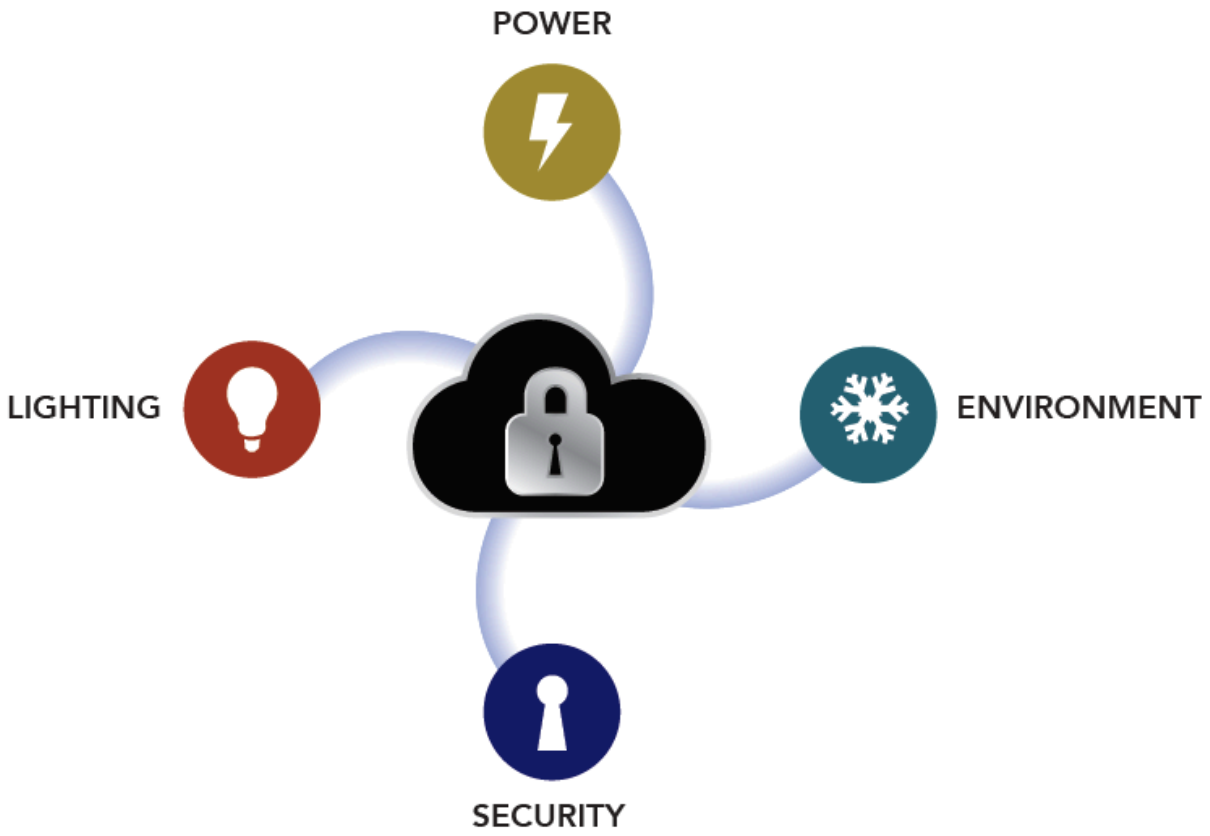
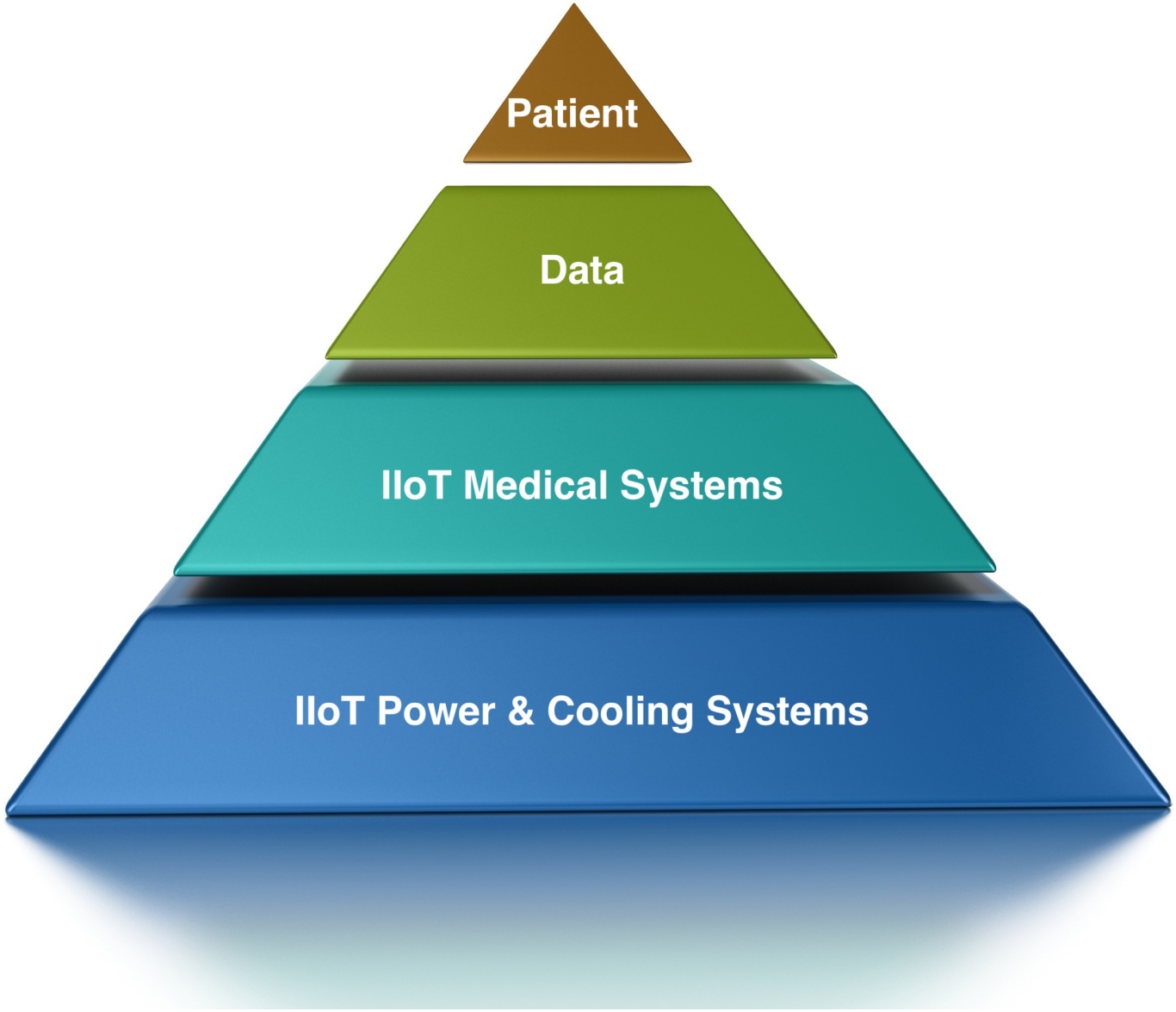
AlphaGuardian™

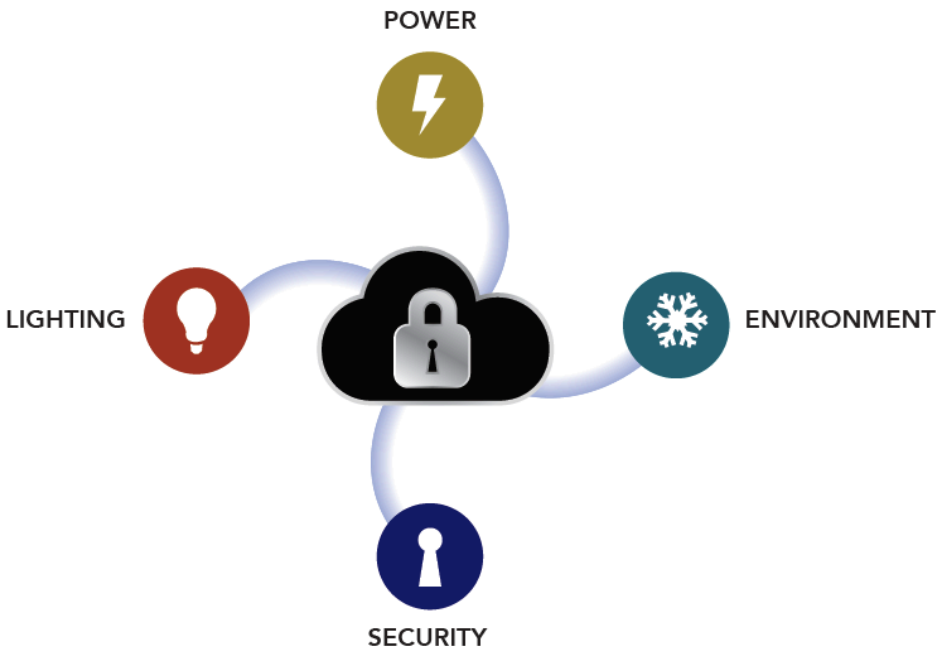
Securing the Industrial Internet of Things



Patients & their Data Sit On Top of IIoT Systems



Designing Secure Systems Is Not an Option



- A single ePHI record can be worth as much as $1,000 on the black market, easily the largest value for a cyber criminal. – Information Week

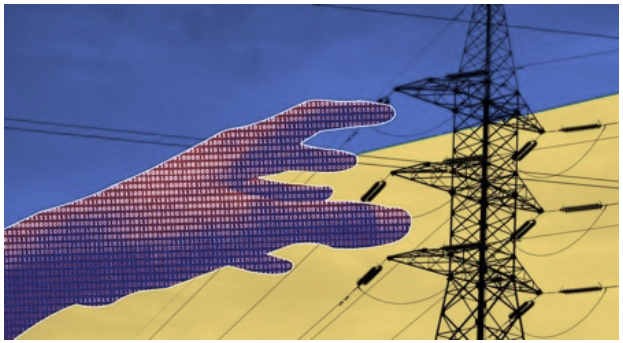
- Healthcare accounts for 25% of all data breaches making it the number one industry target.
  - Becker Hospital Review 4/11/19

Healthcare Breaches Increase Patient Mortality

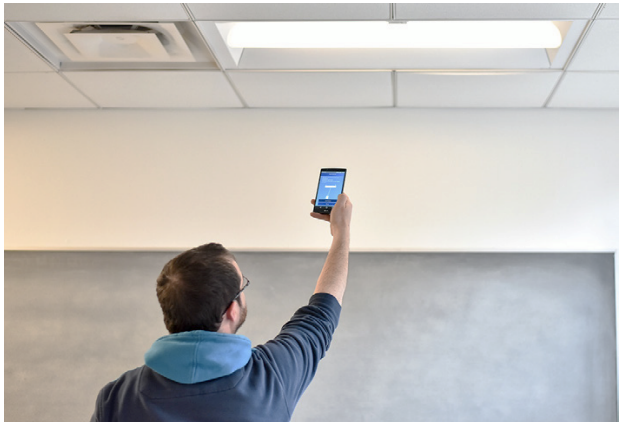
- A major study by Vanderbilt University of 5 years worth of data from 2619 hospitals showed the following:
  - 30 day patient mortality rates increased in all time frames after the breach
  - The increase in mortality rates amounted to 0.34% - 0.45% increase
  - This equates to undoing a full year's worth of mortality gains for an average hospital

IIoT Systems Are Being Actively Exploited

- Major cyber attacks have used IIoT systems as key points of attack.
  - The Russian attack on Ukrainian power plant used control room UPS systems for their attack
  - The Staminus cloud attack used PDU units to attack the data servers
  - Lighting systems have been completely taken over in multiple facilities



staminus™ Communications



Designing Secure IIoT Systems

ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: Advisories by Vendor | Advisories by Vendor - sorted by Last Revised Date

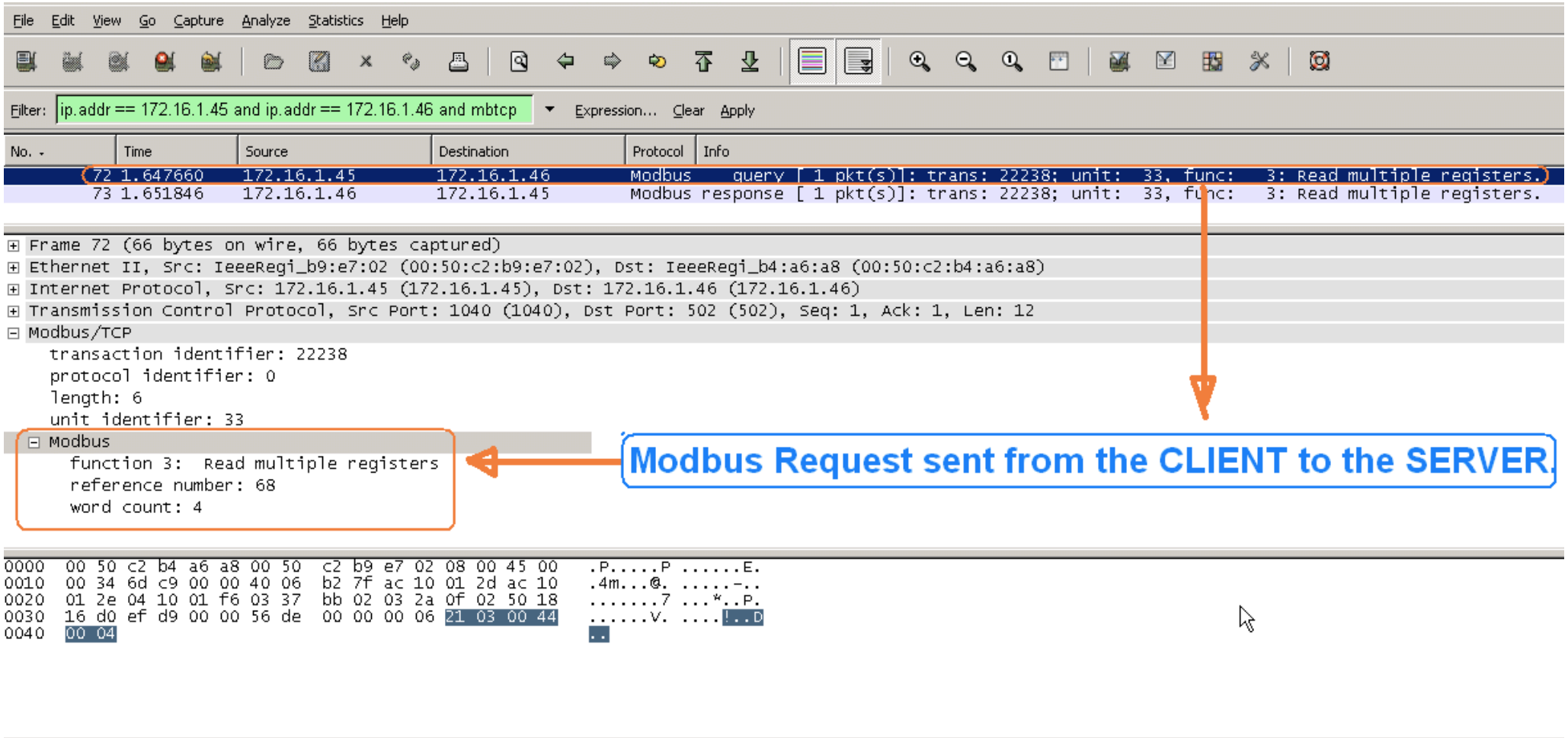
- ICSA-19-050-01 : Intel Data Center Manager SDK
- ICSA-19-050-02 : Delta Industrial Automation CNCSoft
- ICSA-19-050-03 : Horner Automation Cscape
- ICSA-19-050-04 : Rockwell Automation Allen-Bradley PowerMonitor 1000
- ICSA-19-045-01 : Pangea Communications Internet FAX ATA
- ICSA-18-310-01 : gpsd Open Source Project
- ICSA-19-043-01 : OSIsoft PI Vision
- ICSA-19-043-02 : Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relays
- ICSA-19-043-03 : Siemens Licensing Software for SICAM 230 (Update A)
- ICSA-19-043-04 : Siemens SIMATIC S7-300 CPU
- ICSA-19-043-05 : Siemens Intel Active Management Technology of SIMATIC IPCs
- ICSA-19-043-06 : Siemens CP1604 and CP1616
- ICSA-19-038-01 : Siemens SICAM A8000 RTU Series
- ICSA-19-038-02 : Siemens EN100 Ethernet Module
- ICSA-19-036-01 : AVEVA InduSoft Web Studio and InTouch Edge HMI
- ICSA-19-036-02 : Rockwell Automation EtherNet/IP Web Server Modules
- ICSA-19-036-03 : WECON LeviStudioU
- ICSA-19-036-04 : Siemens SIMATIC S7-1500 CPU
- ICSA-19-036-05 : Kunbus PR100088 Modbus Gateway (Update A)
- ICSA-19-031-02 : IDenticard PremiSys
- ICSA-19-031-01 : Schneider Electric EVLink Parking
- ICSMA-19-029-01 : Stryker Medical Beds
- ICSMA-19-029-02 : BD FACSLyric (Update A)
- ICSA-19-029-01 : Yokogawa License Manager Service
- ICSA-19-029-02 : Mitsubishi Electric MELSEC-Q Series PLCs

- IIoT security problems are so pervasive that the Department of Homeland Security has set up a special division just to deal with cybersecurity problems for Industrial Systems: ICS-CERT
- ICS-CERT now issues about 1 new Industrial System Security Advisories every day!

IIoT Communications Are Vulnerable

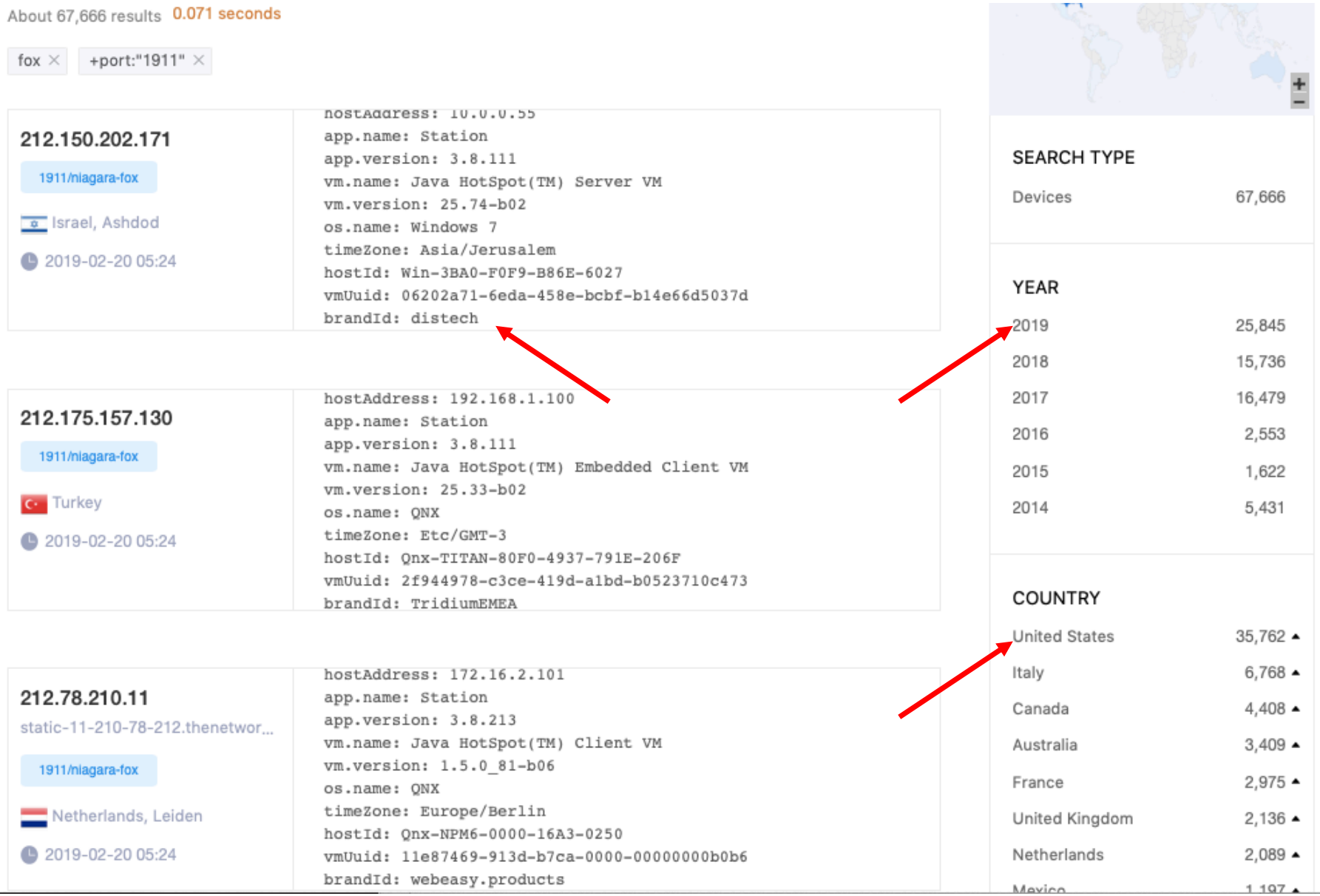
- SNMP
  - Version 1 – No encryption security. All messages broadcast over the network in plain text
  - Version 2 – minimal security. Easy to crack and view.
  - Version 3 – some security but already hacked
- Modbus
  - No security
- BACnet
  - Over 90% of all existing BACnet systems have NO encryption security implemented
  - New BACnet specification promises security but, we will have to wait until it is well tested

Unencrypted Data Is Viewable By Anyone



Hacker Search Engines Produce IIoT Targets

Targting a BMS System



Hospital BMS Systems are Easily Found

166.157.147.73

73.sub-166-157-147.myvzw.com

47808/bacnet

United States

2019-03-05 13:54

```
Vendor ID: Reliable Controls Corporation (35)
  Vendor Name: Reliable Controls Corporation
  Object-identifier: 3501101
  Firmware: 8.24\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
  Application Software: 8.24\x00\x00\x00\x00\x00\x00\x00\x00\x
  Object Name: 1ST-FLOOR-HOSPITAL - MP-C
  Model Name: MACH-ProCom
  Description:
  Location: 1st Floor
```

206.188.239.26

206-188-239-26.static.arvig.net

47808/bacnet

United States, Perham

2019-01-24 21:24

```
Vendor ID: Johnson Controls Inc. (5)
  Vendor Name: JCI
  Object-identifier: 502
  Firmware: 5.2.11.0200
  Application Software:
  Object Name: SET00108D03F41B
  Model Name: MS-NCE2560-0
  Description: PERHAM MEMORIAL HOSPITAL, PERHAM , MN
  Location:
```

Standards Require Secure IIoT Systems

- All major national security standards require protecting critical power systems such as UPS and PDU units and building control systems, such as BMS and lighting control systems.

HIPAA Standards for Power & Enviro Systems

BACKUP POWER MONITORING AND CONTROL

164.308(a)(7)(ii)(C) Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

HHS Security Bulletin 2: "When a covered entity is operating in emergency mode due to a technical failure or power outage, security processes to protect EPHI must be maintained."

ENVIRONMENTAL MONITORING AND CONTROL

164.304 "Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards…"

What Are The Best Practices for Protection?

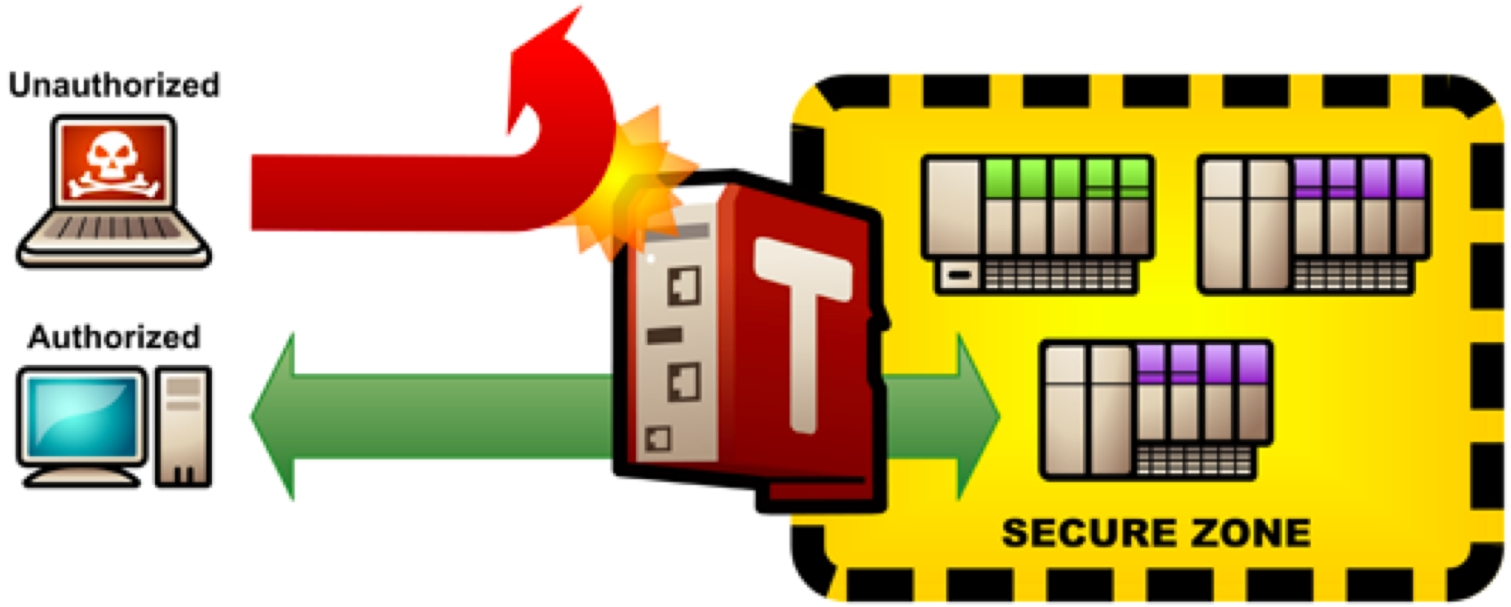
- With cyberattacks being an everyday occurrence, if you fail to plan to protect your site, then you are effectively planning to fail.

  - ✓ *Cybersecurity needs to be part of your basic engineering design.*
  - ✓ *The design must be tested in commissioning*
  - ✓ *Follow up after commissioning to ensure all cybersecurity features are up-to-date*

Use Firewalls

- If you have millions of dollars of facilities equipment, you are not going to keep them safe with a $400 firewall
- Place your firewalls between your BMS/Control System servers and the primary connection to your network
- Ensure that your firewall firmware is continuously updated
- A Firewall is NOT a cure-all but it is the first place to start for security

Use a Firewall

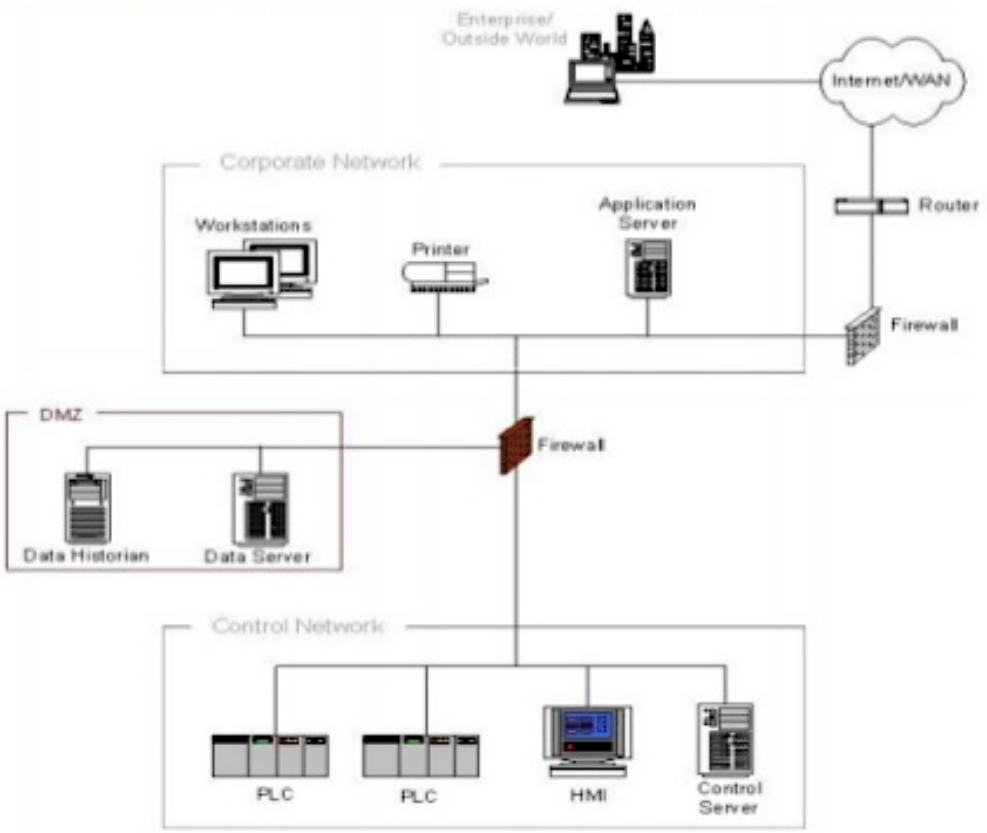


Segment from the IT Network

- NEVER put your control systems on the IT network. Some of the biggest control system breaches have occurred in this type of a system
- Create a De-Militarized Zone between your control network and the IT network
- Segment each logical group of devices on your control network into their own subnetworks

Segment from the IT Network

Common ICS network Segregation Architectures

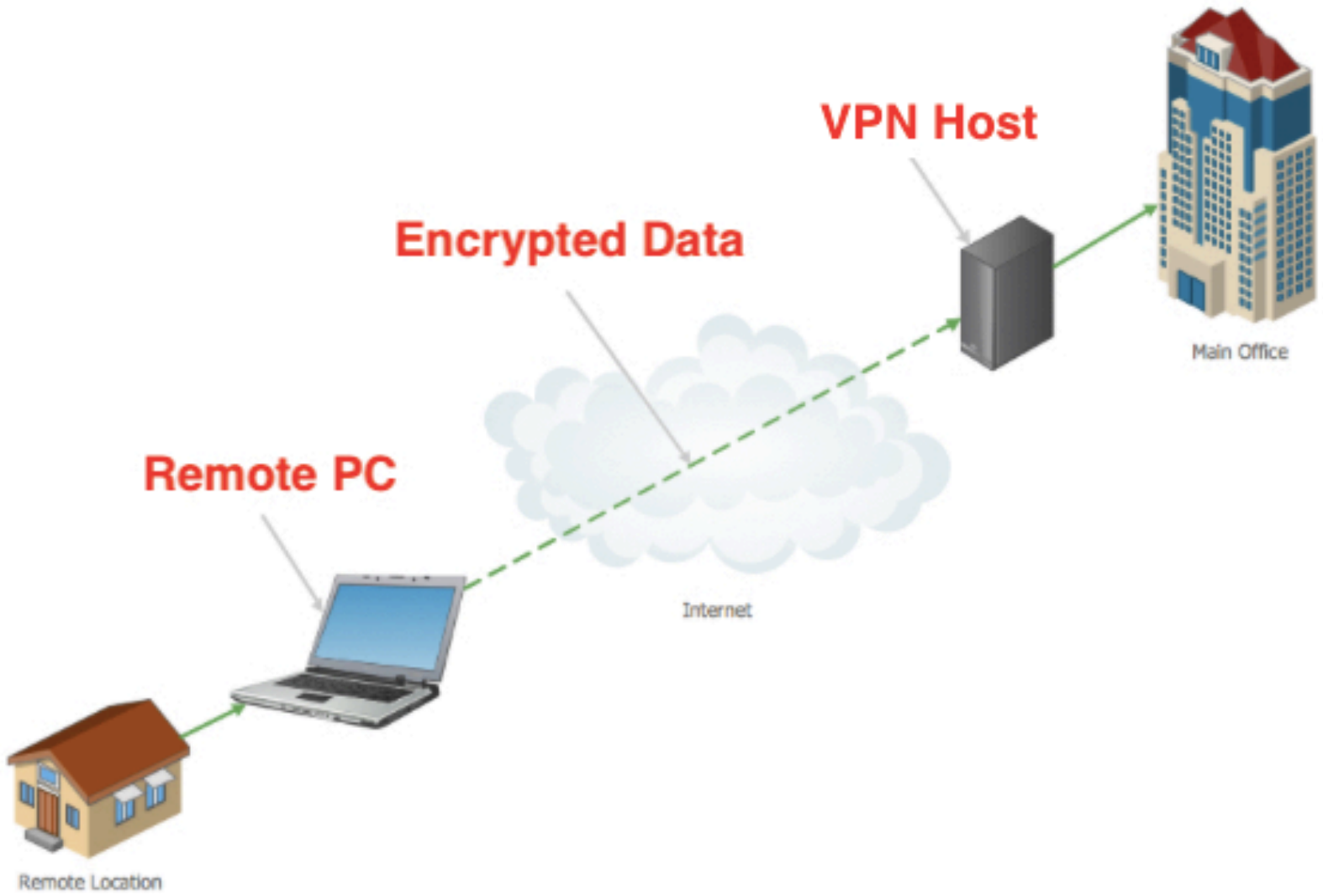


Firewall with DMZ between Corporate Network and Control Network

Use a Virtual Private Network

- A VPN provides a secure, encrypted login to your facilities server
- A VPN provides encryption between your browser and the server for all communications
- There are LOT of choices and you need to make sure you have the right VPN for your network

Use a Virtual Private Network

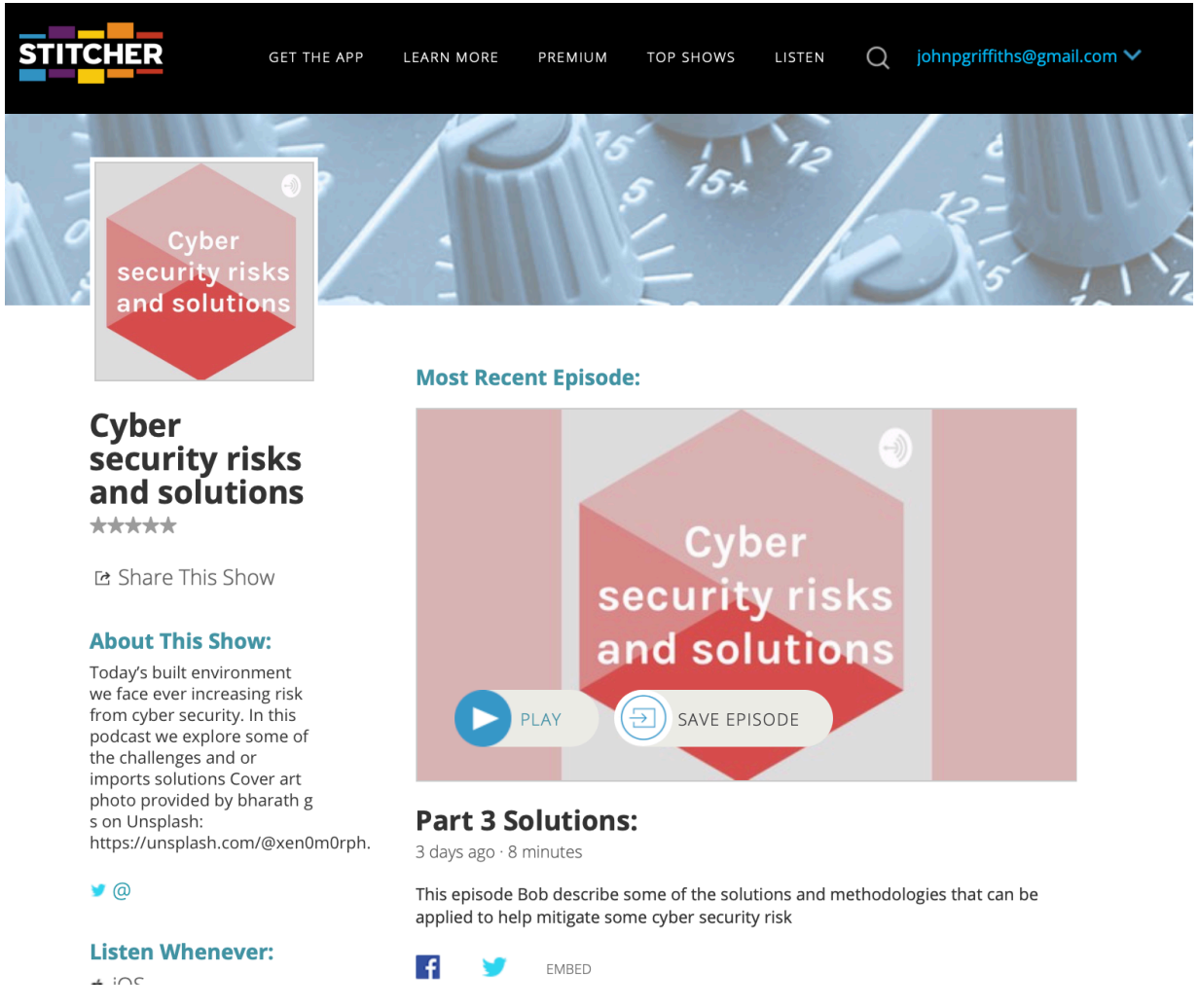


Its a Difficult Task But, Good Planning = Success

- Hackers are banking on the fact that most facilities systems are not well protected.
- By placing the proper security systems in place, you force the bad guys to go find an easier target than your own
- If you follow the steps and choose good products, you can reduce your liability to near $0 because you will be using the latest security designs and best practices

Want to Know More?

[Cyber Security Podcast]



AlphaGuardian™

Contact: Bob Hunter

+1-925-421-0030

111 Deerwood Road, suite 200
San Ramon, CA. 94583

bhunter@alphaguardian.net

www.alphaguardian.net