Critical Infrastructure Cybersecurity: An Overview

Presented by:

Daniel E. Capano, SWPCA

Justin Finnigan, Arcadis

Cybercrime is a Growth Industry

- Typically Low risk and High payoff
- Threat Actors will attack soft targets first
- Soft Targets = Many vulnerabilities
- Soft Targets include "Critical Infrastructure"
- Executive Order 13636 defines Critical Infrastructure as:

"*Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters*"

Water Treatment Facilities

- As more automation is used to control and monitor processes, the attack surface grows with it, and threat grows proportionately.
- Conversely, reduction of the human element will *reduce* the attack surface
- Disruption of water supply or waste treatment processes would have major disruptive and health impacts on the populace.
- While there is no financial or technical incentive, mayhem and disruption remain goals
- Air-gapping of the facility is no longer practical

Modes of Attack

- **Social Engineering:** The Human Element
- **B**ring **Y**our **O**wn **D**evice: Mobile devices can be compromised and contain sensitive info
- **Internal Threats:** malicious or disgruntled employees
- **External Threats:** Hostile governments
- **Reconnaissance:** Find and research the target
- **Assessment:** Determine its vulnerabilities
- **Exploit Vulnerability:** Gain access and commit mayhem

Stuxnet: A Game Changer

- Stuxnet is a precision "Digital Weapon", the first to specifically target a control system
- Stuxnet was designed to destroy 1,000 Uranium Enrichment Centrifuges at the highly secure Natanz nuclear enrichment lab in Iran.
- The facility is "air-gapped":

  It is isolated physically and electronically from the world
- Stuxnet specifically targeted Siemens S7 PLCs and attached frequency converters.
- The Worm spread from infected contractor's laptops, which were infected by USB drives
- The Iranian Government was not pleased and retaliated

Sources: Langner, "To Kill a Centrifuge",

Zetter, "Countdown to Zero Day"

The Iranian Counterattack

- The Iranian Government allegedly targeted the Arthur Bowman Dam in Oregon as part of a wide-ranging cyber attack on US businesses
- The dam is 800 feet long, 245 feet high, impounding 10 billion cubic feet of water
- The attack could have closed the floodgates and caused property damage and possible loss of life
- The attack was coordinated by the Iranian Revolutionary Guard Corps (IRGC)

This is what they got:

- The Bowman *Avenue* Dam in Rye Brook, New York.
- 20 feet high and 50 feet long
- An unsecured wireless modem was accessed
- Fortunately, the modem wasn't connected to anything.
- Seven Iranian Nationals were charged in connection with the attacks.

How the Iranians did it

- Reconnaissance:
  - Google "Dorking"
  - Shodan Search Engine
  - Social media: LinkedIn, Facebook
  - Various IT troubleshooting and auditing tools: ICMP, SNMP
- Assessment:
  - Examined publicly available design documents
  - Correlated information and identified vulnerabilities
  - Designed the attack
- The Attack:
  - Exploited the unsecured wireless link

Critical Infrastructure *can* and *will* be attacked

- Maroochy Water District 2000
- The Aurora Generator Vulnerability 2007: https://www.youtube.com/watch?v=fJyWngDco3g
- Pipelines: Siberia 1982, Belligham, WA 1999
- Airports: Worcester Airport 1997, Viet Nam 2016
- Railroads: CSX Corporation 2003, SF Muni 2016
- Power Grids: Ukraine 2007, Cal-ISO 2001

"The Russian and Chinese intelligence services that conduct these attacks have little to fear because we have no practical deterrents to those attacks. This problem is not going away until that changes." –NSA Director Admiral Michael Rogers, 2014

Lessons Learned

- **Critical infrastructure is now a target**
- If an attacker can find you, they can attack you: reducing your online attack surface is critical
- Anything can be hacked
- Obtaining access is the most important step in any attack. Access is the attacker's primary goal.
- Social engineering is a very powerful tool
- How did Stamford WPCA implement safeguards against these threats?

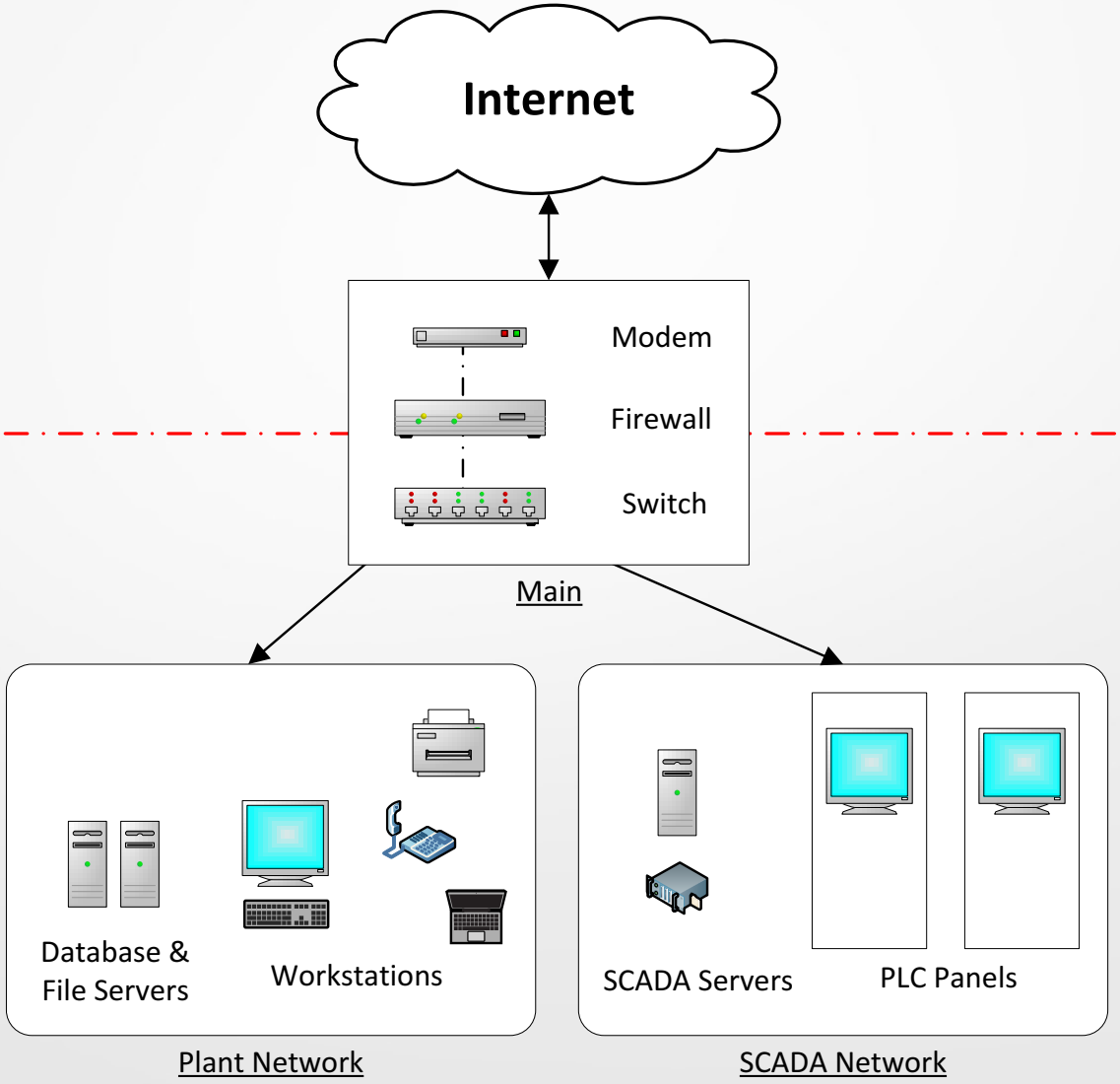
Case Study: WPCA

Case Study: WPCA

- Case Study: Provide separated Plant & SCADA networks with secure VPN access, reporting and expansion capacity
- Network Segmentation
  - Logical networks within an interconnected physical network
  - Access Control Lists for communication between networks
- Encryption for Remote Access
  - VPN for remote SCADA access
- Logging & Reporting for key criteria
  - Intrusion & Threat Detection
  - Bandwidth & Process utilization
  - Security Advisories
- Pros/Cons of this Virtual Networking Approach

Network Topology

- Virtually Isolated Plant & SCADA networks while maintaining physical connectivity
- Provide specific users access to both networks: Database, SCADA, etc.



Network Segmentation I

What is a Firewall?

- A firewall provides data filtering between a secure network and unsecure network.
- Typically an internal network vs. external network (e.g. Internet)
- Can be a *software* or *hardware* based

- Basic home examples:
  - Hardware: Wireless Router
  - Software: Built into Windows/Mac/Linux operating system
  - Standalone examples: pfSense (BSD), IPFire (Linux)

Not robust enough for industrial use

Network Segmentation II

Modem:

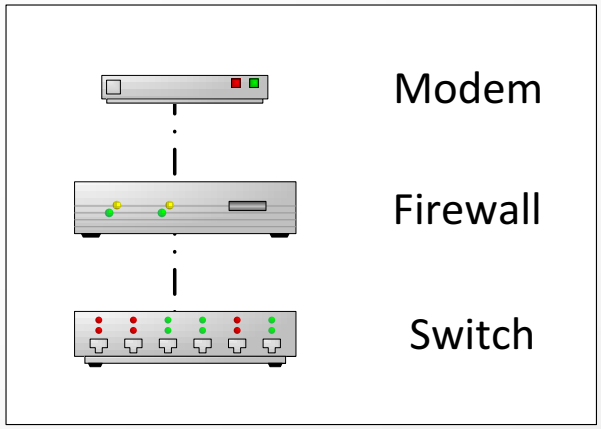
- Connection to Internet: e.g. FIOS, Cable, DSL, Cellular

Firewall:

- Filter data between external and internal networks
- Provide VPN authentication by forming encrypted tunnel
- Reporting: Email reporting

VPN:

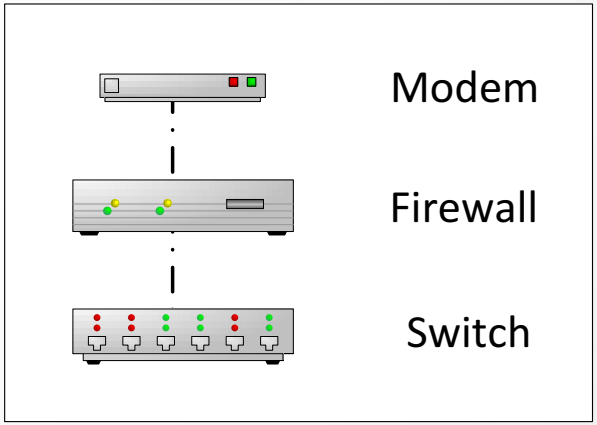
- Remote access to files
- Remote view-only SCADA with iPad



Network Segmentation III

Switch:

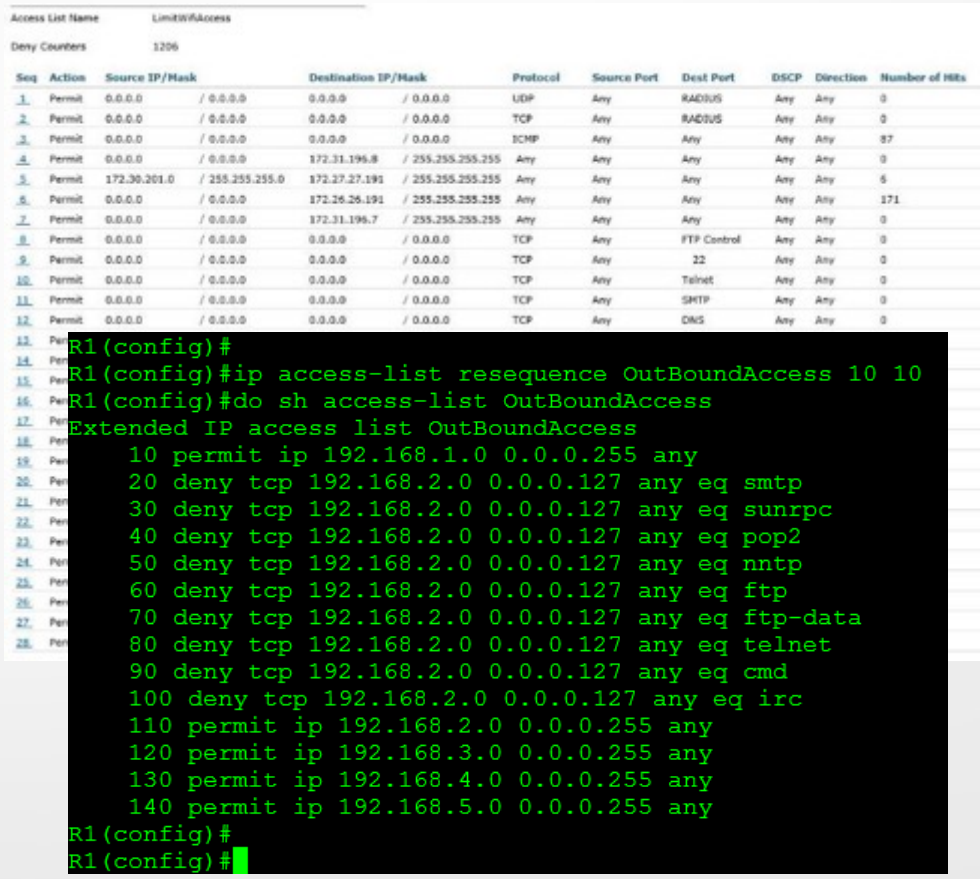
- Support both Copper & Fiber Optic
- Function as Router via OSI *Layer 3* software:
  - Router connects networks
  - Isolates physical networks via Virtual LANs
  - Access Control Lists determine what type of traffic may move in which direction
- Logging & Reporting sent to Email
- Physical separation from Firewall in the event of Intrusion or Failure



Access Control Lists

Provides a layer of security between networks

- Ability to control data flow on a per user basis between networks
- Filter networks based on IP Address and Services
- Limits traffic to improve performance



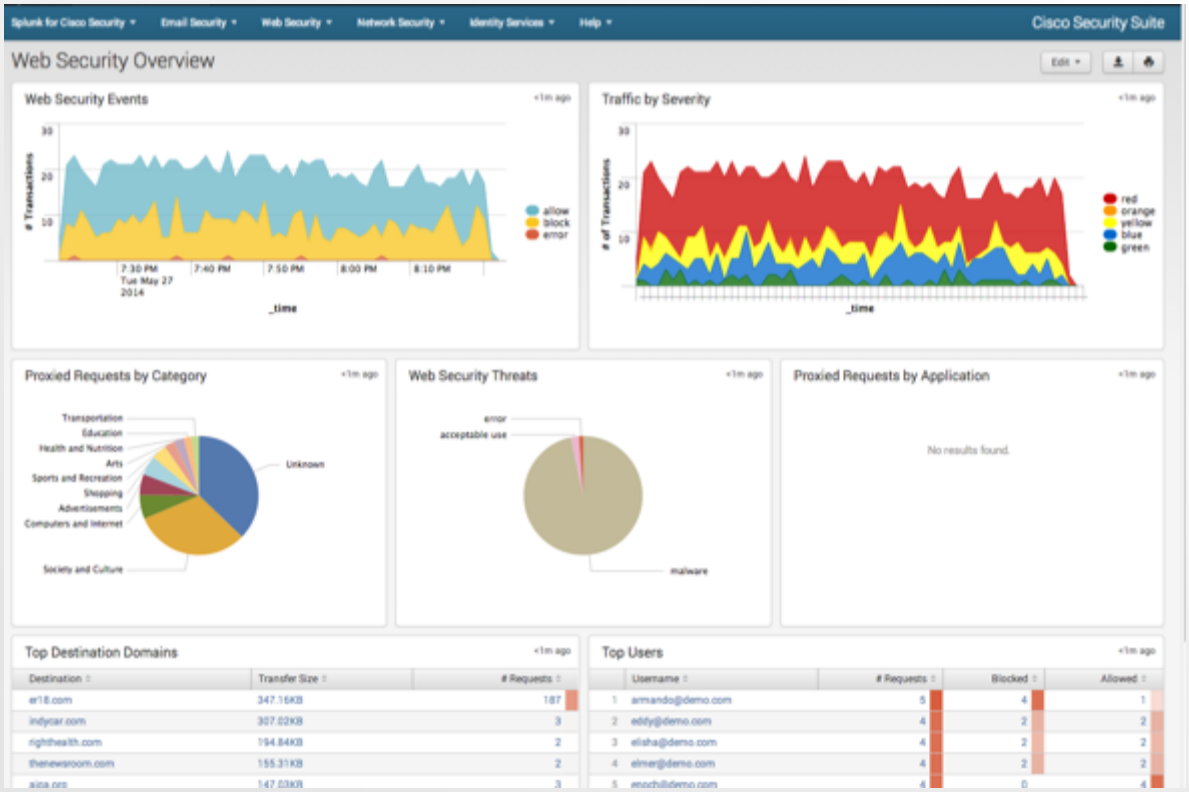
Access List Name LimitWifiAccess

Deny Counters 1206

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	RADIUS	Any	Any	0
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	RADIUS	Any	Any	0
3	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	ICMP	Any	Any	Any	Any	87
4	Permit	0.0.0.0	/ 0.0.0.0	172.31.196.8	/ 255.255.255.255	Any	Any	Any	Any	Any	0
5	Permit	172.30.201.0	/ 255.255.255.0	172.27.27.191	/ 255.255.255.255	Any	Any	Any	Any	Any	6
6	Permit	0.0.0.0	/ 0.0.0.0	172.26.26.191	/ 255.255.255.255	Any	Any	Any	Any	Any	171
7	Permit	0.0.0.0	/ 0.0.0.0	172.31.196.7	/ 255.255.255.255	Any	Any	Any	Any	Any	0
8	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	FTP Control	Any	Any	0
9	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	22	Any	Any	0
10	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	Telnet	Any	Any	0
11	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	SMTP	Any	Any	0
12	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	DNS	Any	Any	0

```
R1(config)#
R1(config)#ip access-list resequence OutBoundAccess 10 10
R1(config)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
    10 permit ip 192.168.1.0 0.0.0.255 any
    20 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
    30 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
    40 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
    50 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
    60 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
    70 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
    80 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
    90 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
    100 deny tcp 192.168.2.0 0.0.0.127 any eq irc
    110 permit ip 192.168.2.0 0.0.0.255 any
    120 permit ip 192.168.3.0 0.0.0.255 any
    130 permit ip 192.168.4.0 0.0.0.255 any
    140 permit ip 192.168.5.0 0.0.0.255 any
R1(config)#
R1(config)#
```

Logging & Reporting



Reporting:

- Process Utilization
- Service-Based Monitoring
- Thread & Intrusion detection
- Breakdowns per service, user, timeframe, etc.

- *Should* keep up with Security Advisories
- *Must* be periodically updated for Security patches

Virtual Networking Benefits

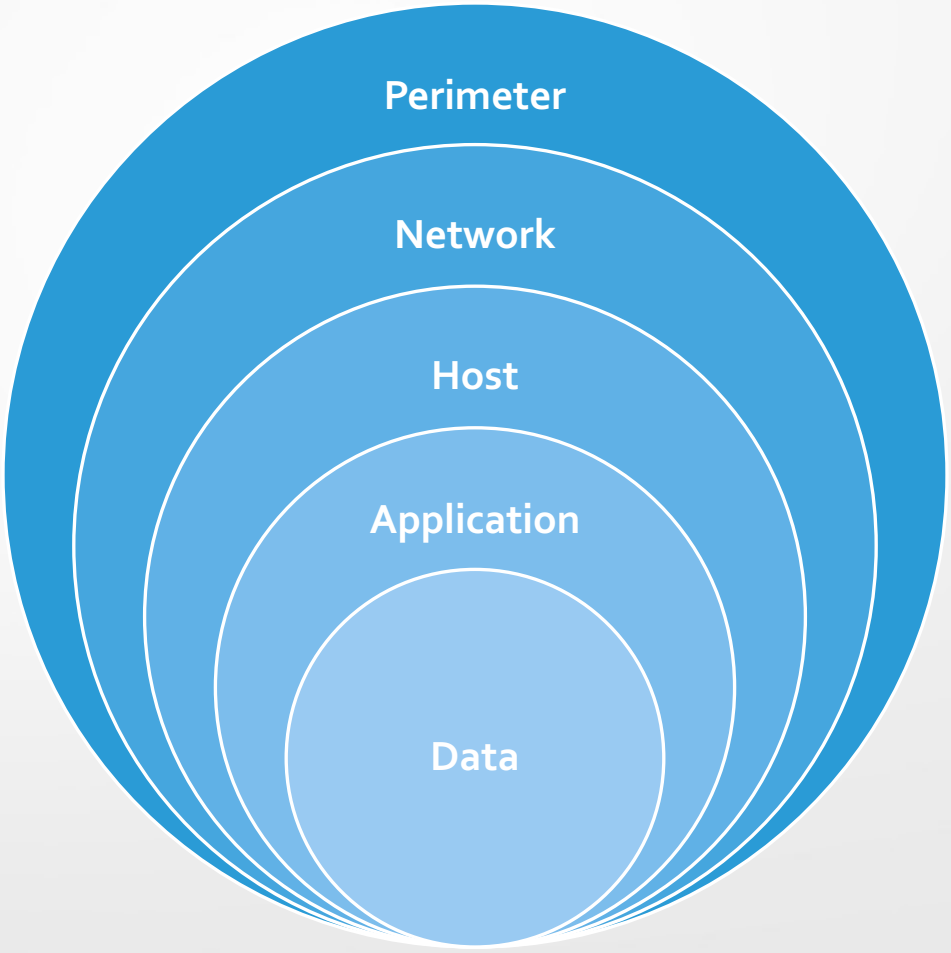
We use Virtual Networking for many reasons!

- Flexibility – logical networks independent of physical hardware
- Security – difficult to determine data paths
- Performance – load sharing across hardware result in more available bandwidth and lower latency
- Management – single points of entry into virtualized management network
- Cost – benefits from economy of scale

A layered and segmented approach to network architecture helps protect critical infrastructure

Defense in Depth

- Layered approach borrowed from the military builds defenses as successive layers around an asset
- Intrusion Detection and Prevention systems (IDS/IPS) are key components
- CIS is based upon this concept using security controls
- Attacker is defeated, misdirected, or captured



Security Controls

Security Controls will reduce your attack surface and frustrate the attacker:

- *Physical: Fences, Guards, locked doors and cabinets, secured IT infrastructure, CCTV*
- *Logical: Firewalls, Segmentation, Obfuscation, Misdirection, Proxy devices, DMZs, reduction of internet facing services*
- *Administrative: Security Policies, Training, Enforcement, "Least Privilege", Separation and classification of responsibilities*

These controls require diligence and enforcement – if you can make an attack infeasible, the attacker will move on to an easier target.

A Few Words on Passwords

- LONGER IS STRONGER
  - Always use mixed upper and lower case, numbers and special characters
  - At least 8 characters – 10 is better
  - Use a phrase as a memory aid or as a passphrase
  - Establish a password policy and enforce it
  - Beware of Phishing Scams: over 90% of cyber attacks begin with a Phishing Email

Social Engineering

- **System Access is the primary goal**
- Regardless of how much money or training or sensational press, humans are the most often compromised component
- Policies, Training, Auditing and Enforcement are the first line of defense
- Reduce your attack surface by reducing your online presence
- Egress control is as important as access control

Thank you

Questions?

Resources For Further Reading

- Executive Order 13636, February 2013
- NIST ICS 800 Series Security Docs:
  - 800-12: Intro to Computer Security; 800-41: Firewalls; 800-82: Industrial Control Systems Security
- Report on Securing and growing the Digital Economy, December 2016
- Presidential Policy Directive 21(PPD-21):Critical Infrastructure Security and Resilience
- DHS – FBI Report: "Grizzly Steppe" December 2016
- Langner: To Kill a centrifuge
- Zetter: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon
- ICS-CERT: https://ics-cert.us-cert.gov/
- The National Strategy for The Physical Protection of Critical Infrastructures, February 2003
- Report on Cybersecurity and Critical Infrastructure in the Americas – OAS, 2015

ARCADIS

The Authors:

- Daniel E. Capano, SWPCA
  - Dan is the SWPCA's vice-chairman and chairs the Authority's Technical committee
  - Certified Wireless Security Professional (CWSP)
- Justin Finnigan, Arcadis
  - 11 years in Water/Wastewater SCADA and Networking
  - Cisco Certified Network Administration (CCNA) trained

ARCADIS