Covering your BAS: Simple Steps to Address Cybersecurity Concerns in Your BAS Installations

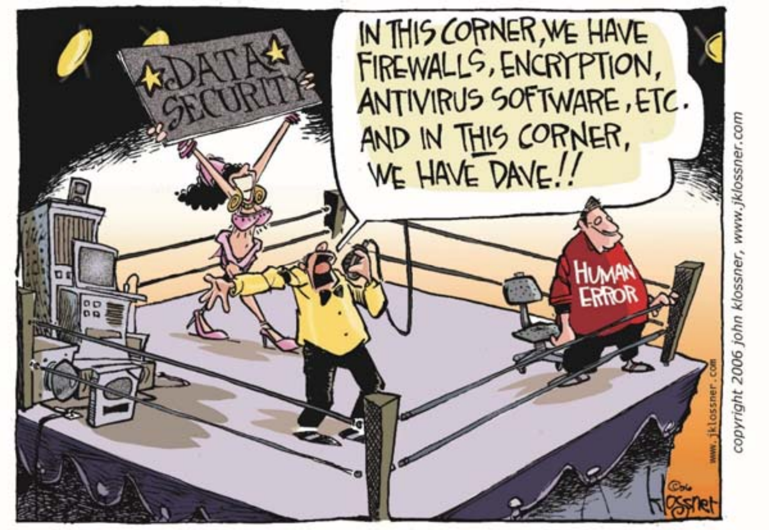
Pook-Ping Yao, CEO
Optigo Networks Inc.

OPTiGO NETWORKS

2017 BICSI *Fall*
CONFERENCE & EXHIBITION
SEPTEMBER 24-28 | LAS VEGAS, NV

Objectives

- Understand cybersecurity threats in Building Internet of Things (B-IoT)
- Understand what can be done to secure B-IoT


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 john klossner, www.jklossner.com
www.jklossner.com
Klossner

Agenda

- Why cybersecurity matters
- Demo
- Basics of cybersecurity
- Secure building networks
- Conclusion

Why cybersecurity matters

Cyber Crime Costs Projected to Reach
$2 Trillion by 2019
- *Forbes*, January 17, 2016

http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6253ee2e3bb0

“IBM's X-Force team hacks into smart building” – CSO Online

“take down a power plant by physically destroying a generator with just 21 lines of code” – Wired.com

“Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.”
- Wikipedia

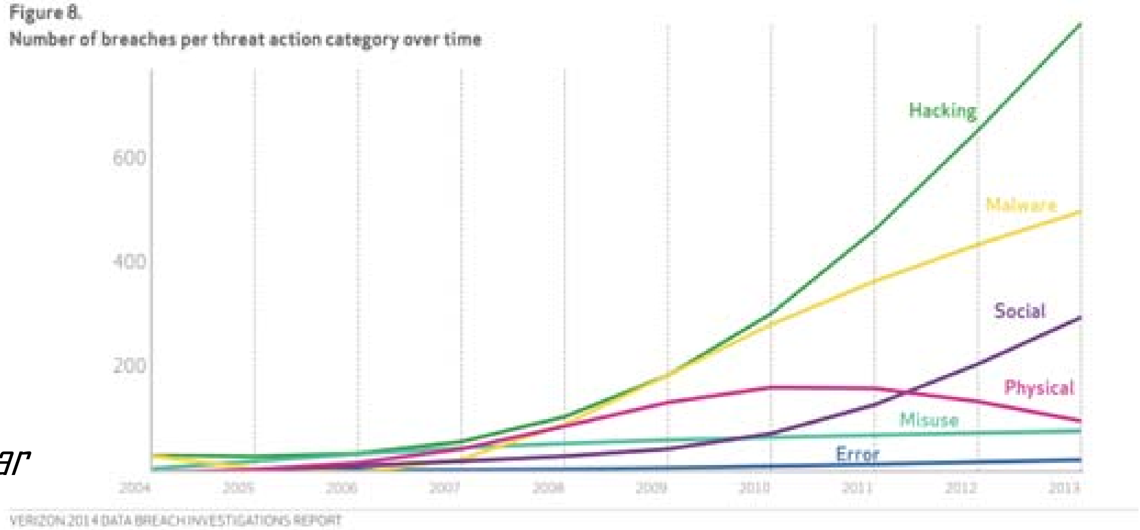
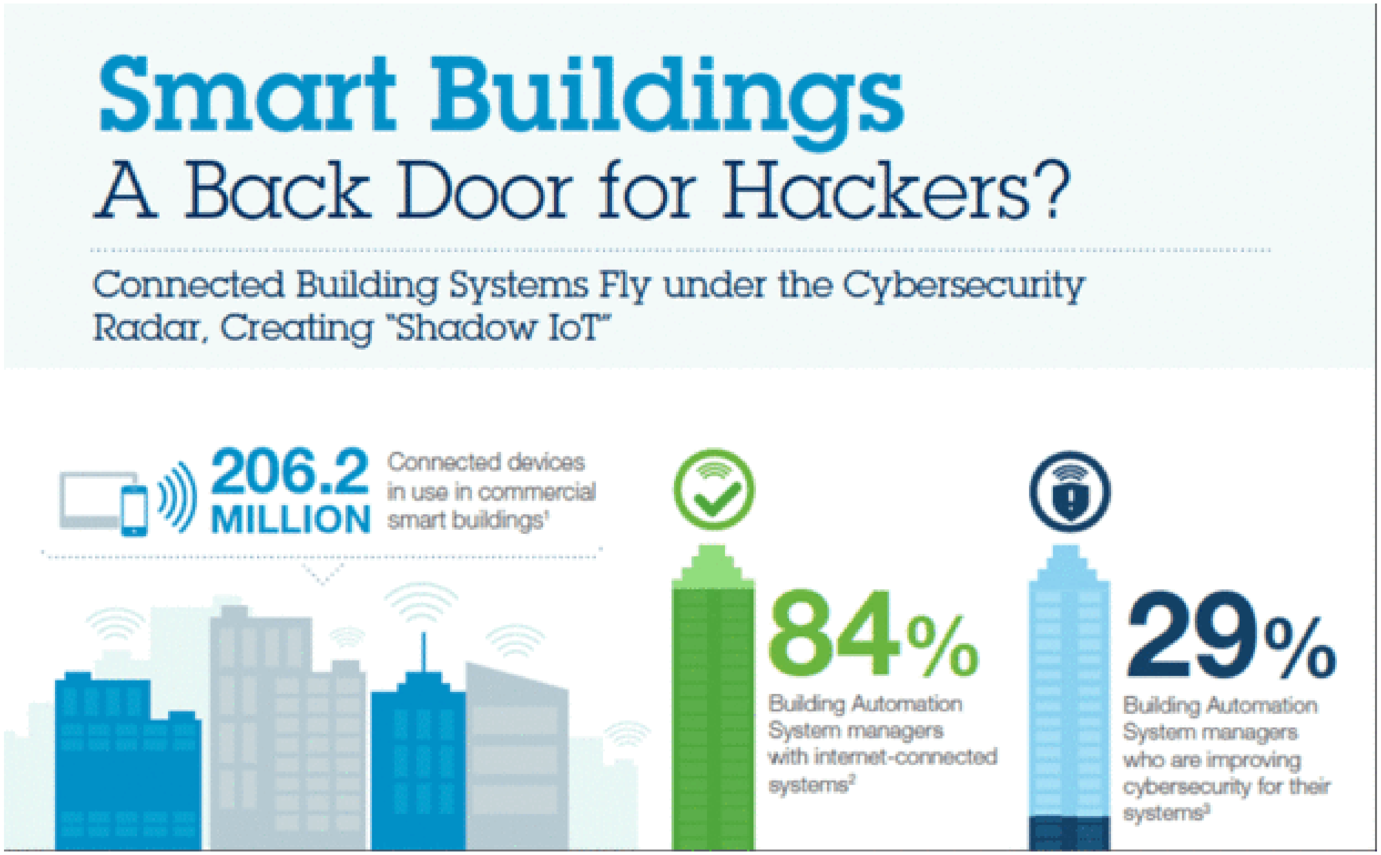


Figure 8.
Number of breaches per threat action category over time

VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

http://resources.infosecinstitute.com/2013-data-breaches-need-know/



Smart Buildings

A Back Door for Hackers?

Connected Building Systems Fly under the Cybersecurity Radar, Creating "Shadow IoT"

206.2 MILLION Connected devices in use in commercial smart buildings[1]

84% Building Automation System managers with internet-connected systems[2]

29% Building Automation System managers who are improving cybersecurity for their systems[3]

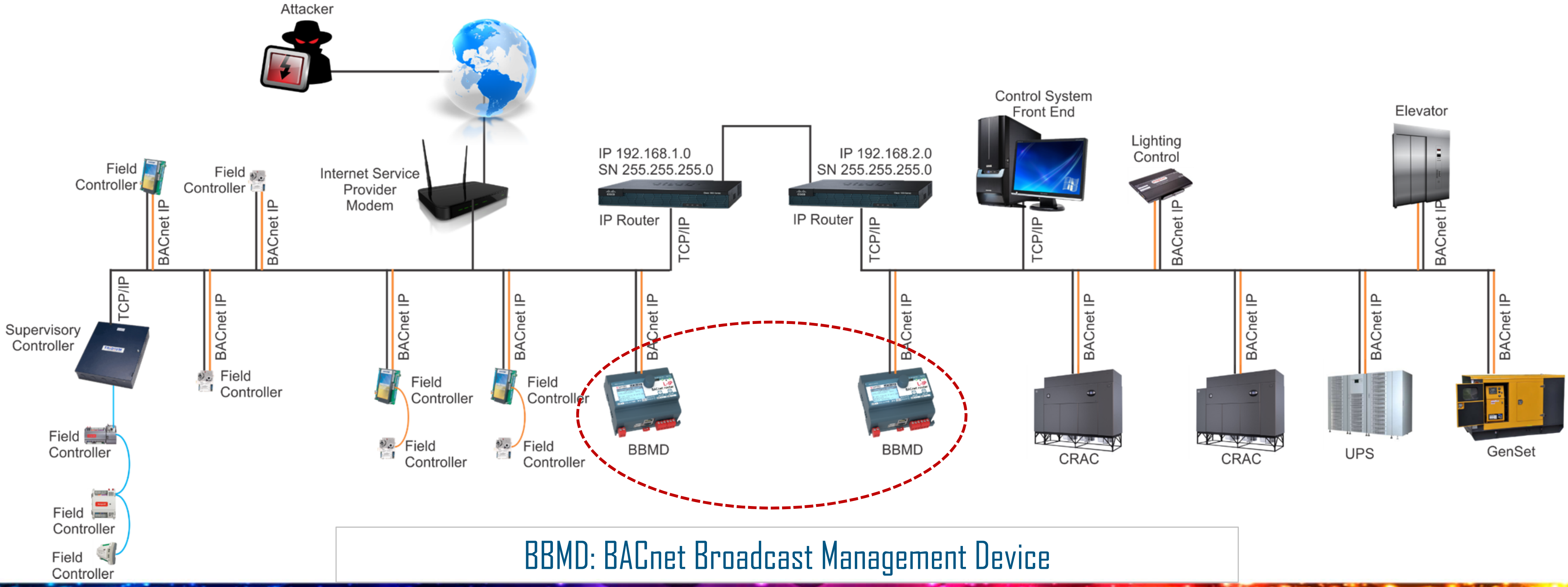
http://www.csoonline.com/article/3031649/security/ibms-x-force-team-hacks-into-smart-building.html

Types of hackers

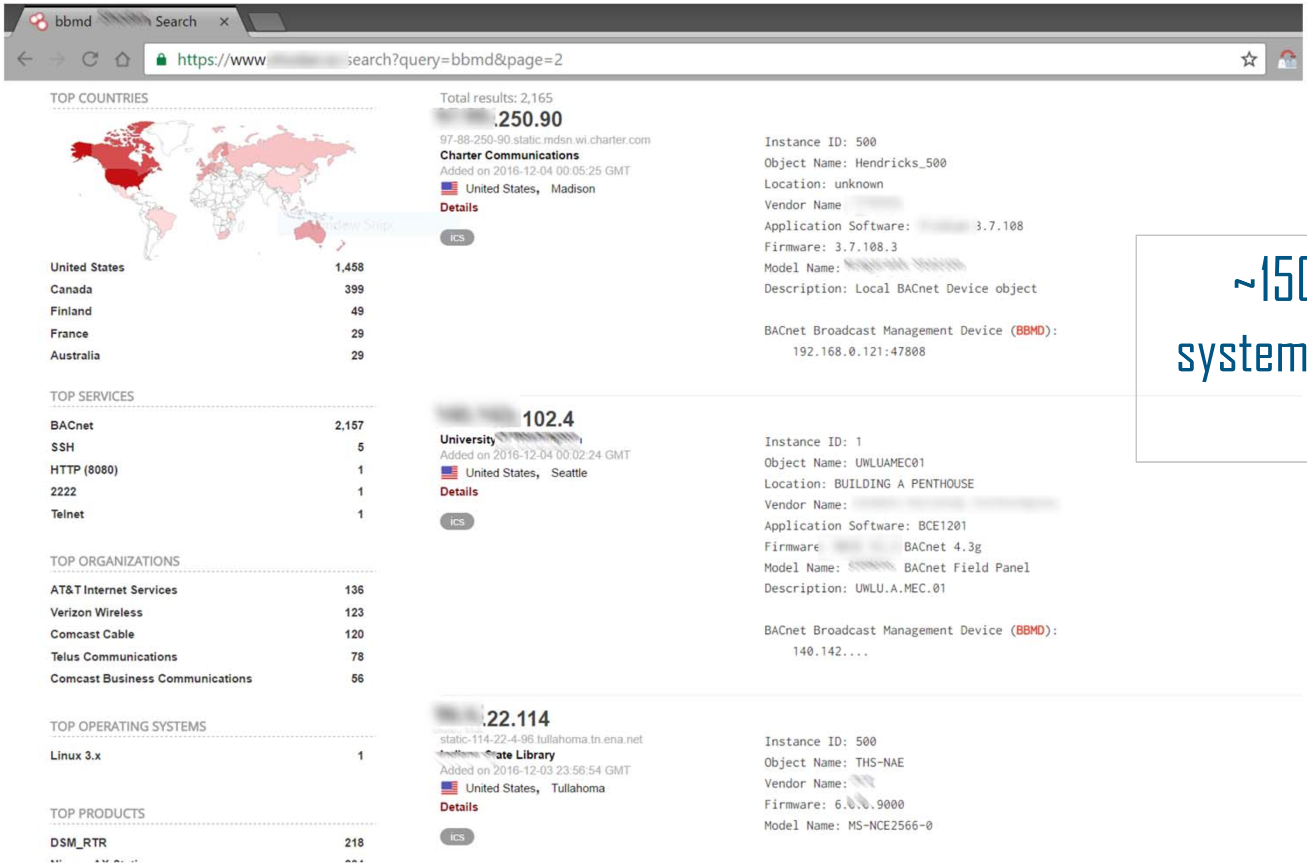
- Script kiddies
- Hacktivist
- Cyber criminals
- National states / sponsored

Demo

Typical Building Automation Systems



BBMD: BACnet Broadcast Management Device



TOP COUNTRIES

United States	1,458
Canada	399
Finland	49
France	29
Australia	29

TOP SERVICES

BACnet	2,157
SSH	5
HTTP (8080)	1
2222	1
Telnet	1

TOP ORGANIZATIONS

AT&T Internet Services	136
Verizon Wireless	123
Comcast Cable	120
Telus Communications	78
Comcast Business Communications	56

TOP OPERATING SYSTEMS

Linux 3.x	1

TOP PRODUCTS

DSM_RTR	218

Total results: 2,165

[redacted].250.90
97-88-250-90.static.mdsn.wi.charter.com
Charter Communications
Added on 2016-12-04 00:05:25 GMT
United States, Madison
Details
ics

```
Instance ID: 500
Object Name: Hendricks_500
Location: unknown
Vendor Name [redacted]
Application Software: [redacted]3.7.108
Firmware: 3.7.108.3
Model Name: [redacted]
Description: Local BACnet Device object

BACnet Broadcast Management Device (BBMD):
    192.168.0.121:47808
```

[redacted]102.4
University[redacted]
Added on 2016-12-04 00:02:24 GMT
United States, Seattle
Details
ics

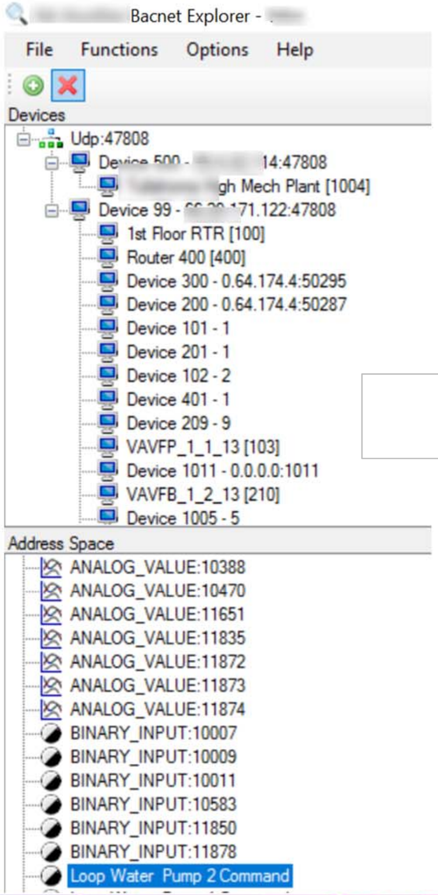
```
Instance ID: 1
Object Name: UWLUAMEC01
Location: BUILDING A PENTHOUSE
Vendor Name: [redacted]
Application Software: BCE1201
Firmware [redacted] BACnet 4.3g
Model Name: [redacted] BACnet Field Panel
Description: UWLU.A.MEC.01

BACnet Broadcast Management Device (BBMD):
    140.142....
```

[redacted].22.114
static-114-22-4-96.tullahoma.tn.ena.net
[redacted]tate Library
Added on 2016-12-03 23:56:54 GMT
United States, Tullahoma
Details
ics

```
Instance ID: 500
Object Name: THS-NAE
Vendor Name: [redacted]
Firmware: 6.[redacted].9000
Model Name: MS-NCE2566-0
```

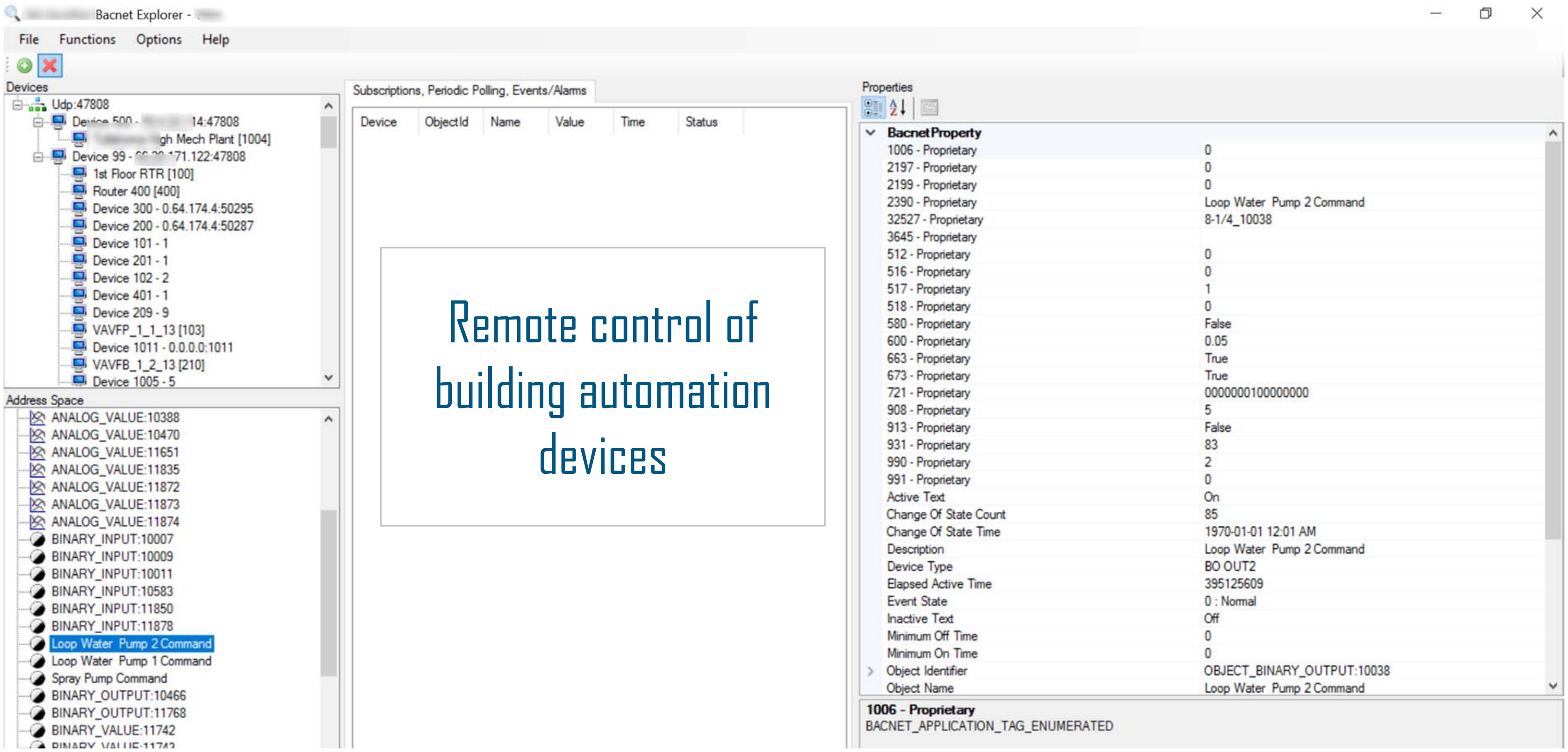
~1500 exposed BACnet systems in one search in the USA



```
Udp:47808
    Device 500 - [redacted]14:47808
        [redacted]gh Mech Plant [1004]
    Device 99 - [redacted]171.122:47808
        1st Floor RTR [100]
        Router 400 [400]
        Device 300 - 0.64.174.4:50295
        Device 200 - 0.64.174.4:50287
        Device 101 - 1
        Device 201 - 1
        Device 102 - 2
        Device 401 - 1
        Device 209 - 9
        VAVFP_1_1_13 [103]
        Device 1011 - 0.0.0.0:1011
        VAVFB_1_2_13 [210]
        Device 1005 - 5
```

```
ANALOG_VALUE:10388
ANALOG_VALUE:10470
ANALOG_VALUE:11651
ANALOG_VALUE:11835
ANALOG_VALUE:11872
ANALOG_VALUE:11873
ANALOG_VALUE:11874
BINARY_INPUT:10007
BINARY_INPUT:10009
BINARY_INPUT:10011
BINARY_INPUT:10583
BINARY_INPUT:11850
BINARY_INPUT:11878
Loop Water Pump 2 Command
```

No login



[redacted] Bacnet Explorer - [redacted]

Devices

- Udp:47808
  - Device 500 - [redacted]14:47808
    - [redacted]gh Mech Plant [1004]
  - Device 99 - [redacted]171.122:47808
    - 1st Floor RTR [100]
    - Router 400 [400]
    - Device 300 - 0.64.174.4:50295
    - Device 200 - 0.64.174.4:50287
    - Device 101 - 1
    - Device 201 - 1
    - Device 102 - 2
    - Device 401 - 1
    - Device 209 - 9
    - VAVFP_1_1_13 [103]
    - Device 1011 - 0.0.0.0:1011
    - VAVFB_1_2_13 [210]
    - Device 1005 - 5

Address Space

- ANALOG_VALUE:10388
- ANALOG_VALUE:10470
- ANALOG_VALUE:11651
- ANALOG_VALUE:11835
- ANALOG_VALUE:11872
- ANALOG_VALUE:11873
- ANALOG_VALUE:11874
- BINARY_INPUT:10007
- BINARY_INPUT:10009
- BINARY_INPUT:10011
- BINARY_INPUT:10583
- BINARY_INPUT:11850
- BINARY_INPUT:11878
- Loop Water Pump 2 Command
- Loop Water Pump 1 Command
- Spray Pump Command
- BINARY_OUTPUT:10466
- BINARY_OUTPUT:11768
- BINARY_VALUE:11742
- BINARY_VALUE:11743

Subscriptions, Periodic Polling, Events/Alarms

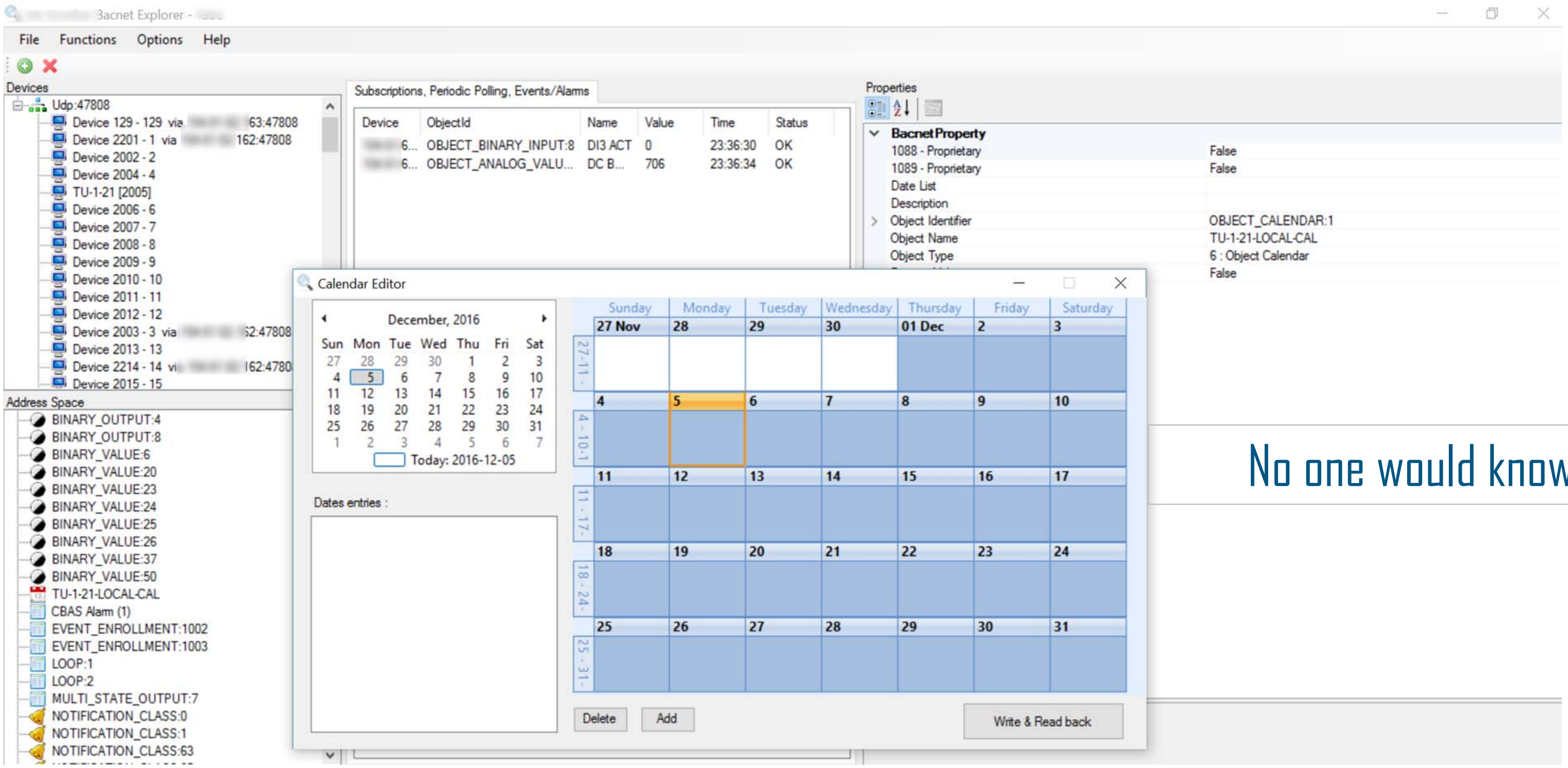
Device	ObjectId	Name	Value	Time	Status

Properties

Bacnet Property	
1006 - Proprietary	0
2197 - Proprietary	0
2199 - Proprietary	0
2390 - Proprietary	Loop Water Pump 2 Command
32527 - Proprietary	8-1/4_10038
3645 - Proprietary	
512 - Proprietary	0
516 - Proprietary	0
517 - Proprietary	1
518 - Proprietary	0
580 - Proprietary	False
600 - Proprietary	0.05
663 - Proprietary	True
673 - Proprietary	True
721 - Proprietary	0000000100000000
908 - Proprietary	5
913 - Proprietary	False
931 - Proprietary	83
990 - Proprietary	2
991 - Proprietary	0
Active Text	On
Change Of State Count	85
Change Of State Time	1970-01-01 12:01 AM
Description	Loop Water Pump 2 Command
Device Type	BO OUT2
Elapsed Active Time	395125609
Event State	0 : Normal
Inactive Text	Off
Minimum Off Time	0
Minimum On Time	0
Object Identifier	OBJECT_BINARY_OUTPUT:10038
Object Name	Loop Water Pump 2 Command

1006 - Proprietary
BACNET_APPLICATION_TAG_ENUMERATED

Remote control of building automation devices


[redacted] Bacnet Explorer - [redacted]
File
Functions
Options
Help
Devices
Subscriptions, Periodic Polling, Events/Alarms
Properties
Calendar Editor
Delete
Add
Write & Read back

Udp:47808
- Device 129 - 129 via [redacted] 63:47808
- Device 2201 - 1 via [redacted] 162:47808
- Device 2002 - 2
- Device 2004 - 4
- TU-1-21 [2005]
- Device 2006 - 6
- Device 2007 - 7
- Device 2008 - 8
- Device 2009 - 9
- Device 2010 - 10
- Device 2011 - 11
- Device 2012 - 12
- Device 2003 - 3 via [redacted] 52:47808
- Device 2013 - 13
- Device 2214 - 14 via [redacted] 162:4780
- Device 2015 - 15

Address Space

- BINARY_OUTPUT:4
- BINARY_OUTPUT:8
- BINARY_VALUE:6
- BINARY_VALUE:20
- BINARY_VALUE:23
- BINARY_VALUE:24
- BINARY_VALUE:25
- BINARY_VALUE:26
- BINARY_VALUE:37
- BINARY_VALUE:50
- TU-1-21-LOCAL-CAL
- CBAS Alarm (1)
- EVENT_ENROLLMENT:1002
- EVENT_ENROLLMENT:1003
- LOOP:1
- LOOP:2
- MULTI_STATE_OUTPUT:7
- NOTIFICATION_CLASS:0
- NOTIFICATION_CLASS:1
- NOTIFICATION_CLASS:63

Device	ObjectId	Name	Value	Time	Status
[redacted] 6...	OBJECT_BINARY_INPUT:8	DI3 ACT	0	23:36:30	OK
[redacted] 6...	OBJECT_ANALOG_VALU...	DC B...	706	23:36:34	OK

Bacnet Property	
1088 - Proprietary	False
1089 - Proprietary	False
Date List	
Description	
Object Identifier	OBJECT_CALENDAR:1
Object Name	TU-1-21-LOCAL-CAL
Object Type	6 : Object Calendar
	False

December, 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: 2016-12-05

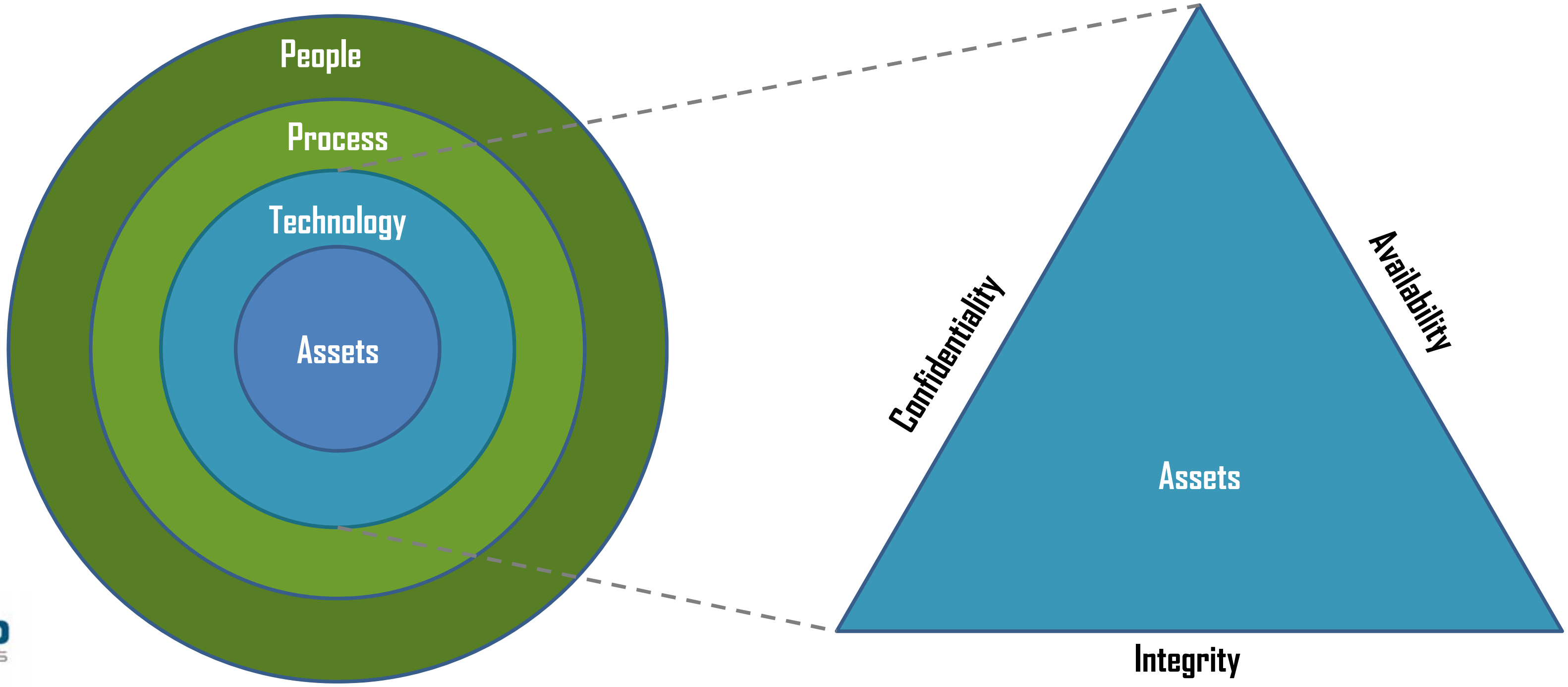
Dates entries :

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
27 - 11 -	27 Nov	28	29	30	01 Dec	2	3
4 - 10 - 1	4	5	6	7	8	9	10
11 - 17 -	11	12	13	14	15	16	17
18 - 24 -	18	19	20	21	22	23	24
25 - 31 -	25	26	27	28	29	30	31

No one would know

Basics of cybersecurity

Basics of cybersecurity



Resources

NIST Cybersecurity Framework

SANS Institute: Training and Research

ISA/IEC-62443:
Standard for securing IACS

ICS-CERT:
US DHS Alerts, training and assessments

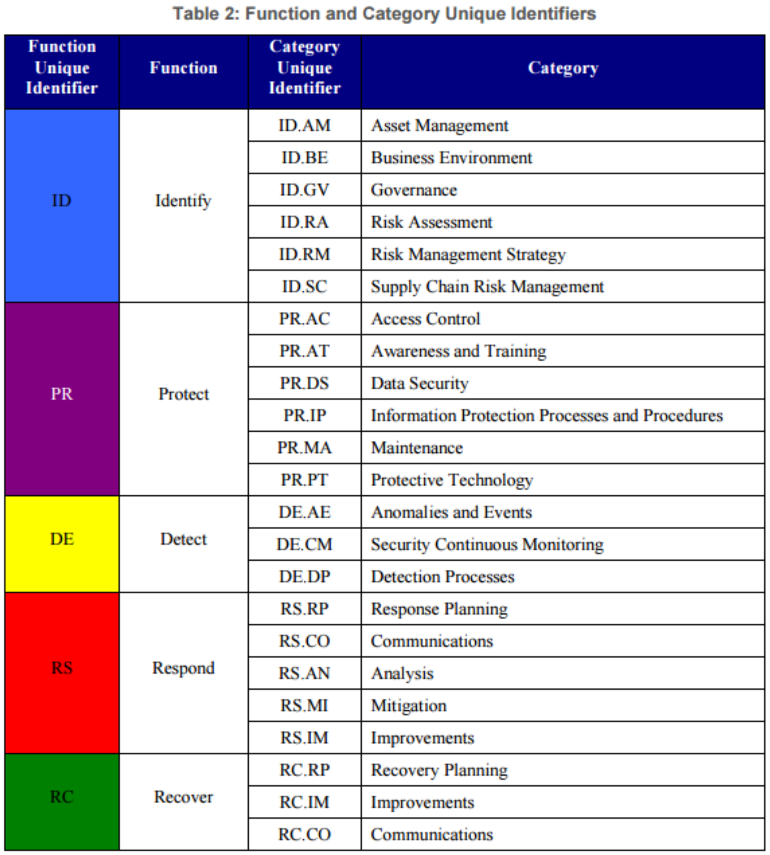


Table 2: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

https://www.nist.gov/sites/default/files/documents/2017/01/17/draft-cybersecurity-framework-v1.1.pdf - page 30

Secure building networks

Protecting B-IoT by securing the network

Why the network? Because…

- Common to all systems
- Everything* goes through it
- Scalable
- IoT communications is predictable

OPTiGO NETWORKS

Three key principles to secure building networks

1) Isolation

- Dedicated networks
- VLAN
- VRF
- Firewall
- …

2) Observability

- Reports
- Logs
- Notifications
- Monitoring
- …

3) Controllability

- Port control
- Port security
- ACL
- …

Take action today

1) **Isolate your Building Systems from IT**
   - Dedicated Building Network
   - Separate VLAN for each service and vendor

2) **Observe what is happening**
   - Ask for regular reports of # of connected devices and # of disconnected ports
   - Review network management log files for user login

3) **Control the flow of information**
   - Disable unused ports
   - Set MAC filtering/security rules

Conclusion

- Cybersecurity is serious and needs to be addressed.
- Protect the network, protect the system.
- Start today.
- Q&A

Pook-Ping Yao
CEO, Optigo Networks Inc.
ping@optigo.net