

Covering your BAS

Simple Steps to Address Cyber Security Concerns in Your BAS Installations

Pook-Ping Yao, CEO
Optigo Networks Inc.



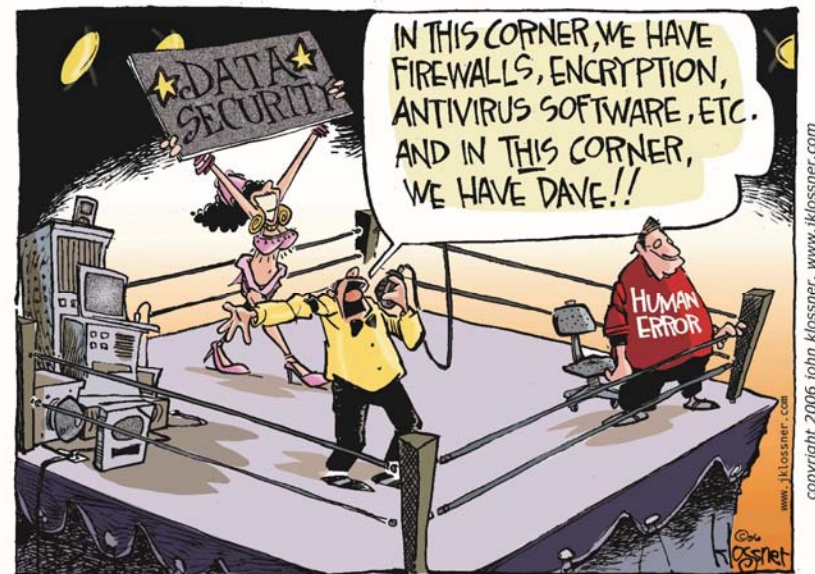
2017 BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Objective

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



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Agenda

- Why Cybersecurity Matters
- “Demo”
- Basics of Cybersecurity
- Secure Building Networks
- Conclusion



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



WHY CYBERSECURITY MATTERS



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



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>



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL

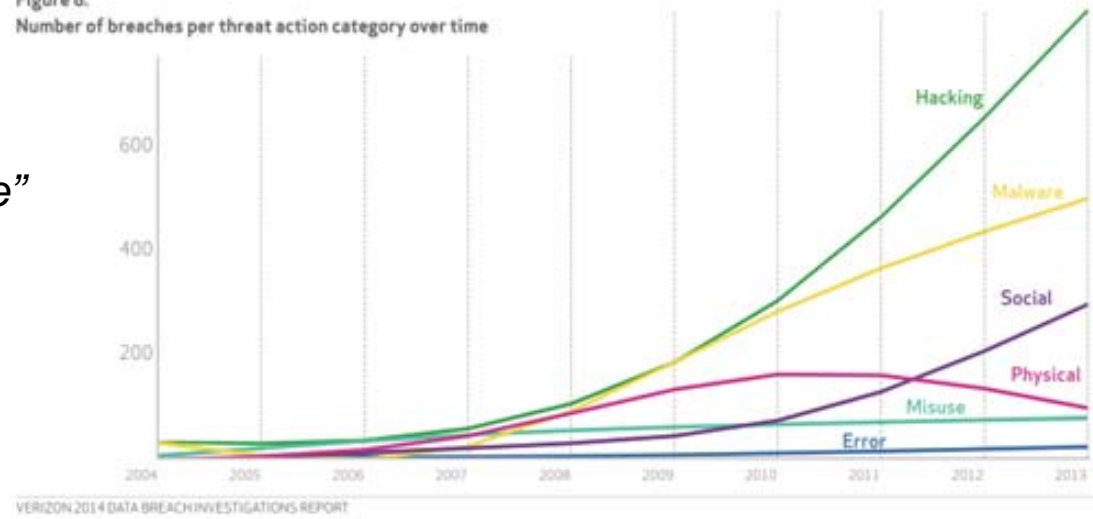


“IBM's X-Force team hacks into smart building”
– CSO Online

*“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



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



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Smart Buildings

A Back Door for Hackers?

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



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



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



DEMO



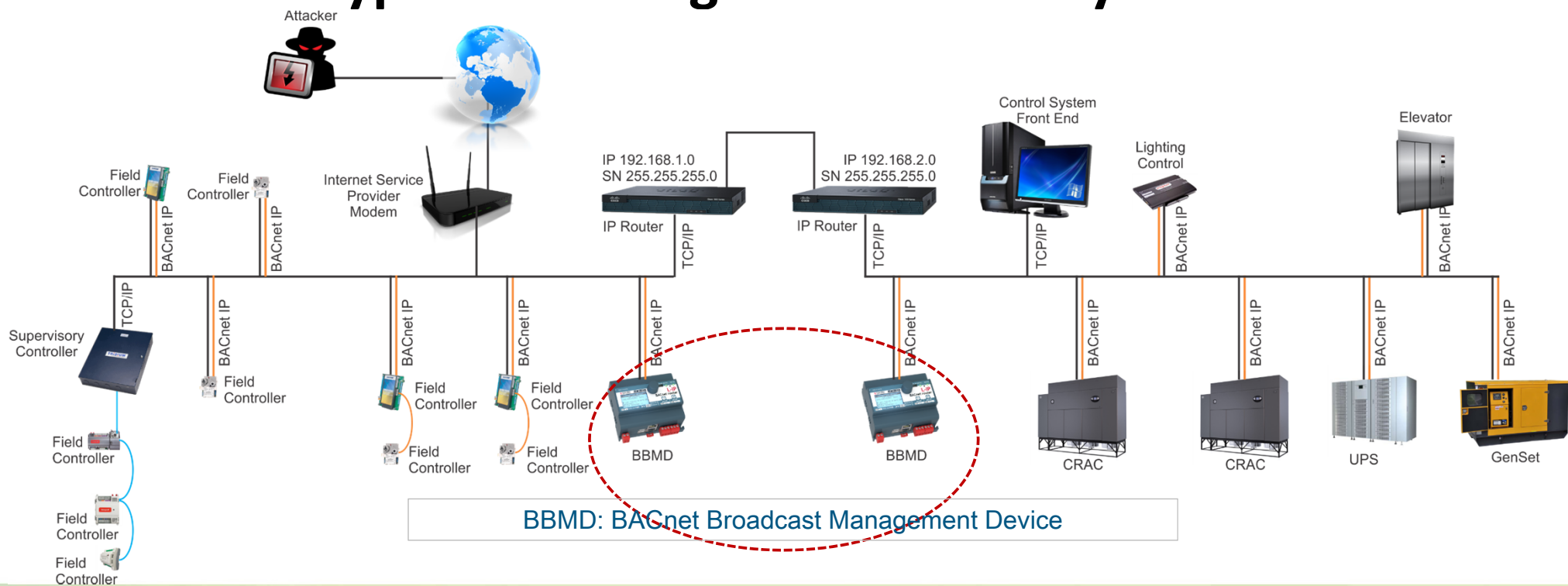
2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Typical Building Automation Systems



2017


BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



bbmd Search x
 https://www. search?query=bbmd&page=2

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

1250.90
 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:
 Application Software: 3.7.108
 Firmware: 3.7.108.3
 Model Name:
 Description: Local BACnet Device object
 BACnet Broadcast Management Device (BBMD):
 192.168.0.121:47808

102.4
 University
 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:
 Application Software: BCE1201
 Firmware: BACnet 4.3g
 Model Name: BACnet Field Panel
 Description: UWLU.A.MEC.01
 BACnet Broadcast Management Device (BBMD):
 140.142....

22.114
 static-114-22-4-96.tulahoma.in.ena.net
 State Library
 Added on 2016-12-03 23:56:54 GMT
 United States, Tullahoma
Details
 ICS

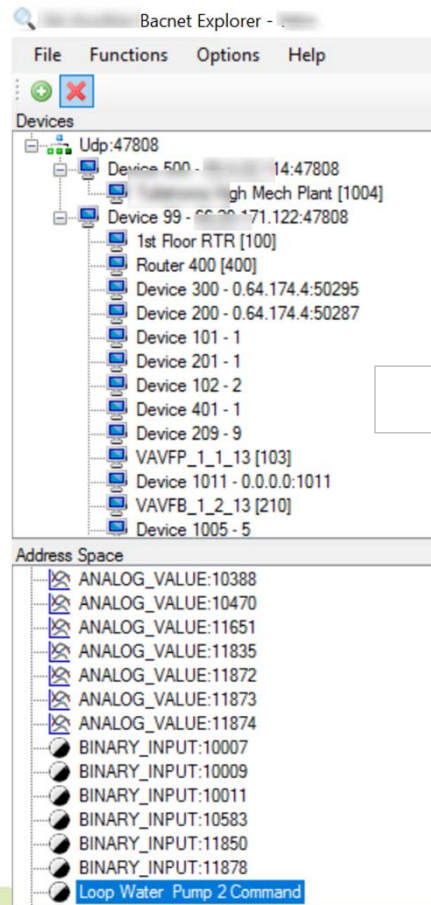
Instance ID: 500
 Object Name: THS-NAE
 Vendor Name:
 Firmware: 6.0.0.9000
 Model Name: MS-NCE2566-0

~1500 exposed BACnet systems in one search in the USA



2017
BICSI Winter Conference & Exhibition
 January 22-26 • Tampa, FL





No Login



2017
BICSI Winter Conference & Exhibition
January 22-26 • Tampa, FL



The screenshot displays the Bacnet Explorer interface. On the left, the 'Devices' tree shows a hierarchy starting with 'Udp:47808' and 'High Mech Plant [1004]'. Below it, the 'Address Space' lists various BACnet objects, with 'Loop Water Pump 2 Command' selected. The central pane shows a table for 'Subscriptions, Periodic Polling, Events/Alarms' with columns for Device, ObjectId, Name, Value, Time, and Status. A text box is overlaid on this pane with the text 'Remote Control of Building Automation Devices'. On the right, the 'Properties' pane shows details for the selected object, including its name 'Loop Water Pump 2 Command' and various proprietary values.

**Remote Control of
Building Automation
Devices**

Device	ObjectId	Name	Value	Time	Status
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		



2017
BICSI Winter Conference & Exhibition
 January 22-26 • Tampa, FL



The screenshot shows the Bacnet Explorer interface. On the left, there is a 'Devices' list and an 'Address Space' list. The main window displays a table of subscriptions with columns for Device, ObjectId, Name, Value, Time, and Status. A 'Calendar Editor' window is open in the foreground, showing a calendar for December 2016. The date December 5th is highlighted in orange. To the right of the calendar editor, there is a text box containing the text 'No one would know'. The 'Properties' pane on the right shows details for a 'BacnetProperty' object, including its name and value.

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

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
27 Nov	28	29	30	01 Dec	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



2017
BICSI Winter Conference & Exhibition
 January 22-26 • Tampa, FL



BASICS OF CYBERSECURITY



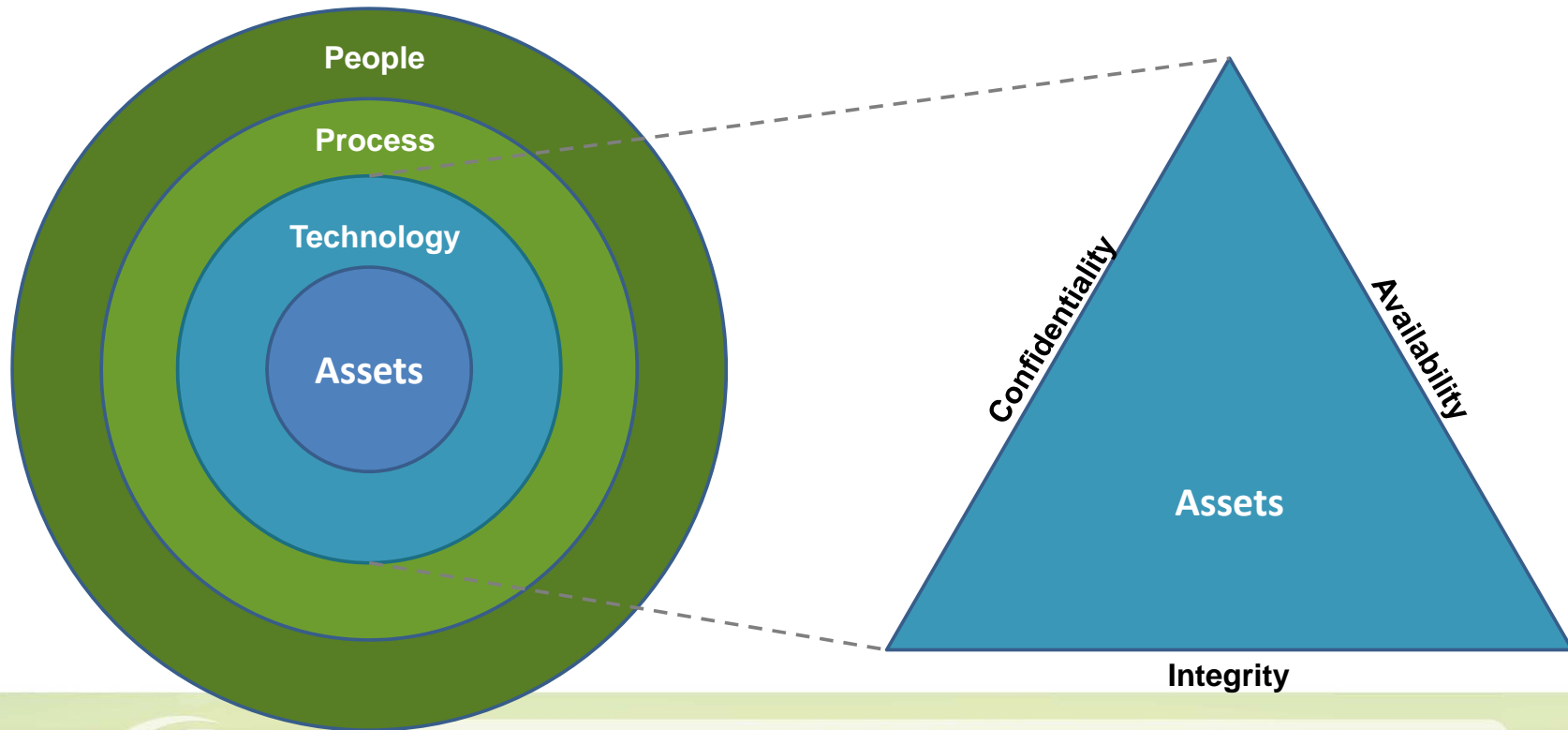
2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Basics of Cybersecurity



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



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

Resources

NIST Cybersecurity Framework

SANS Institute: Training and Research

ISA/IEC-62443:

Standard for securing IACS

ICS-CERT:

US DHS Alerts, training and assessments

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



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



SECURE BUILDING NETWORKS



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Protecting B-IoT by Securing the Network



Why the network? Because...

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



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



3 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
- ...



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



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



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL



Conclusion

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

Pook-Ping Yao

CEO, Optigo Networks Inc.
ping@optigo.net



2017

BICSI Winter Conference & Exhibition

January 22-26 • Tampa, FL

