Internet2 IoT Systems Risk Management Task Force 2016-2017 Outcomes

Internet2 IoT Systems Risk Management Task Force 2016-2017 Outcomes

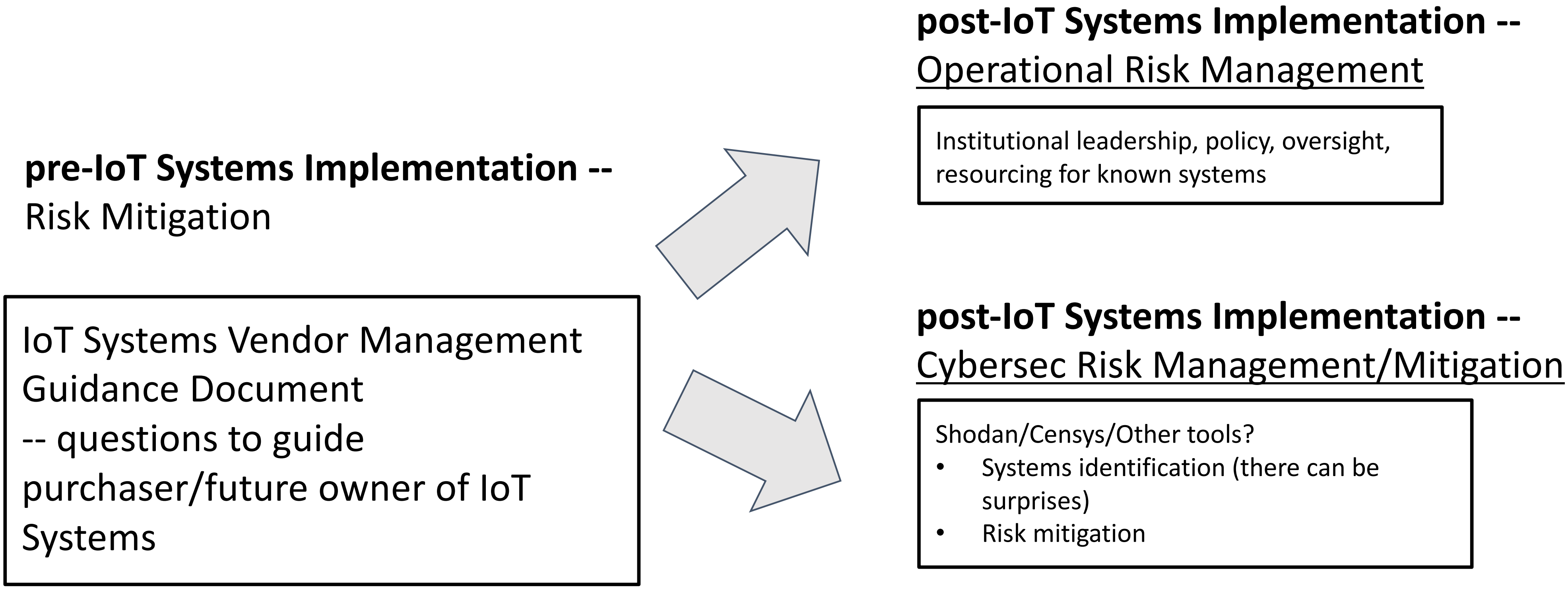
- Explore notion of ***a lifecycle of IoT Systems risk & operational management*** in Higher Ed institutions

- **Develop 2 tools/practices as starting place**:
  - HE practice of using Shodan and Censys tools to develop IoT Systems risk exposure for an HE institution
  - IoT Systems Vendor Management document/checklist to guide multiple departments/orgs within an HE institution on selection, procurement, management of IoT Systems

- Identify potential for future work

- Identify & share other resources

Developing an IoT Systems Risk Mitigation Life Cycle



pre-IoT Systems Implementation --
Risk Mitigation

IoT Systems Vendor Management Guidance Document
-- questions to guide purchaser/future owner of IoT Systems

post-IoT Systems Implementation --
Operational Risk Management

Institutional leadership, policy, oversight, resourcing for known systems

post-IoT Systems Implementation --
Cybersec Risk Management/Mitigation

Shodan/Censys/Other tools?

- Systems identification (there can be surprises)
- Risk mitigation

Jan Cheetham
Research Cyberinfrastructure Liaison
Office of the CIO
University of Wisconsin-Madison

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

IoT research initiatives

Internet of Things
SYSTEMS RESEARCH CENTER
UNIVERSITY OF WISCONSIN–MADISON

WiNEST
Template for a model wireless city

CloudLab

IoT Vulnerabilities: DDoS attacks

Mirai, BASHLITE, and evolving malware

OVH	krebsonsecurity.com	ORACLE + Dyn	
9/18/16 1.1 Tbps	9/20/16 620 Gbps	10/21/16 1.2 Tbps	Un-named US University Late 2016

DVRs, CCTV cameras, home routers

Campus vending machines, light sensors, refrigerators

IoT Vulnerabilities: Industrial control systems

2008
Turkish oil pipeline

BBC News

2014
German blast furnace

Industrial Control & Critical Infrastructure in Higher Ed

Utility distribution

Building/Room environment control (HVAC)

We also care about these:

Research Systems

Building, Internal Space, Animal Facility, BSL3 Access

And others …

Taskforce benchmarking activity

SHODAN

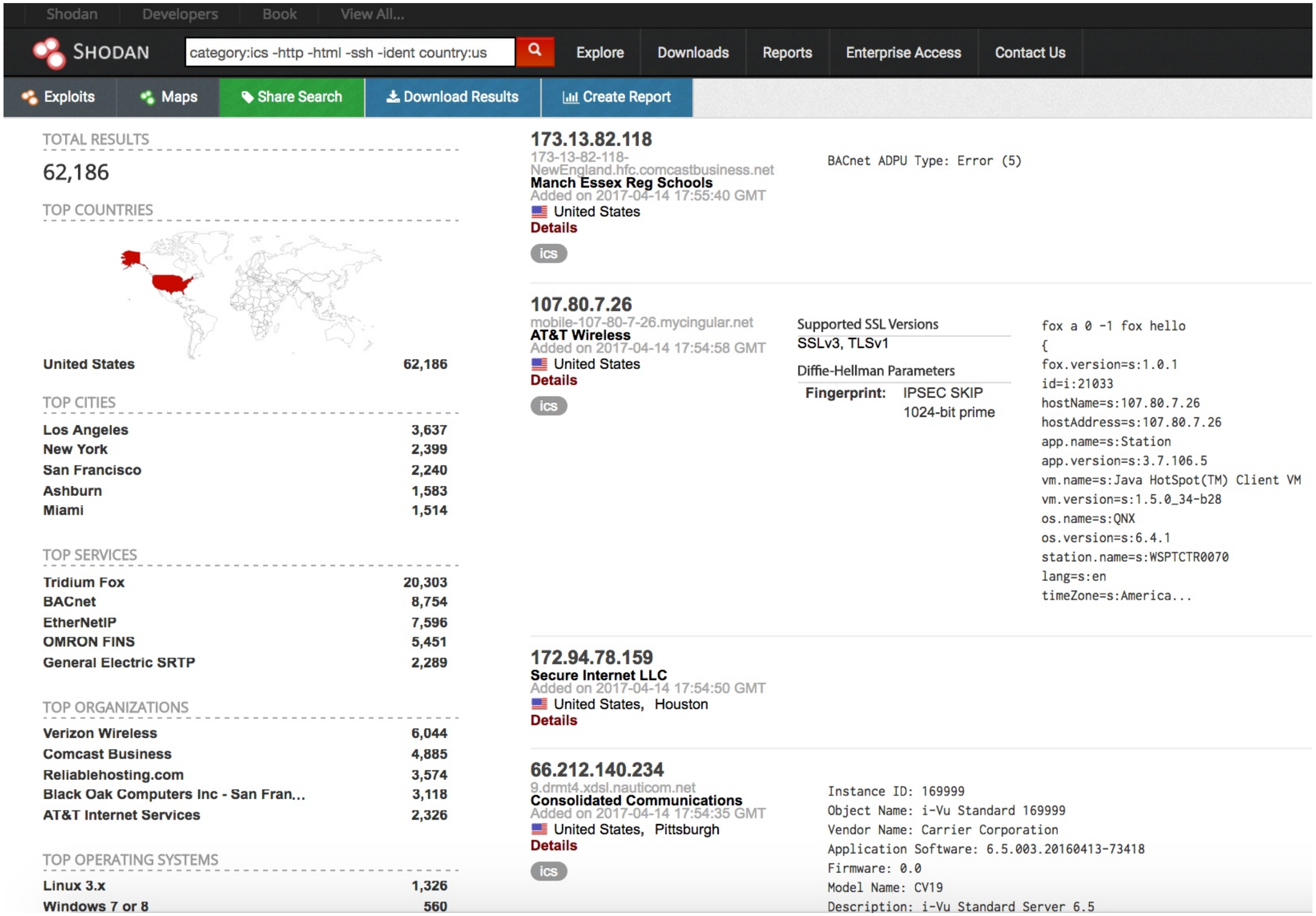
- Proprietary
- Developed by former Mesa Community College student
- Used by private sector and academia
- Shawn Merdinger, Valdosta State presentation at Educause 2014

censys

- Open source
- Developed at Univ of Michigan/Illinois
- Daily ZMap and ZGrab scans of IPv4 address space across important ports and protocols

Both do full text searching on protocol banners and other metadata on websites, servers, devices

WARNING: Consult your CISO office before using! Prior notice and authorization may be required.



TOTAL RESULTS

62,186

TOP COUNTRIES

United States	62,186

TOP CITIES

Los Angeles	3,637
New York	2,399
San Francisco	2,240
Ashburn	1,583
Miami	1,514

TOP SERVICES

Tridium Fox	20,303
BACnet	8,754
EtherNetIP	7,596
OMRON FINS	5,451
General Electric SRTP	2,289

TOP ORGANIZATIONS

Verizon Wireless	6,044
Comcast Business	4,885
Reliablehosting.com	3,574
Black Oak Computers Inc - San Fran...	3,118
AT&T Internet Services	2,326

TOP OPERATING SYSTEMS

Linux 3.x	1,326
Windows 7 or 8	560

173.13.82.118
173-13-82-118-NewEngland.hfc.comcastbusiness.net
Manch Essex Reg Schools
Added on 2017-04-14 17:55:40 GMT
United States
Details
ics

```
BACnet ADPU Type: Error (5)
```

107.80.7.26
mobile-107-80-7-26.mycingular.net
AT&T Wireless
Added on 2017-04-14 17:54:58 GMT
United States
Details
ics

Supported SSL Versions
SSLv3, TLSv1

Diffie-Hellman Parameters

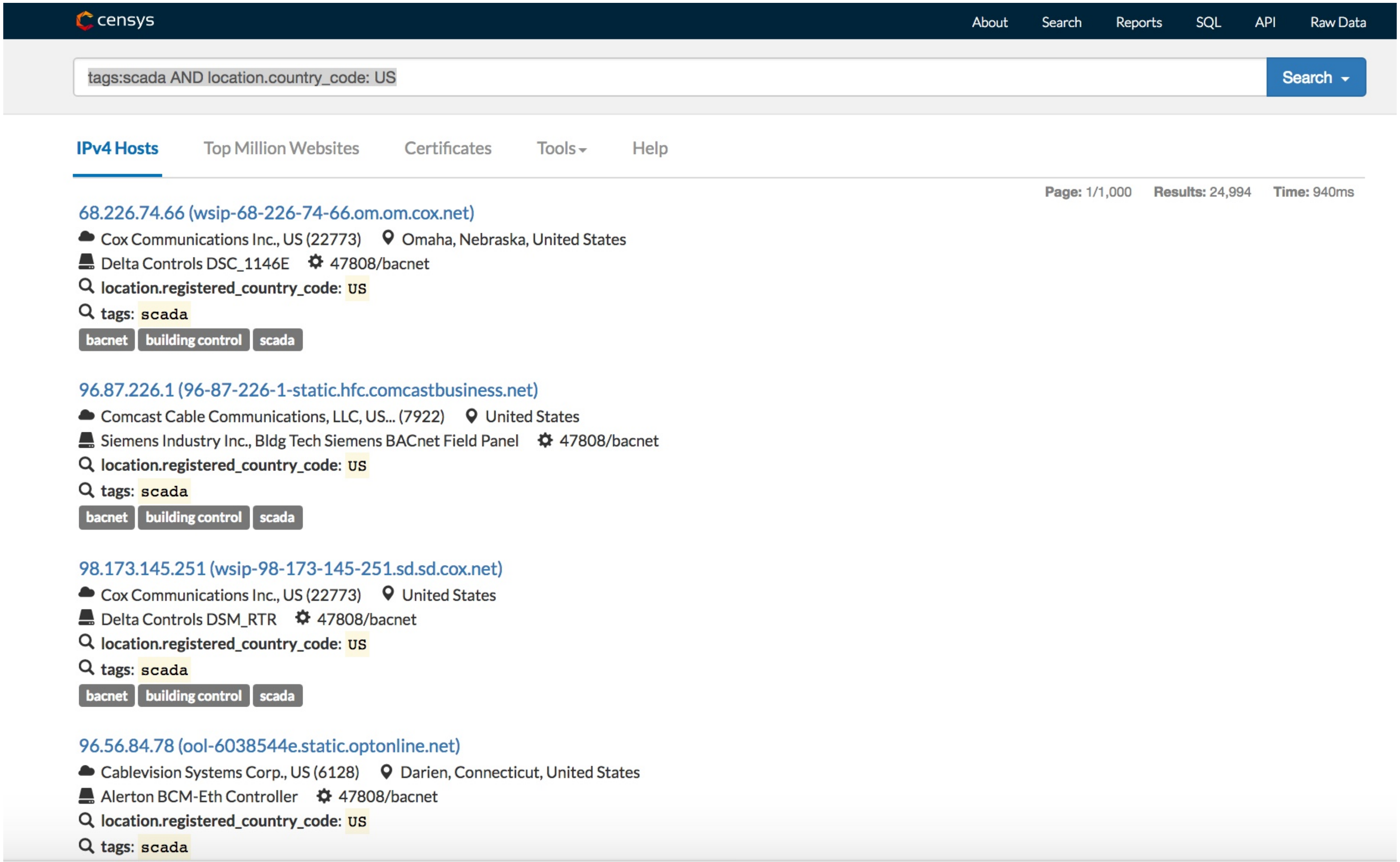
Fingerprint:	IPSEC SKIP 1024-bit prime

```
fox a 0 -1 fox hello
{
fox.version=s:1.0.1
id=i:21033
hostName=s:107.80.7.26
hostAddress=s:107.80.7.26
app.name=s:Station
app.version=s:3.7.106.5
vm.name=s:Java HotSpot(TM) Client VM
vm.version=s:1.5.0_34-b28
os.name=s:QNX
os.version=s:6.4.1
station.name=s:WSPTCTR0070
lang=s:en
timeZone=s:America...
```

172.94.78.159
Secure Internet LLC
Added on 2017-04-14 17:54:50 GMT
United States, Houston
Details

66.212.140.234
9.drmt4.xdsl.nauticom.net
Consolidated Communications
Added on 2017-04-14 17:54:35 GMT
United States, Pittsburgh
Details
ics

```
Instance ID: 169999
Object Name: i-Vu Standard 169999
Vendor Name: Carrier Corporation
Application Software: 6.5.003.20160413-73418
Firmware: 0.0
Model Name: CV19
Description: i-Vu Standard Server 6.5
```



tags:scada AND location.country_code: US

Page: 1/1,000 **Results:** 24,994 **Time:** 940ms

68.226.74.66 (wsip-68-226-74-66.om.om.cox.net)

Cox Communications Inc., US (22773) Omaha, Nebraska, United States
Delta Controls DSC_1146E 47808/bacnet
location.registered_country_code: US
tags: scada
bacnet building control scada

96.87.226.1 (96-87-226-1-static.hfc.comcastbusiness.net)

Comcast Cable Communications, LLC, US... (7922) United States
Siemens Industry Inc., Bldg Tech Siemens BACnet Field Panel 47808/bacnet
location.registered_country_code: US
tags: scada
bacnet building control scada

98.173.145.251 (wsip-98-173-145-251.sd.sd.cox.net)

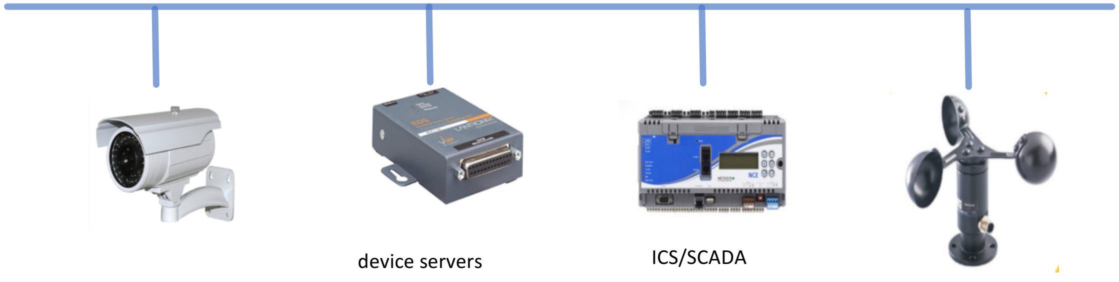
Cox Communications Inc., US (22773) United States
Delta Controls DSM_RTR 47808/bacnet
location.registered_country_code: US
tags: scada
bacnet building control scada

96.56.84.78 (ool-6038544e.static.optonline.net)

Cablevision Systems Corp., US (6128) Darien, Connecticut, United States
Alerton BCM-Eth Controller 47808/bacnet
location.registered_country_code: US
tags: scada

What we found

Cameras Building Automation Sensors



Search terms	”camera”	”scada,” “ICS,” “HVAC,” “Tridium Fox,” “BACnet,” “Modbus”	”AMQP” “RabbitMQ” “MQTT”
Potential Risk	Weak, hard-coded passwords	Components of building control systems exposed on Internet, protocols lacking authentication, encryption	Complex, layered systems with physical security issues, protocols lacking authentication

May be others

Other types of devices we didn't search for

- Vending machines
- Refrigerators
- Health care monitors

Image sources: MegaLab, AlerSense, UAI Vending

Brief background

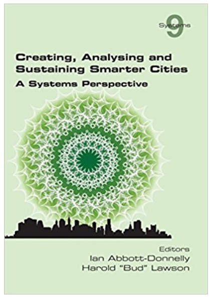
Chuck Benson

Facilities Services IT, UW
Drone policy working group, UW
Chair Internet2 IoT Systems Risk Management Task Force
Former Chair UW-IT Service Management Board, UW
Former Chair Protection of Industrial Controls (PICS) Task Force

Chair Internet2 IoT Systems Risk Management Task Force

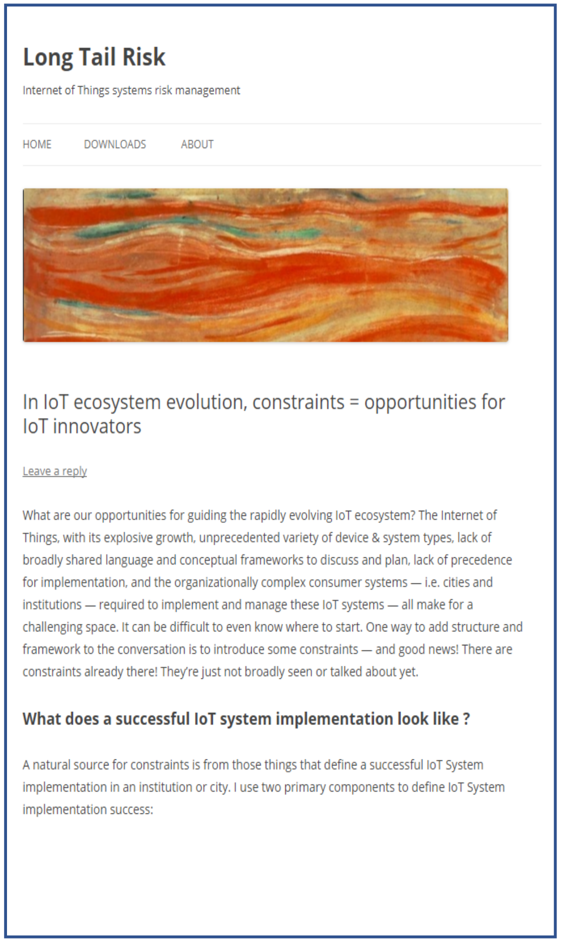
Articles June & July 2016 –

“Internet of Things, IoT Systems, and Higher Education” &
“Raising Expectations for IoT Systems Vendors”



Book Chapter in book, “Creating, Analysing, and Sustaining Smarter Cities – A Systems Perspective”

Chapter Title: “IoT Systems – Systems Seams & Systems Socialization”



Long Tail Risk

Internet of Things systems risk management

In IoT ecosystem evolution, constraints = opportunities for IoT innovators

Leave a reply

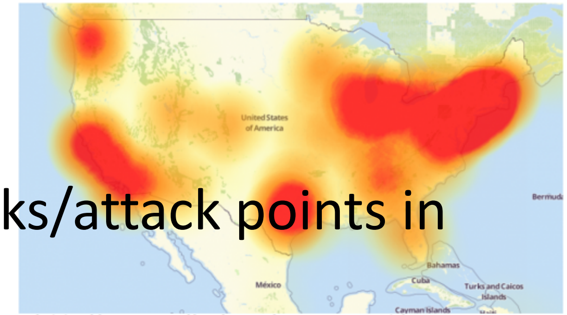
What are our opportunities for guiding the rapidly evolving IoT ecosystem? The Internet of Things, with its explosive growth, unprecedented variety of device & system types, lack of broadly shared language and conceptual frameworks to discuss and plan, lack of precedence for implementation, and the organizationally complex consumer systems — i.e. cities and institutions — required to implement and manage these IoT systems — all make for a challenging space. It can be difficult to even know where to start. One way to add structure and framework to the conversation is to introduce some constraints — and good news! There are constraints already there! They're just not broadly seen or talked about yet.

What does a successful IoT system implementation look like ?

A natural source for constraints is from those things that define a successful IoT System implementation in an institution or city. I use two primary components to define IoT System implementation success:

(and the obligatory twitter feed -- @cabenson361)

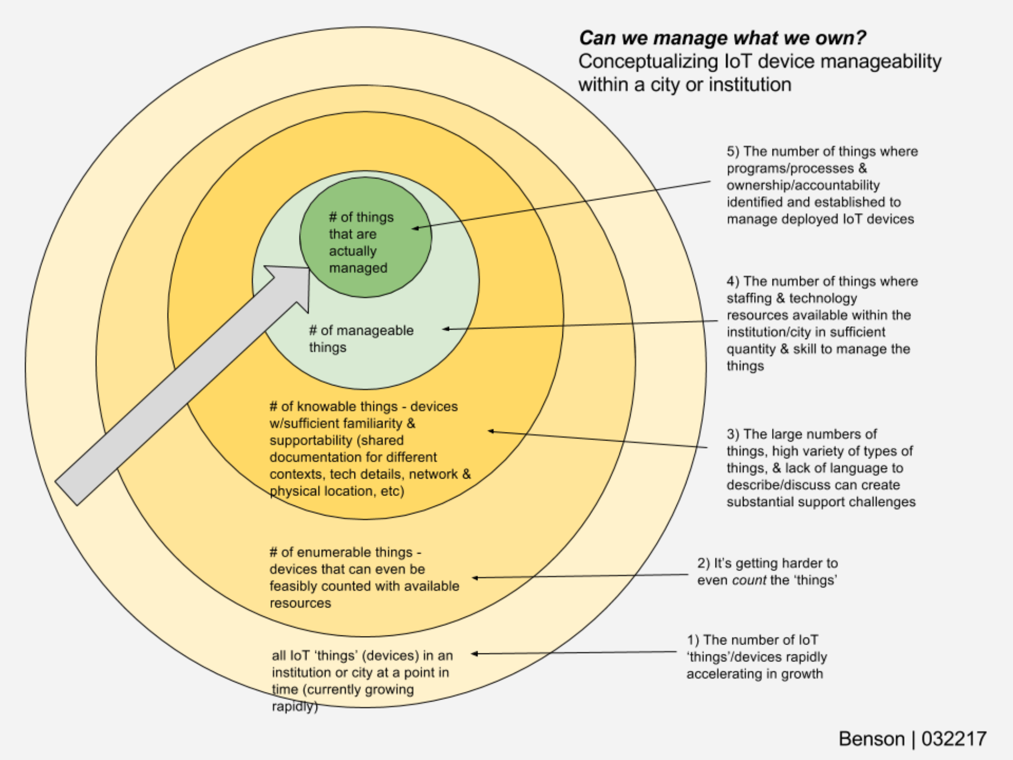
IoT Systems Vendor Management Document



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

- Shodan, Censys, and non-published tools reveal cracks/attack points in our institutions
  - Creating potentially substantial additional risk
- We can lower that risk
  - By raising the bar & setting expectations of the IoT Systems vendor
  - RFI, RFP, contract negotiation, & relationship management phases with the vendor

Can we manage what we own?



Can we manage what we own?
Conceptualizing IoT device manageability within a city or institution

# of things that are actually managed
# of manageable things
# of knowable things - devices w/sufficient familiarity & supportability (shared documentation for different contexts, tech details, network & physical location, etc)
# of enumerable things - devices that can even be feasibly counted with available resources
all IoT 'things' (devices) in an institution or city at a point in time (currently growing rapidly)

5) The number of things where programs/processes & ownership/accountability identified and established to manage deployed IoT devices

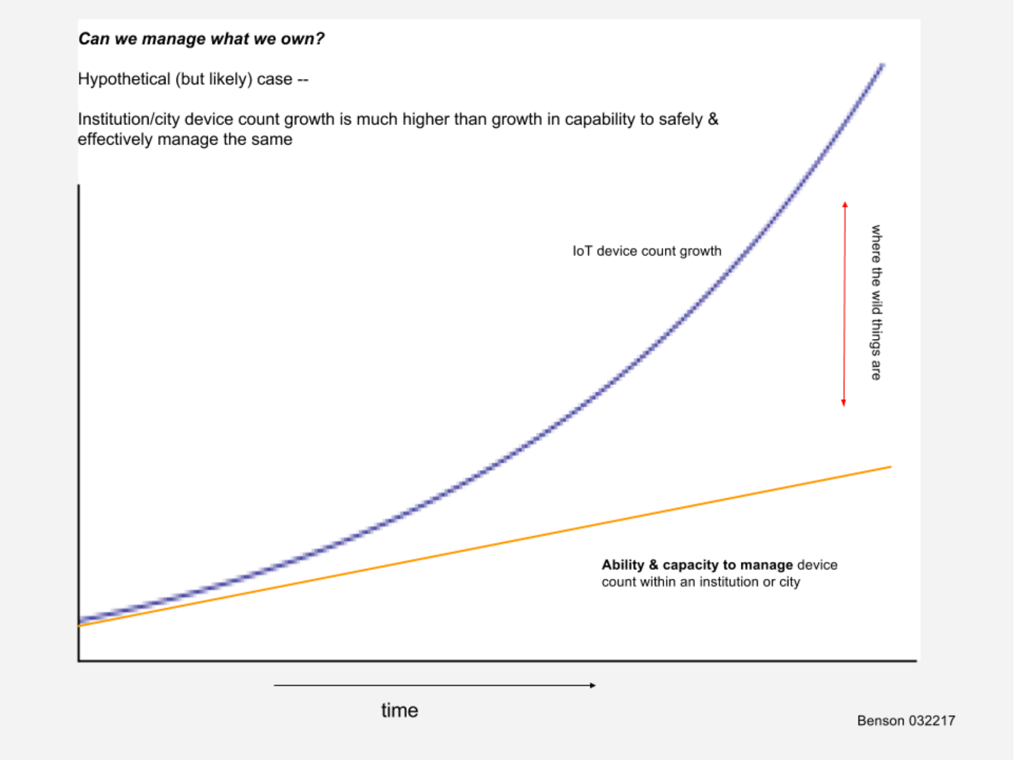
4) The number of things where staffing & technology resources available within the institution/city in sufficient quantity & skill to manage the things

3) The large numbers of things, high variety of types of things, & lack of language to describe/discuss can create substantial support challenges

2) It's getting harder to even *count* the 'things'

1) The number of IoT 'things'/devices rapidly accelerating in growth

Benson | 032217



Can we manage what we own?

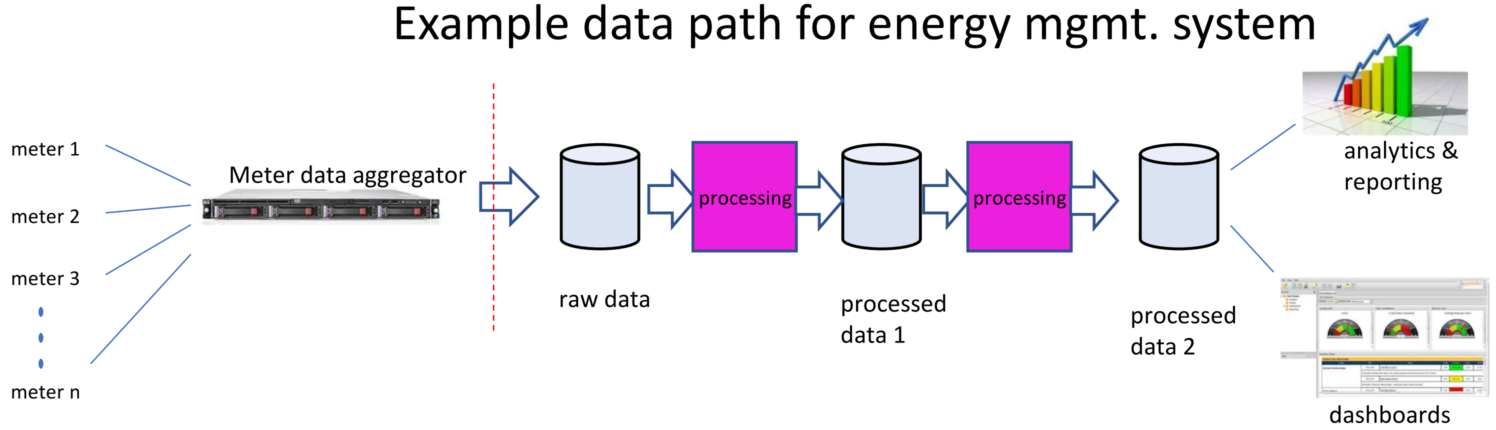
Hypothetical (but likely) case --

Institution/city device count growth is much higher than growth in capability to safely & effectively manage the same

Benson 032217

And the IoT System is deployed in a system of human & technical systems …

Example data path for energy mgmt. system



meter 1

meter 2

meter 3

meter n

Meter data aggregator

raw data

processing

processed data 1

processing

processed data 2

analytics & reporting

dashboards

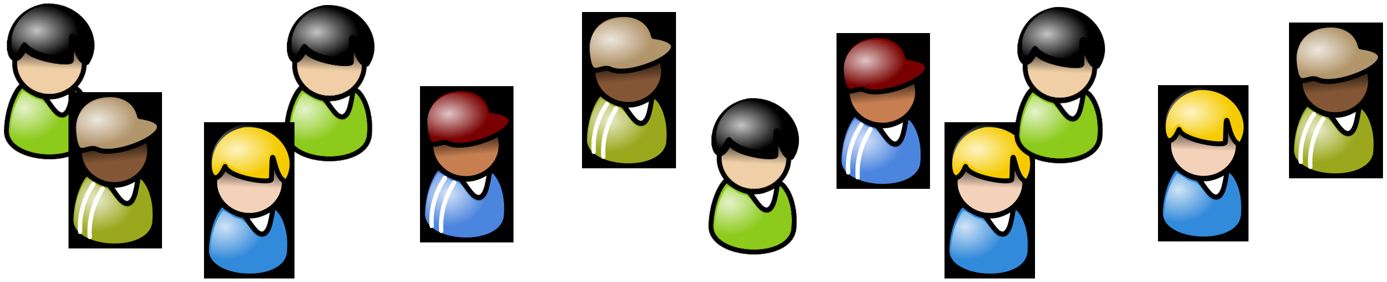
Technical infrastructure

Existing IT/Info Mgmt Infrastructure (eg physical network & physical implementation points)

Organizational structure

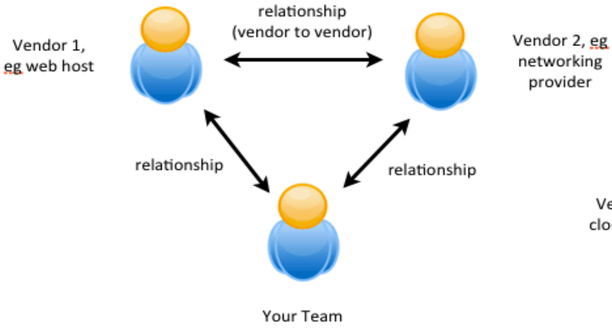
Central IT | Distributed IT | Facilities Mgmt | Institution Leadership | Acad/Admin Dept 1 | Acad/Admin Dept n | Vendor 1 | Vendor n

People – with roles, expectations, patterns, routines, opinions



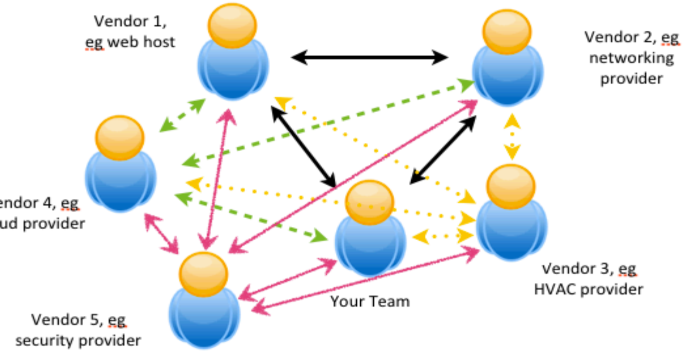
Increasing vendor/system count increases systems complexity & management overhead

the old days
-- smaller number of providers --



# of endpoints	potential # of relationships requiring management
3	3
...	...

the new world
-- IoT innovation & growth increases vendor count & relationships requiring management --



# of endpoints	potential # of relationships requiring management
3	3
4	6
5	10
6	15
7	21
...	...

Note: addition of a *single* endpoint later in the series creates *many* more relationships to be managed. This is the part that can sneak up on us. (Same reason why growing committee size gets unwieldy).

ChuckBenson@longtailrisk.com | 051415

Vendor management complexity grows rapidly with #IoT systems @cabenson361 #risk #i2summit17

IoT Systems Vendor Management Document

- Acknowledge that:
  - IoT Systems increasingly ***entering institution in non-traditional ways***
    - Eg not central IT – but end-users/PI’s, facilities, capital planning, planning/budgeting
  - IoT Systems are ***deployed in non-traditional ways***
    - These are not traditional enterprise systems
    - Often not with central IT
    - Often with vendor-heavy influence
  - Generally, ***limited vetting for IoT Systems***
    - Many, most? of these systems will not be managed by central IT

- IoT Systems Vendor Management Doc
  - Designed to assist:
    - selection
    - RFI
    - RFP
    - contraction negotiation
    - systems management

  - Doc needs broad utility & consumability -- Needs to be readable or ‘parseable’ by organizations fulfilling multiple different roles – not just IT

Snippet from document cover –

Purpose of Document
This document is intended to provide different organizations within Higher Education institutions with items to consider as they engage with IoT Systems vendors at the different phases of selection, procurement, deployment, and management. For example, …

It is acknowledged that IoT Systems are selected, acquired and deployed by Higher Education Institutions through multiple paths. Systems may arrive through PI's …

The more historical acquisition approach of selection, acquisition, deployment, and management of traditional enterprise IT systems through central IT is not sufficient for doing the same with IoT Systems. … while IoT Systems will likely use IT infrastructure, … it is very likely that central IT will not have the resources or expertise to support the wide-ranging performance aspects required of the IoT System.

IoT Systems are unique in that they span many organizations, … ***They are also unique in that they affect many types of risk within an institution*** to include financial, reputation, operational, safety and other types of risk.

For each of the statements or questions below for use in managing vendor relationships, ***two additional columns are provided: one for type(s) of risk involved and one for example organizations on campus*** ... In both cases – risk type and organization -- it is acknowledged that there can be overlap between types. For example, financial risk can also affect reputation risk. (Almost everything affects an institution's reputation risk). ***The risk item or the organization indicated are primarily intended to be used as examples and potential talking, negotiating, and management points.***

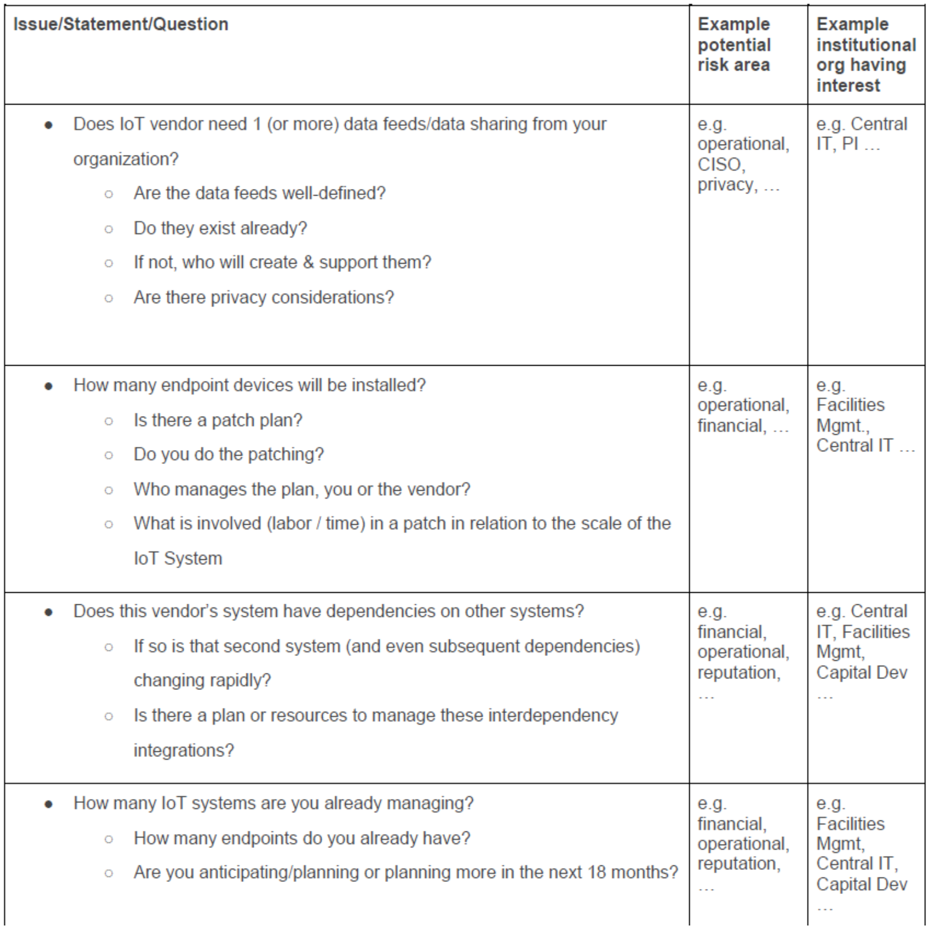
Snippet from document cover –

Example Higher Ed institutional organizations having interest include:
- Principal Investigator (PI) & lab staff
- Planning/budgeting office
- Capital development
- Facilities management
- Police department
- Central IT
- Distributed IT groups
- Risk, compliance, CISO, & privacy offices

Example Higher Ed risk areas include:
- Privacy
- Financial
- Operational
- Reputation
- Compliance
- Safety
- Cybersecurity

Both lists are not exhaustive and both lists have items that have interdependency on other items. The intention is to consider them in planning, talking, negotiation, and vendor management activities and to inform and elevate the conversation.

Snippet from document --



Issue/Statement/Question	Example potential risk area	Example institutional org having interest
- Does IoT vendor need 1 (or more) data feeds/data sharing from your organization? ○ Are the data feeds well-defined? ○ Do they exist already? ○ If not, who will create & support them? ○ Are there privacy considerations?	e.g. operational, CISO, privacy, …	e.g. Central IT, PI …
- How many endpoint devices will be installed? ○ Is there a patch plan? ○ Do you do the patching? ○ Who manages the plan, you or the vendor? ○ What is involved (labor / time) in a patch in relation to the scale of the IoT System	e.g. operational, financial, …	e.g. Facilities Mgmt., Central IT …
- Does this vendor's system have dependencies on other systems? ○ If so is that second system (and even subsequent dependencies) changing rapidly? ○ Is there a plan or resources to manage these interdependency integrations?	e.g. financial, operational, reputation, …	e.g. Central IT, Facilities Mgmt, Capital Dev …
- How many IoT systems are you already managing? ○ How many endpoints do you already have? ○ Are you anticipating/planning or planning more in the next 18 months?	e.g. financial, operational, reputation, …	e.g. Facilities Mgmt, Central IT, Capital Dev …

IoT Systems Vendor Management Document

-- example items --

operational risks (eg resourcing & planning)

- □ Does vendor need 1 (or more) data feeds/data sharing from your organization?
  - □ Are the data feeds well-defined?
  - □ Do they exist already?
    - □ If not, who will create & support them

- □ Who pays for vendor systems requirements (eg hardware, supporting software, networking, etc?)
  - □ Does local support (FTE) exist? Is it available? Will it remain available?
  - □ If hosted in a data center, who pays for those costs?
  - □ If cloud-hosted, eg AWS, who pays for those costs?
  - □ Above questions answered for both implementation & long term support?

- □ What is total operational cost after installation?
  - □ Licensing
  - □ Support contracts
  - □ Hosting requirements
  - □ Business resilience requirements (eg redundancy, recovery, etc for OS, db, other)

- □ Can IoT system vendor maintenance contract offset local IT support shortages?
  - □ for 10’s, 100’s, 1000’s of new endpoints ?

cybersec (bad guy) risks

- □ Is there a commissioning plan? Or have installation expectations otherwise been stated?
  - □ Default logins & passwords changed & recorded?
  - □ Non-required default ports closed?
  - □ Devices port scanned (or similar) after installation

- □ For remote support, how does vendor safeguard login/account information?
  - □ Is it in contract?

- □ Who, in your organization, will manage the IoT system vendor contract?
  - □ Central IT?
  - □ Facilities?
  - □ Tenant/customer dept ?
  - □ Other? PD/security? CISO? CSO?

both

- □ How many endpoint devices will be installed?
  - □Is there a patch plan? Who manages this?

- □ How many IoT systems are you already managing?
  - □ Are you anticipating more in next 18 months?

- □ Is the IoT vendor system implementation documented?
  - □ Architecture diagram ?
    - □ w/IP addresses & physical location of devices?
    - □ w/required ports documented

- □ Does this vendor’s system have dependencies on other systems?

- □ Is a risk sharing agreement in place for shared institutional information?

Internet2/ITANA IoT Working Group

Two resources that will be available early 2018:

- Campus Briefing document

  Memo for high level campus stakeholders to raise awareness of IoT opportunities and risks

- Enterprise Lifecycle IoT Management checklist

  Staged inventory of risks/issues to be considered in the acquisition and management of campus IoT systems

Many other resources (some longer to read than others)

- NIST Cybersecurity for IoT Program
  - https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
- FTC & IoT Privacy
  - https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
- Industrial Internet of Things Security Framework
  - http://www.iiconsortium.org/IISF.htm
- GSMA IoT Security Guidelines
  - http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
- OWASP IoT Security Guidance
  - https://www.owasp.org/index.php/IoT_Security_Guidance
- DHS Strategic Principles for Securing the Internet of Things
  - https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
- Shodan for the .Edu
  - http://www.educause.edu/sites/default/files/library/presentations/SEC14/SESS08/shodan_for_edu_educause_security_conference_2014_public_version_shawn_merdinger.pdf

Possible future work in area

- IoT Systems Costing
  - Few, if any, institutions have a handle on this
- Network segment portfolio strategies
  - Segmentation is all the rage, but how are those segmentation portfolios managed
- Internal ICS & IoT exposure
  - Shodan/Censys do public addresses
    - Internal VLAN’s, VRF’s, etc not covered
- Benchmark/standard for exposure in HE

Questions/Comments?