Pacific Northwest
NATIONAL LABORATORY

Cybersecurity for Buildings and IoT

September 25, 2019

Penny McKenzie
Cybersecurity Engineer

VOLTTRON™

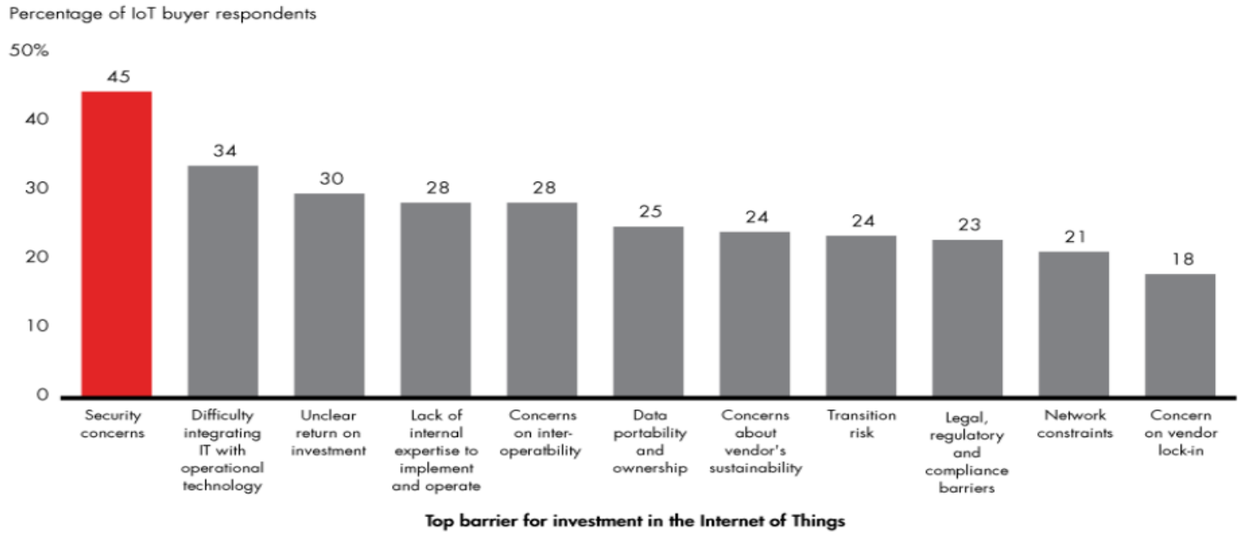
Pacific Northwest
NATIONAL LABORATORY

Internet Connections Worldwide

- There are over 26.66 billion internet-connected devices worldwide in 2019.
- By 2025, there be well over 75.4 billion. WOW!

Challenge

- Security cited as the number one concern in adopting IoT technology
  - Most IoT source code is open source
- Industry could view cybersecurity reputation and remediation downside risks as far exceeding benefits in productivity and energy efficiency
- Roundtable highlighted need for tailored resources and solutions for building industry based on established and proven cybersecurity frameworks



Source: Bain 2018 IoT customer survey (n=521)

https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things

Pacific Northwest NATIONAL LABORATORY

Q Does cybersecurity in software matter?

Early 2017
"Smart" Teddy Bear
Computerworld

Spring 2018
Vegas Casino
Business Insider

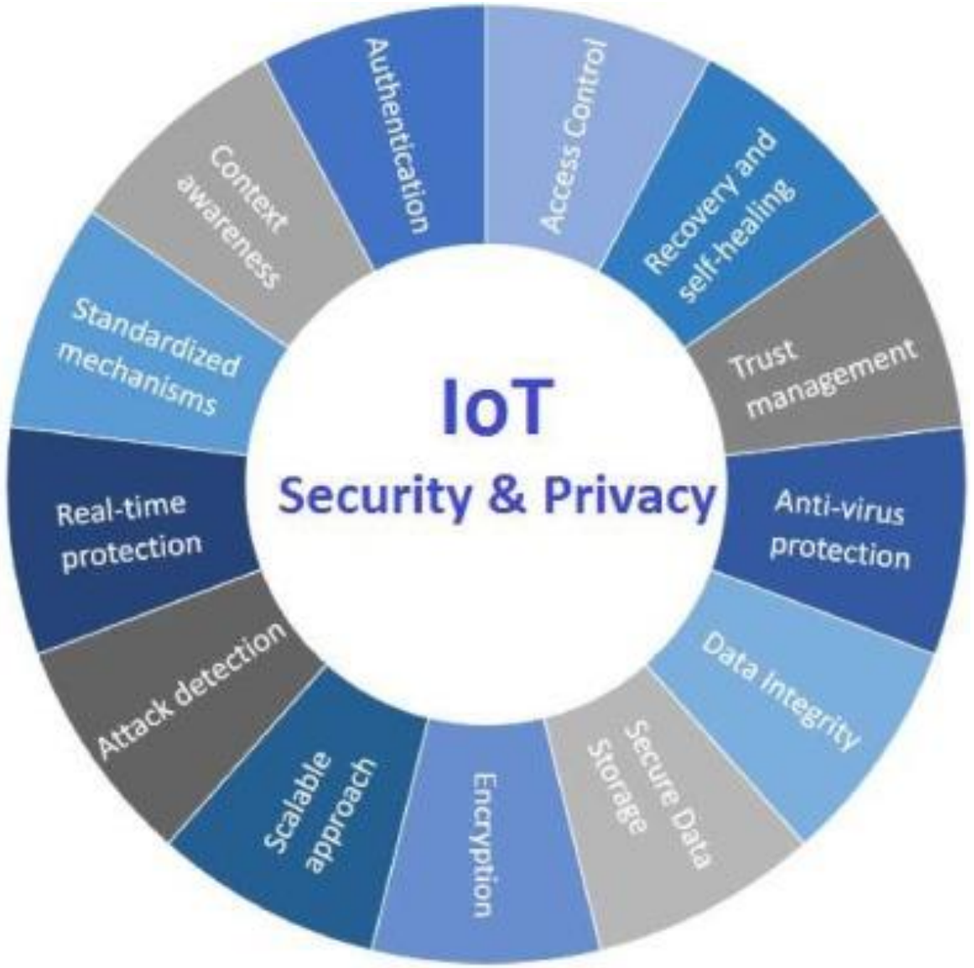
A Yes! Even in fish tanks and teddy bears it matters!!

Q Should it matter at PNNL?

Fall 2018
VOLTTRON™

Building and IoT Challenges

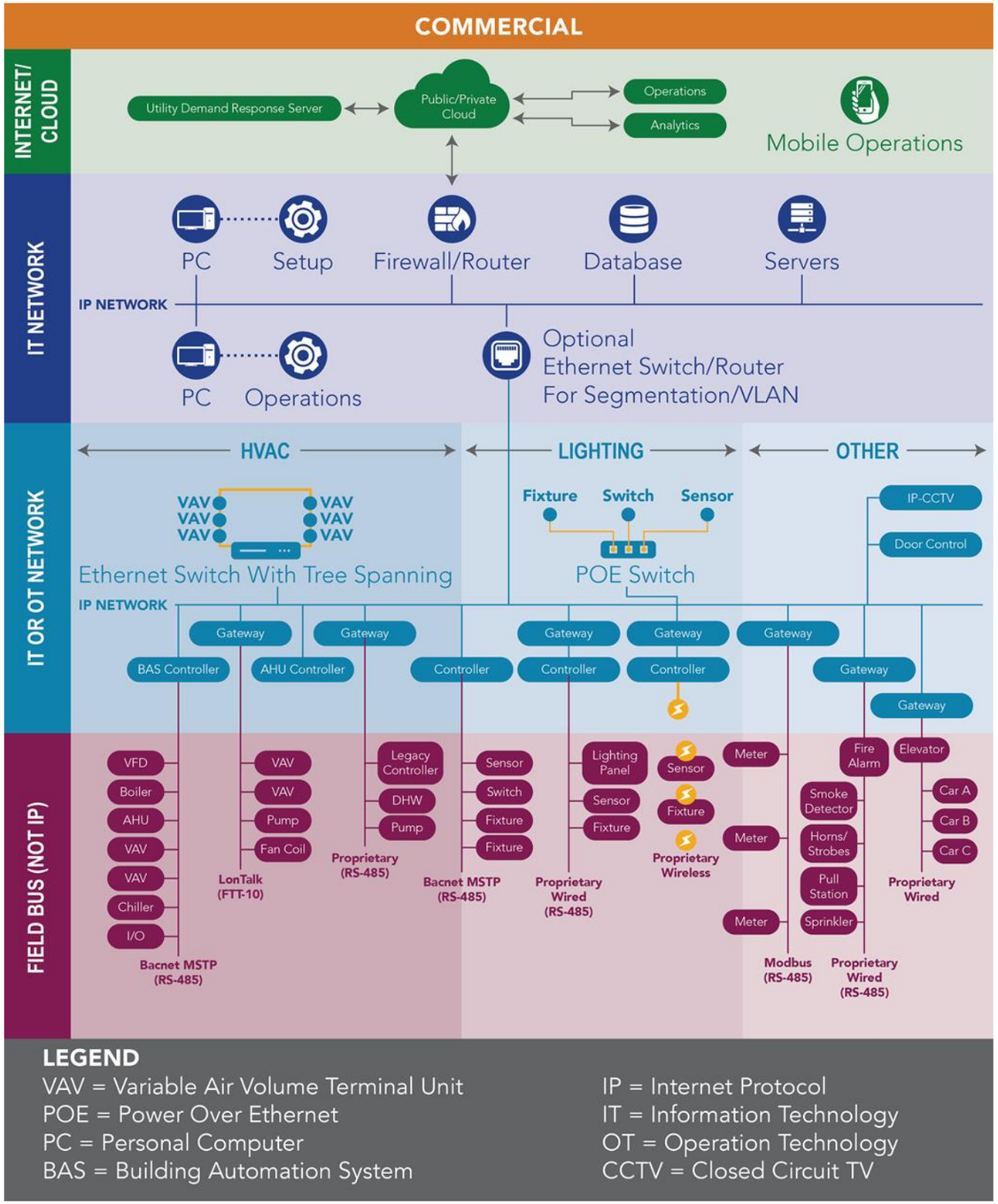
- Technological:
  - Data Storage
  - Obsolescence
  - Complexity
- Industry:
  - Owner Resistance
  - Commercial Suppliers
  - Residential/IoT Suppliers
  - The Cycle of Blame
- Workforce:
  - Proper Cyber Secure Deployment
  - Risk Awareness
  - Training
  - Validation



Pacific Northwest
NATIONAL LABORATORY

Schematic of Commercial Building Controls Communications Architecture

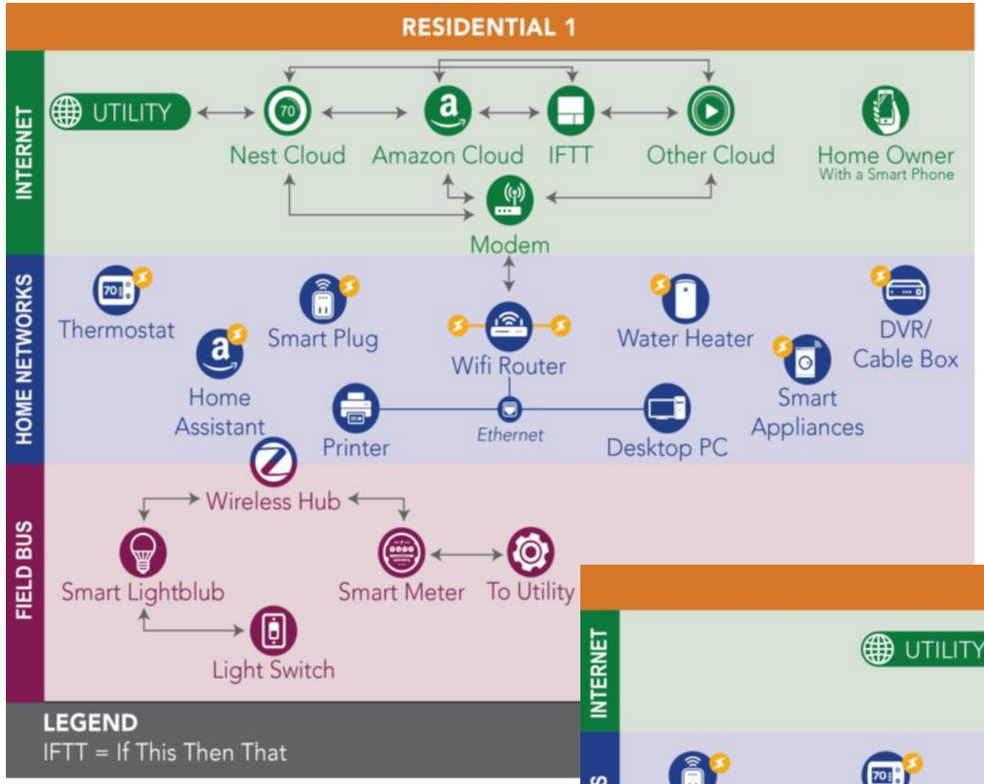
- HVAC
- Lighting
- Cameras
- Metering
- Fire Protection
- Access control

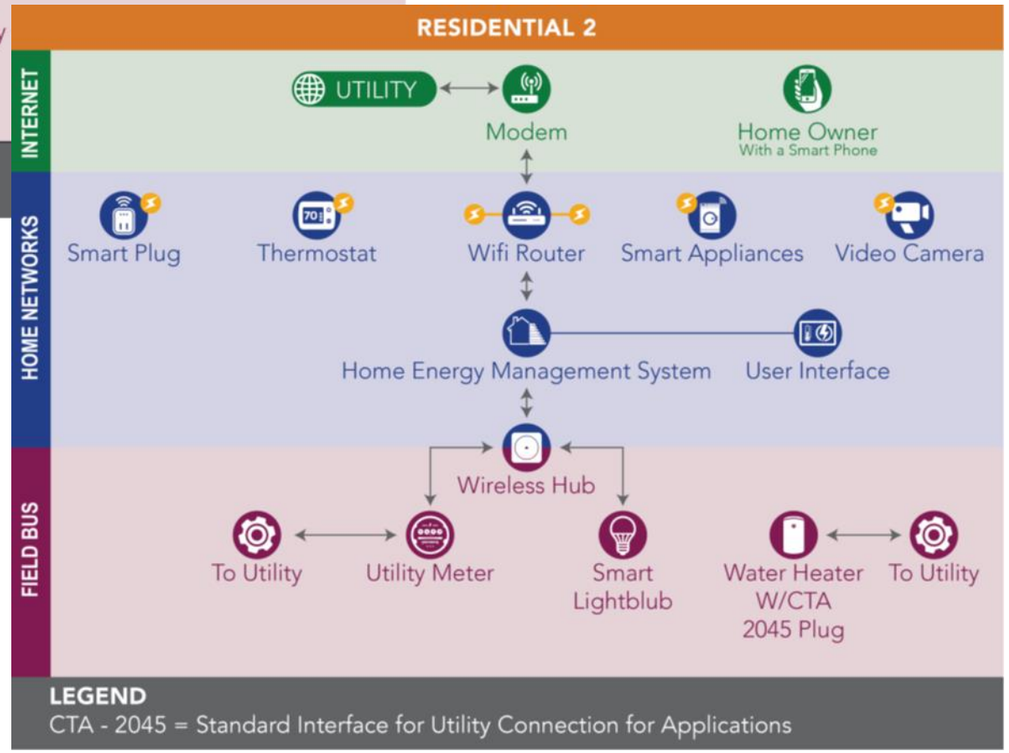


Pacific Northwest
NATIONAL LABORATORY

Residential IoT Controls Communications Architecture

- Low cost
- Easily installed
- Rapidly expanding
- Home Management System





NIST Cybersecurity Framework

Recovery:
System functionality returned
Key lessons-learned incorporated

Need to identify:
- Physical and software assets
- Risks and vulnerabilities
- Organizational R&Rs

Response plan:
Detected events are reported, contained and mitigated

Protections in place for:
Access control, training, data security, system configuration and maintenance

Detection of:
Anomalous data flows and malicious software for baseline operation

Key Gaps and Research Needs

Facilitate stakeholder engagement, education, and knowledge sharing

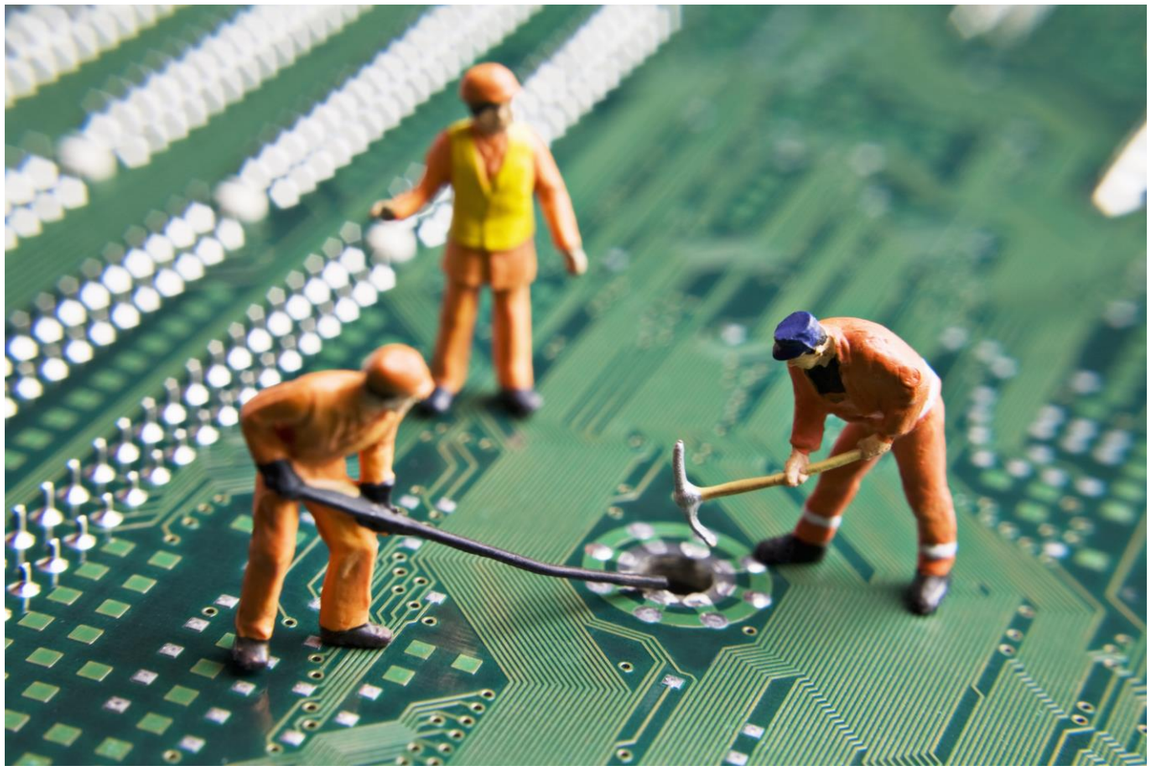
Adaptive, resilient controls for self-healing system

Advanced analytics and ML for vulnerability and attack detection

Tools that allow stakeholders to understand their cyber posture & vulnerability

Resources to close gaps based on risk profile

Methods to assess and test emerging technologies (e.g. Connected lighting)



Conclusions

- Considerable expertise has been developed in existing cybersecurity frameworks and tools and resources for adjacent applications (SCADA and industrial control systems for the grid and manufacturing).
- There is an opportunity to continue to adapt these to the needs of the building community and support adoption.
- PNNL has a number of efforts underway (FCF, MEEDS, PACIFIC) that are contributing to this.
- Recommend systematically identifying remaining research gaps for the built environment.

Pacific Northwest
NATIONAL LABORATORY

Thank you