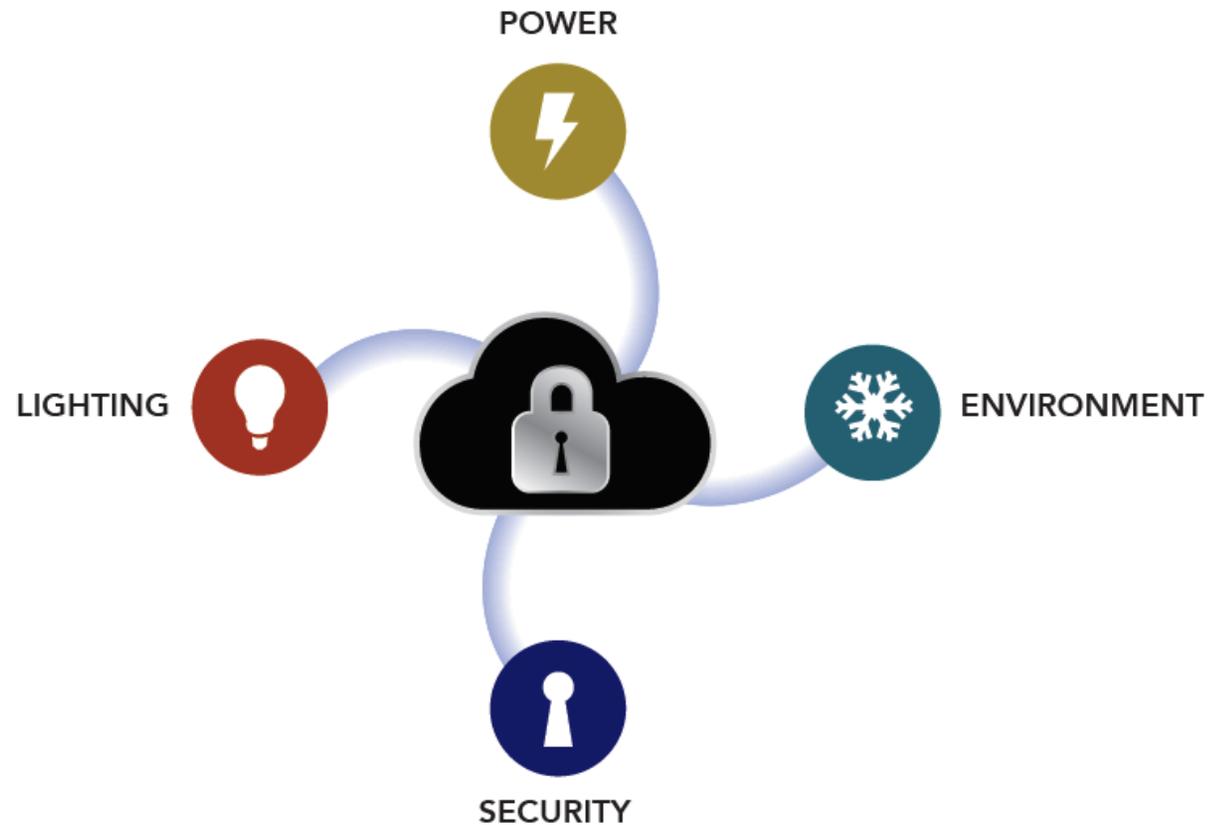


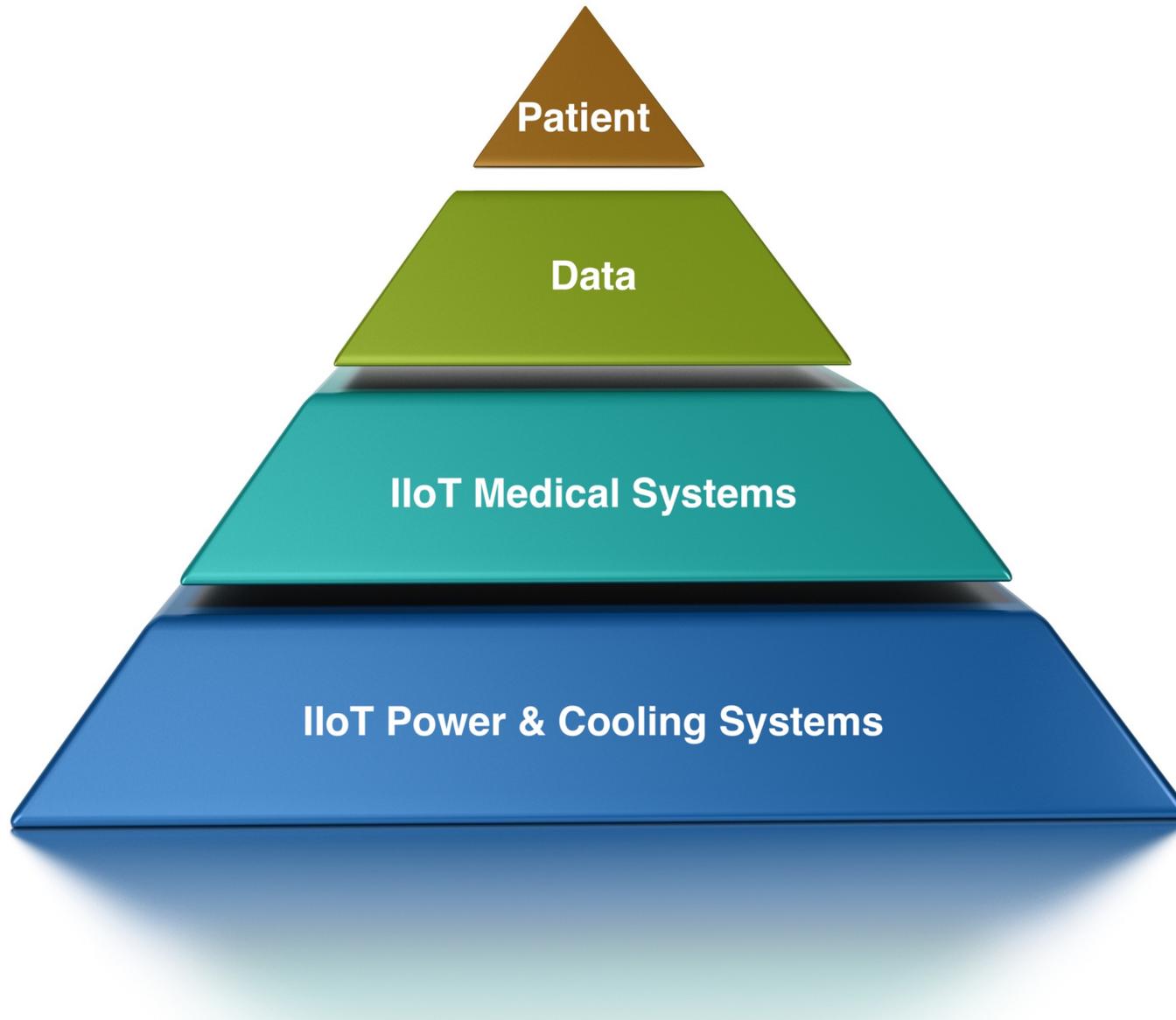


AlphaGuardian™

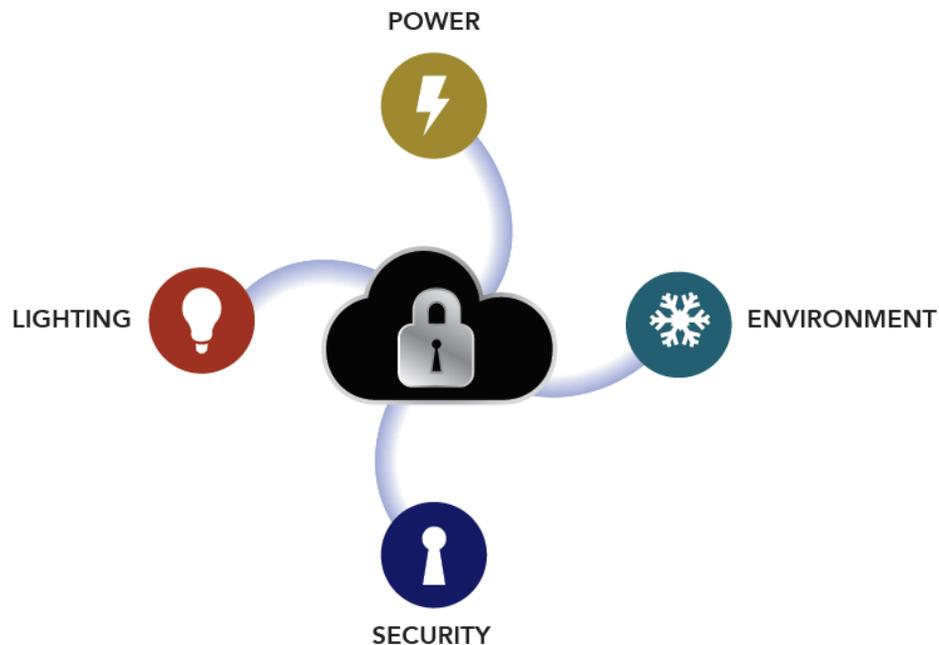
Securing the Industrial Internet of Things



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



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 : OSIssoft 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

The image shows a Wireshark network traffic capture. The filter is set to `ip.addr == 172.16.1.45 and ip.addr == 172.16.1.46 and mbtcp`. The packet list shows two packets: a Modbus query (No. 72) and a Modbus response (No. 73). The packet details pane is expanded to show the Modbus/TCP layer, which includes the transaction identifier (22238), protocol identifier (0), length (6), and unit identifier (33). The Modbus layer is also expanded, showing function 3 (Read multiple registers), reference number 68, and word count 4. A blue callout box with an arrow points to the Modbus layer details, containing the text "Modbus Request sent from the CLIENT to the SERVER". The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
72	1.647660	172.16.1.45	172.16.1.46	Modbus	query [1 pkt(s)]: trans: 22238; unit: 33, func: 3: Read multiple registers.
73	1.651846	172.16.1.46	172.16.1.45	Modbus	response [1 pkt(s)]: trans: 22238; unit: 33, func: 3: Read multiple registers.

Frame 72 (66 bytes on wire, 66 bytes captured)

- Ethernet II, Src: IeeeRegi_b9:e7:02 (00:50:c2:b9:e7:02), Dst: IeeeRegi_b4:a6:a8 (00:50:c2:b4:a6:a8)
- Internet Protocol, src: 172.16.1.45 (172.16.1.45), dst: 172.16.1.46 (172.16.1.46)
- Transmission Control Protocol, Src Port: 1040 (1040), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
- Modbus/TCP
 - transaction identifier: 22238
 - protocol identifier: 0
 - length: 6
 - unit identifier: 33
 - Modbus
 - function 3: Read multiple registers
 - reference number: 68
 - word count: 4

Modbus Request sent from the CLIENT to the SERVER

```
0000 00 50 c2 b4 a6 a8 00 50 c2 b9 e7 02 08 00 45 00 .P.....P.....E.
0010 00 34 6d c9 00 00 40 06 b2 7f ac 10 01 2d ac 10 .4m...@. ....-..
0020 01 2e 04 10 01 f6 03 37 bb 02 03 2a 0f 02 50 18 .....7 ...*.P.
0030 16 d0 ef d9 00 00 56 de 00 00 00 06 21 03 00 44 .....V. ....!..D
0040 00 04 ..
```

Hacker Search Engines Produce IIoT Targets

About 67,666 results 0.07

fox × +port:"1911" ×

212.150.202.171

1911/niagara-fox

Israel, Ashdod

2019-02-20 05:24

```
nostAddress: 10.0.0.55
app.name: Station
app.version: 3.8.111
vm.name: Java HotSpot(TM) Server VM
vm.version: 25.74-b02
os.name: Windows 7
timeZone: Asia/Jerusalem
hostId: Win-3BA0-F0F9-B86E-6027
vmUuid: 06202a71-6eda-458e-bcbf-b14e66d5037d
brandId: distech
```

212.175.157.130

1911/niagara-fox

Turkey

2019-02-20 05:24

```
hostAddress: 192.168.1.100
app.name: Station
app.version: 3.8.111
vm.name: Java HotSpot(TM) Embedded Client VM
vm.version: 25.33-b02
os.name: QNX
timeZone: Etc/GMT-3
hostId: Qnx-TITAN-80F0-4937-791E-206F
vmUuid: 2f944978-c3ce-419d-a1bd-b0523710c473
brandId: TridiumEMEA
```

212.78.210.11

static-11-210-78-212.th

1911/niagara-fox

Netherlands, Leiden

2019-02-20 05:24

```
hostAddress: 172.16.2.101
app.name: Station
app.version: 3.8.213
vm.name: Java HotSpot(TM) Client VM
vm.version: 1.5.0_81-b06
os.name: QNX
```



SEARCH TYPE

Devices 67,666

YEAR

2019	25,845
2018	15,736
2017	16,479
2016	2,553
2015	1,622
2014	5,431

COUNTRY

United States	35,762 ▲
Italy	6,768 ▲
Canada	4,408 ▲
Australia	3,409 ▲
France	2,975 ▲
United Kingdom	2,136 ▲
Netherlands	2,089 ▲
Mexico	1,197 ▲

Targeting a BMS System

About 67,666 results 0.071 seconds

fox × +port:"1911" ×

212.150.202.171
1911/niagara-fox
Israel, Ashdod
2019-02-20 05:24

```
nostAddress: 10.0.0.55
app.name: Station
app.version: 3.8.111
vm.name: Java HotSpot(TM) Server VM
vm.version: 25.74-b02
os.name: Windows 7
timeZone: Asia/Jerusalem
hostId: Win-3BA0-F0F9-B86E-6027
vmUuid: 06202a71-6eda-458e-bcbf-b14e66d5037d
brandId: distech
```

212.175.157.130
1911/niagara-fox
Turkey
2019-02-20 05:24

```
hostAddress: 192.168.1.100
app.name: Station
app.version: 3.8.111
vm.name: Java HotSpot(TM) Embedded Client VM
vm.version: 25.33-b02
os.name: QNX
timeZone: Etc/GMT-3
hostId: Qnx-TITAN-80F0-4937-791E-206F
vmUuid: 2f944978-c3ce-419d-a1bd-b0523710c473
brandId: TridiumEMEA
```

212.78.210.11
static-11-210-78-212.thenetwor...
1911/niagara-fox
Netherlands, Leiden
2019-02-20 05:24

```
hostAddress: 172.16.2.101
app.name: Station
app.version: 3.8.213
vm.name: Java HotSpot(TM) Client VM
vm.version: 1.5.0_81-b06
os.name: QNX
timeZone: Europe/Berlin
hostId: Qnx-NPM6-0000-16A3-0250
vmUuid: 11e87469-913d-b7ca-0000-00000000b0b6
brandId: webeasy.products
```



SEARCH TYPE

Devices 67,666

YEAR

2019	25,845
2018	15,736
2017	16,479
2016	2,553
2015	1,622
2014	5,431

COUNTRY

United States	35,762 ▲
Italy	6,768 ▲
Canada	4,408 ▲
Australia	3,409 ▲
France	2,975 ▲
United Kingdom	2,136 ▲
Netherlands	2,089 ▲
Mexico	1,197 ▲

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

Application Software: 8.24\x00

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...”

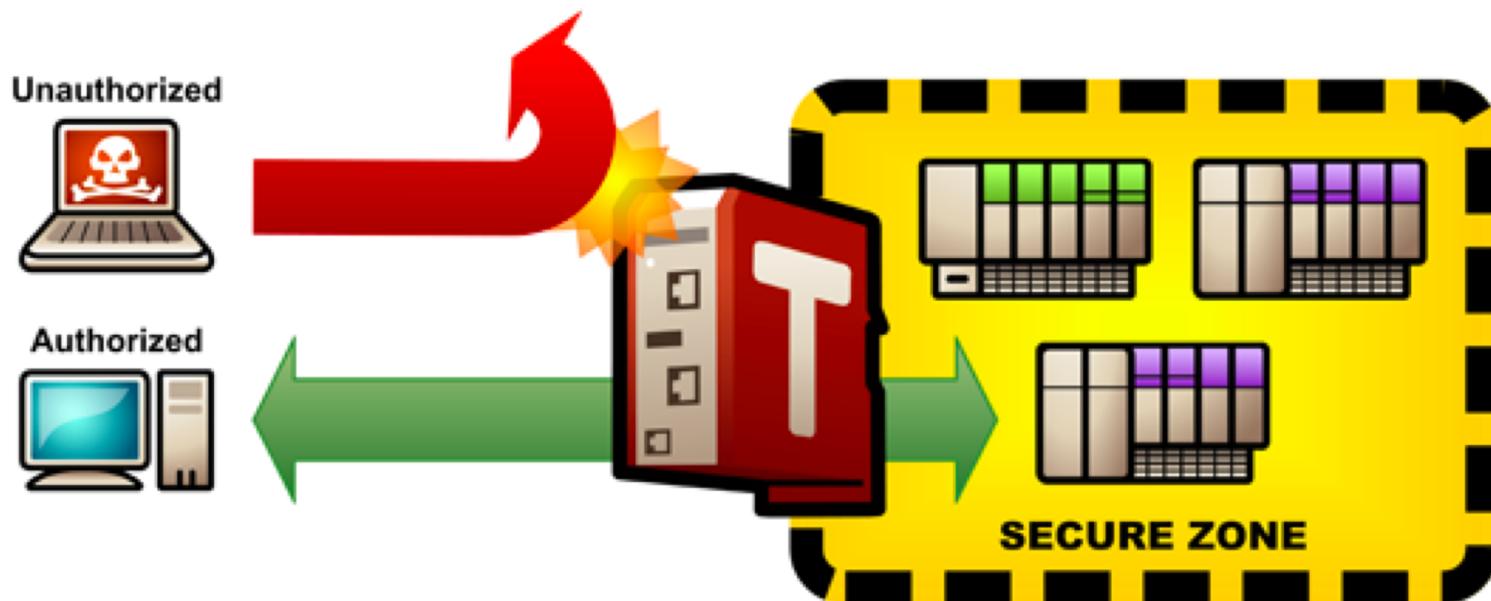
What Are The Best Practices for Protection?

- 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

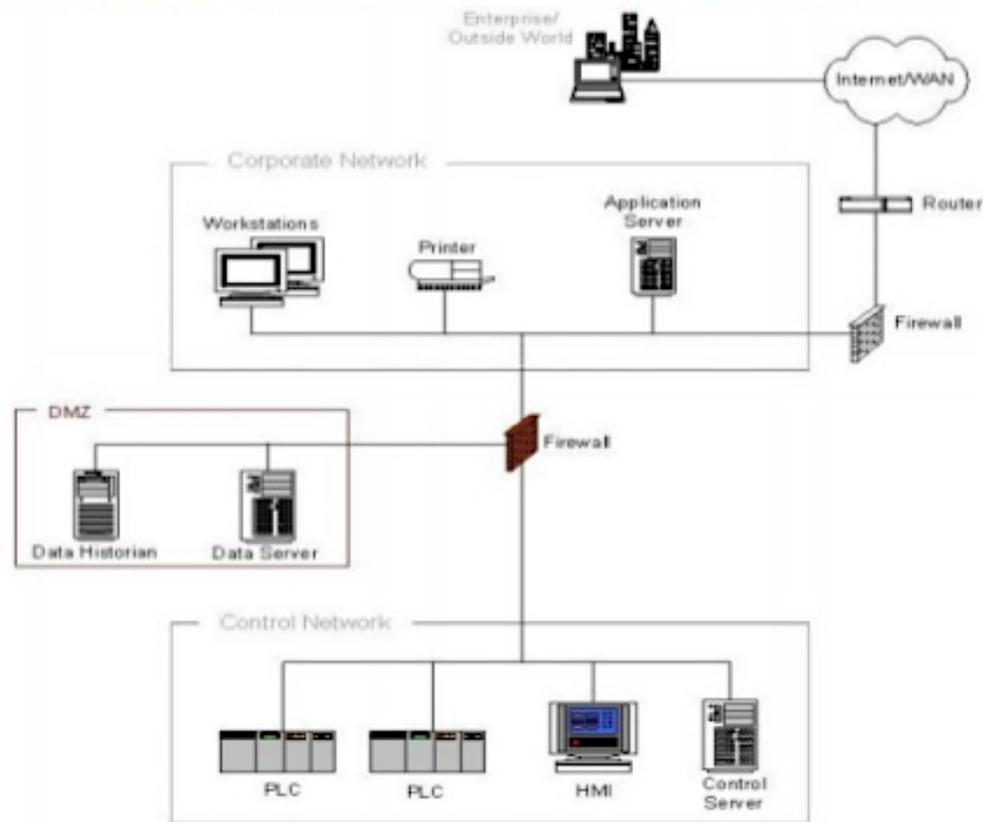


Segment from the IT Network

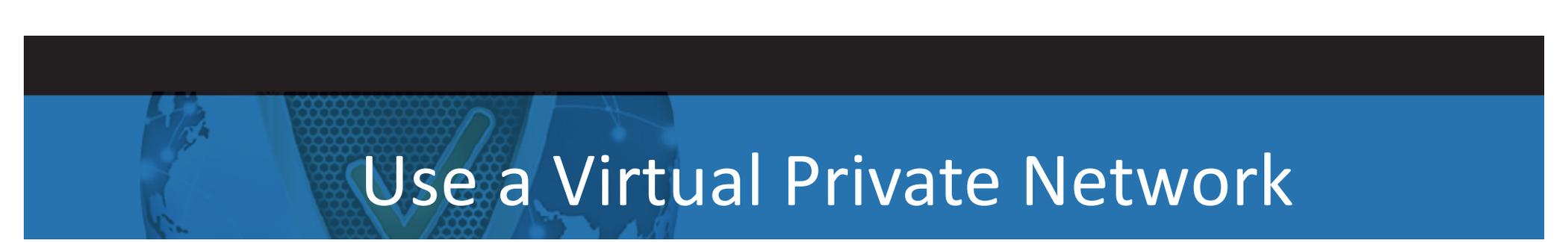
- NEVER put your control systems on the IT network. Some of the biggest control system breaches have occurred in this type of a system
- Create a De-Militarized Zone between your control network and the IT network
- Segment each logical group of devices on your control network into their own subnetworks

Segment from the IT Network

Common ICS network Segregation Architectures



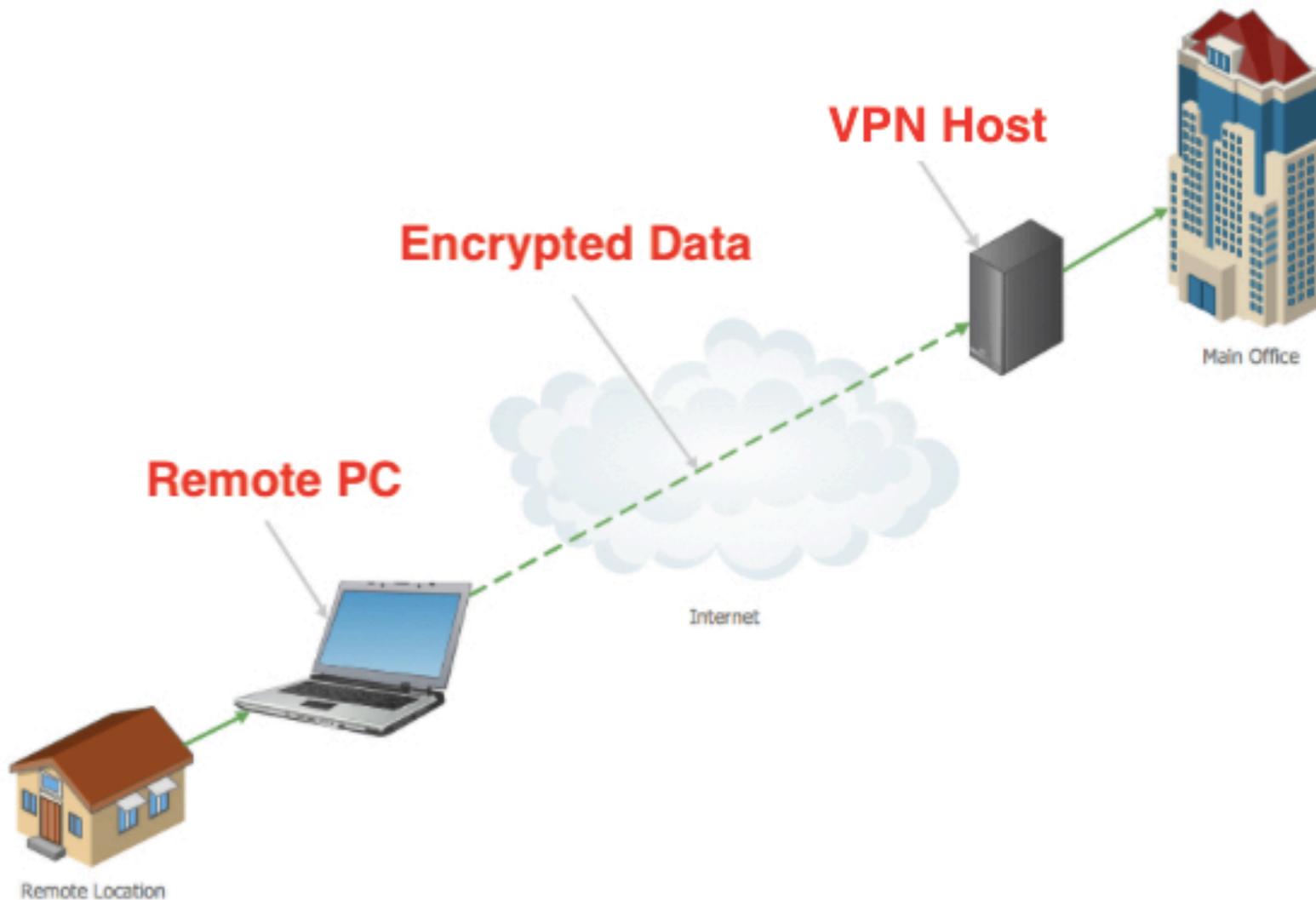
Firewall with DMZ between Corporate Network and Control Network



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

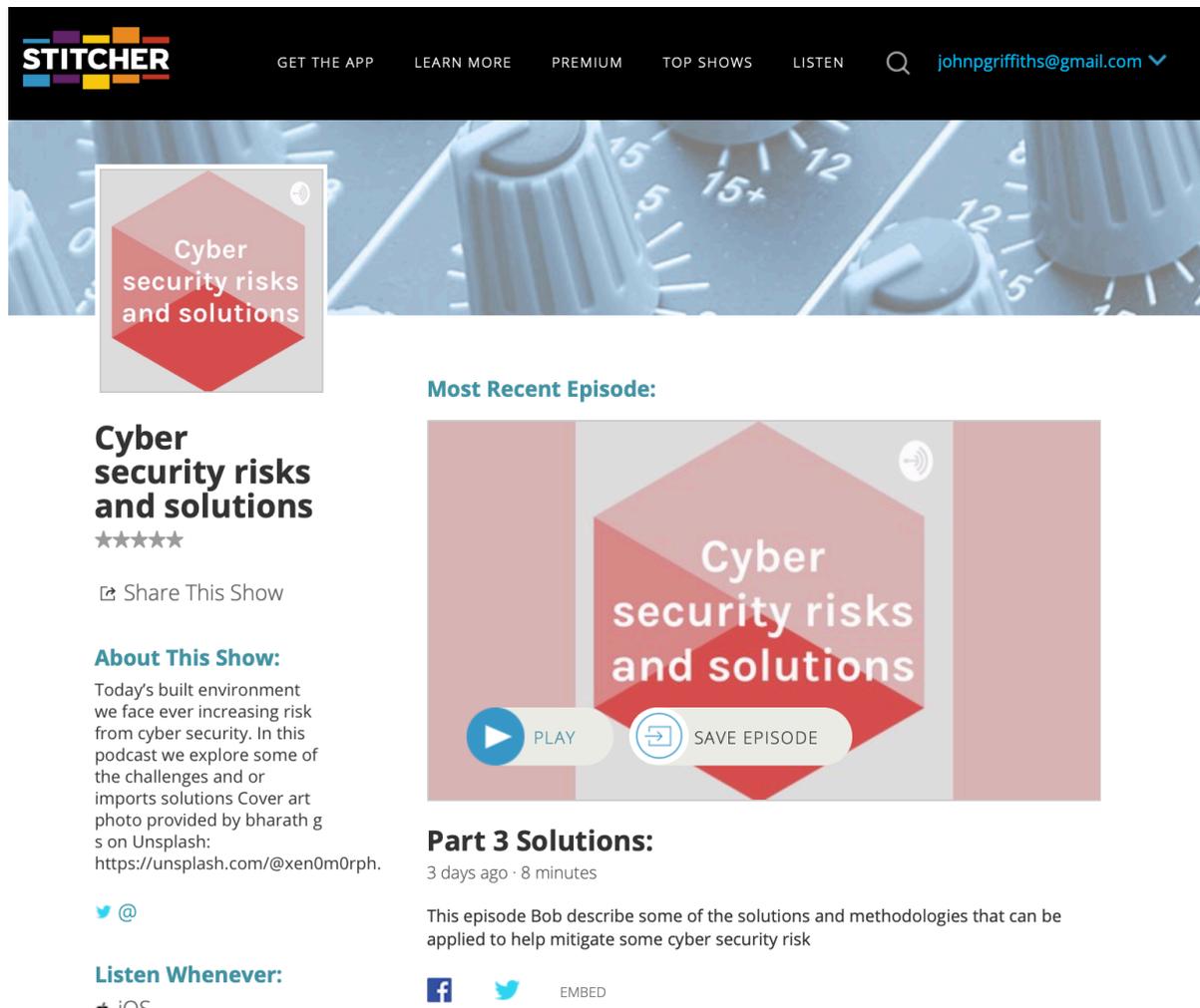


Its a Difficult Task But, Good Planning = Success

- 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



The screenshot shows the Stitcher app interface. At the top, the 'STITCHER' logo is on the left, and navigation links for 'GET THE APP', 'LEARN MORE', 'PREMIUM', 'TOP SHOWS', and 'LISTEN' are in the center. A search icon and the user's email 'johngriffiths@gmail.com' are on the right. Below the navigation bar is a large image of a control panel with knobs and buttons. A red hexagonal overlay on the left contains the text 'Cyber security risks and solutions'. Below this, the podcast title 'Cyber security risks and solutions' is displayed with a five-star rating. A 'Share This Show' link is present. The 'About This Show:' section describes the podcast's focus on cyber security risks and solutions, mentioning a cover art photo by bharath g on Unsplash. A 'Listen Whenever:' section is partially visible. To the right, the 'Most Recent Episode:' section features a large red hexagonal overlay with the podcast title and a 'PLAY' button. Below this, the episode title 'Part 3 Solutions:' is shown with a duration of '3 days ago · 8 minutes'. A description of the episode follows, and social media sharing icons for Facebook and Twitter are at the bottom.

STITCHER GET THE APP LEARN MORE PREMIUM TOP SHOWS LISTEN  johngriffiths@gmail.com 

Cyber security risks and solutions

Cyber security risks and solutions
★★★★★

[Share This Show](#)

About This Show:
Today's built environment we face ever increasing risk from cyber security. In this podcast we explore some of the challenges and or imports solutions Cover art photo provided by bharath g s on Unsplash: <https://unsplash.com/@xen0m0rph>.

[@](#)

Listen Whenever:

Most Recent Episode:

Cyber security risks and solutions

 PLAY  SAVE EPISODE

Part 3 Solutions:
3 days ago · 8 minutes

This episode Bob describe some of the solutions and methodologies that can be applied to help mitigate some cyber security risk

  EMBED



AlphaGuardian™

Contact: Bob Hunter

+1-925-421-0030

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

bhunter@alphaguardian.net

www.alphaguardian.net