and in transit
- Encrypt your email



What To Do?

- Examine and harden physical security
- Segmentation of Network
- Least Privilege authorization
- Develop and test business continuity plan
- Defense in Depth – multiple layers of protection
- Get commitment from the top level – CEO, Board of Directors

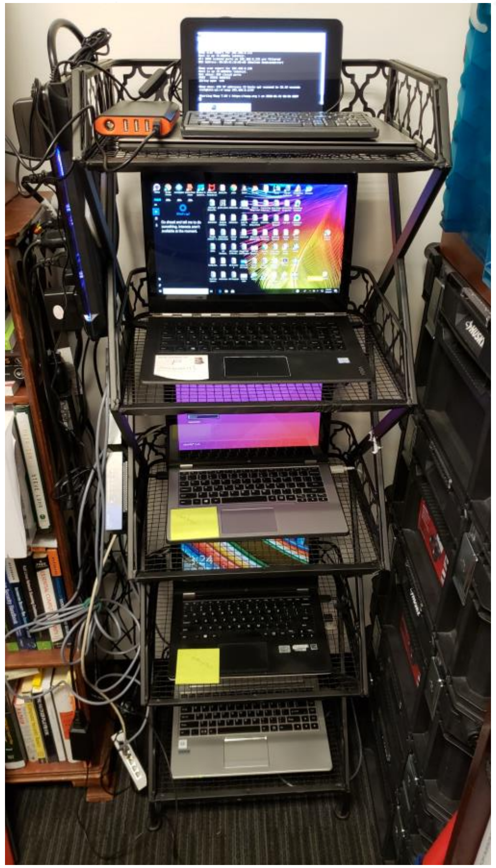
What To Do?

- Lock computers when away from workspace
- Prevent shoulder surfing
- Protect PII (Personal Identifiable Information)
- Examine printer / copier security
- Understand risk appetite
- Understand current state of risk and protection

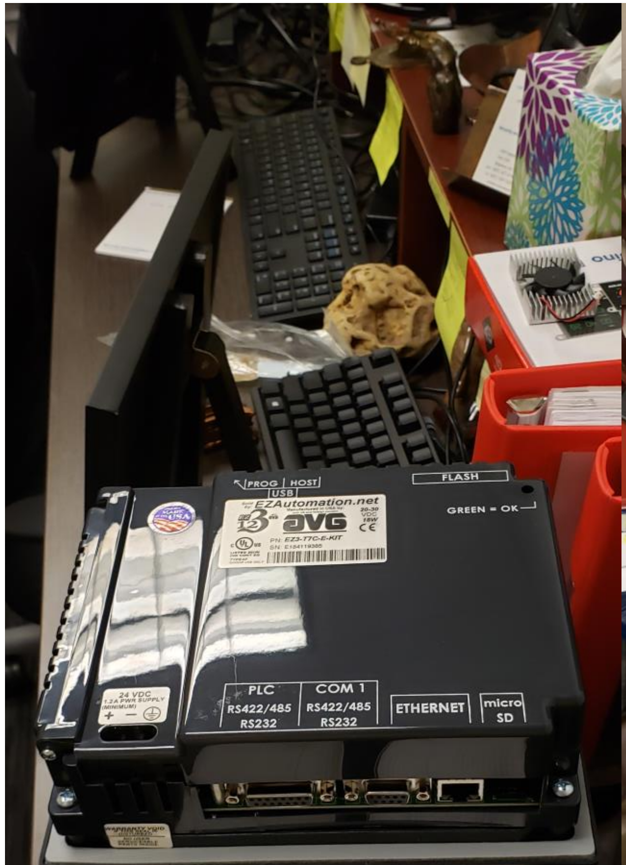
Testing / Experimentation Lab

- Lab contains both IT and OT components
- Closed network running Kali Linux, Windows 7, Ubuntu, Metasploitable,
- Integrated PLCs, SCADA, HMI, and other industrial components
- PLCs open to access and reprogramming for insider threats

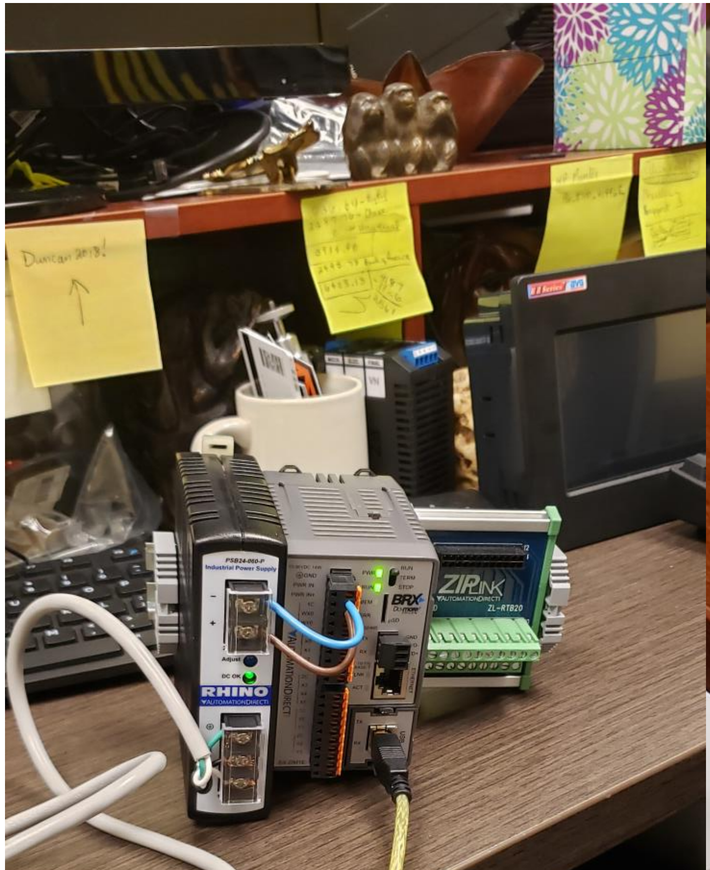
Testing / Experimentation Lab
Kali Linux & IT Equipment



Testing / Experimentation Lab
IDC / SCADA Equipment



Testing / Experimentation Lab
IDC / SCADA Equipment



Current Status of IoT Security Legislation Senate Bill 734 & House Bill 1668

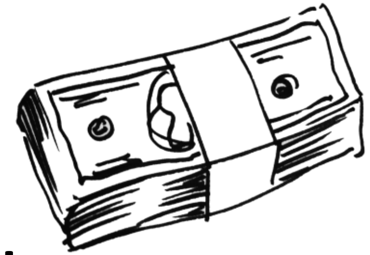
- General Bill that originally included PLCs as “general-purpose computing devices”
- Changes to H.R. 1668 have exempted them; however, that is a concern because of the increase connectivity of OT to IT and thereby, indirectly to the Internet
- Primary purpose of the bills is “To leverage Federal Government procurement power to encourage increase cybersecurity for Internet of Things devices, and for other purposes.”
- There are, however, exemptions that allow a Federal agency to still select insecure devices as long as they are need for national security or research.
- The topic of IToT is not addressed directly in the legislation.

References

- incibe, “Protocols and network security in ICS infrastructures, “ Spanish National Cybersecurity Institute, May, 2015.
- NIST, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-92, Revision 2, May 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Pascal Ackerman, Industrial Cybersecurity, Packt>, 2017.
- Sravani Bhattacharjee, Practical Industrial Internet of Things Security, Packt>, 2018.
- Steve Mackay, Edwin Wright, John Parm Deon Reynders, Practical Industrial Data Networks: Design, Installation and Troubleshooting, IDC Technologies, Elsevier Ltd., 2004.
- Lawrence M. Thompson, Tim Shaw, Industrial Data Communication, 5th Ed., International Society of Automation, 2016
- Trendmicro https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

Things To Remember

- The list can go on and on, cybersecurity and threats never end
- Never enough time, people, and money
- Keep your resume' up-to-date - you never know when it is time to leave or you are asked to leave or the business was hacked and no longer exists



Questions & Answers & Notes

- We can never learn enough about cybersecurity
- We don’t even know how to spell cyber security / cybersecurity
- If you need help please call someone professional –

Who do you call ? Hackbusters!

Security and Analytics, LLC 601-427-4760

Questions & Answers & Notes

- The slides are available on my corporate website – www.securityandanalytics.com
- Continued research will be posted on that site
- Contact me @ gws@securityandanalytics.com
- Office: 601.427.4760
- Business cards are available for all interested