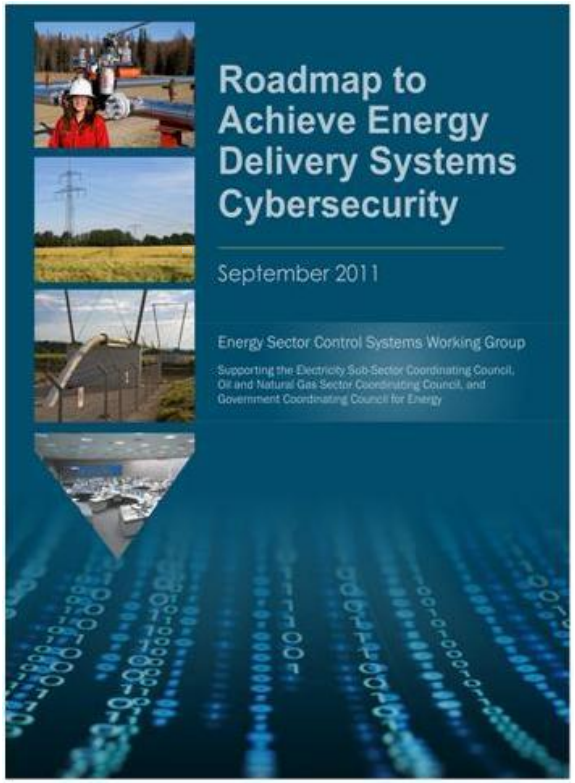
Cybersecurity for Energy Delivery Systems (CEDS) R&D

Following the Energy Sector's Roadmap



Carol Hawk, Ph.D.
CEDS R&D Program Manager

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

U.S. Government Role and Responsibilities

Department of Homeland Security (DHS)

Provide strategic guidance, promote national unity of effort, and coordinate the overall Federal effort for secure and resilient critical infrastructure including identification and analysis of interdependencies among critical infrastructure sectors

Critical Infrastructure Sector

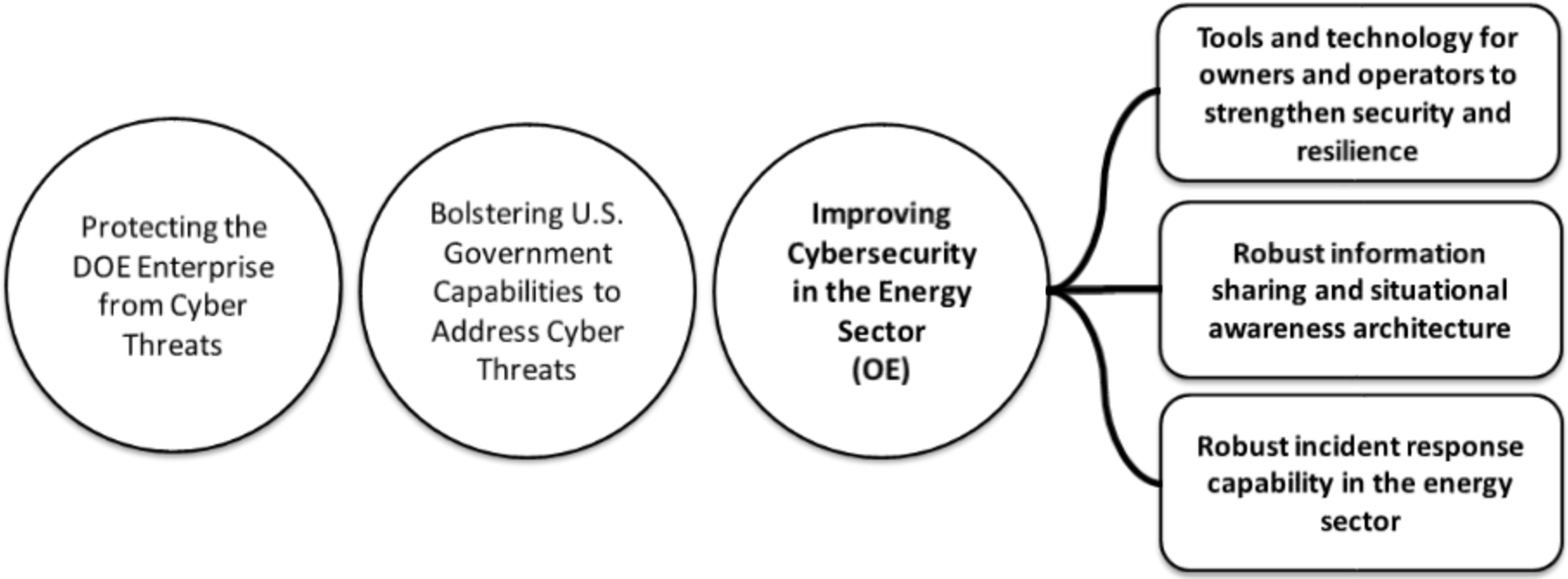
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- ***Energy***
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, & Waste
- Transportation Systems
- Water and Wastewater Systems

DOE - Sector-Specific Agency (SSA) to:

- Collaborate with infrastructure owners and operators to strengthen the security and resilience of critical infrastructure
- Serve as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities
- Carryout incident management responsibilities consistent with statutory authority and other appropriate policies
- Provide technical assistance to the sector to identify vulnerabilities and help mitigate incidents

Department of Energy's Cybersecurity Roles

Office of Electricity Delivery & Energy Reliability (OE) focuses on DOE's role as a Sector Specific Agency (SSA)



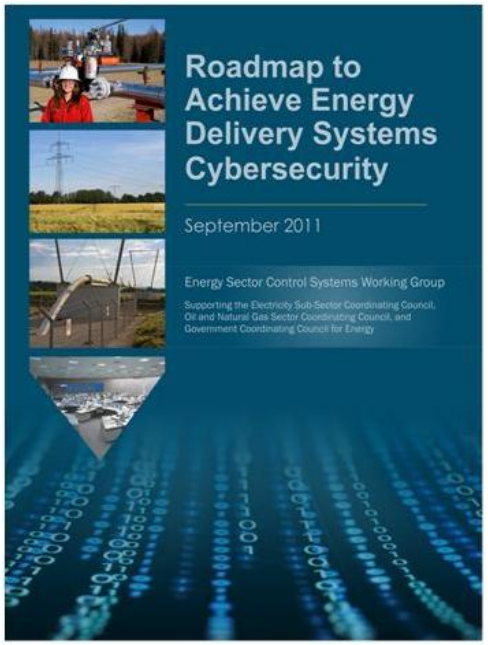
Energy Sector Cybersecurity

Different Priorities

Energy Delivery Control Systems ≠ ***Business IT Systems***

- Energy delivery control systems (EDS) must be able to survive a cyber incident while sustaining critical functions
- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- The modern grid contains a mixture of legacy and modernized components and controls
- EDS components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment
- EDS components are widely dispersed over wide geographical regions, and located in publicly accessible areas where they are subject to physical tampering
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory

Roadmap – Framework for Collaboration



- *Energy Sector's* synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

For more information go to: www.controlsystemsroadmap.net

CEDS Encourages R&D Collaboration

Asset Owners/Operators

- Ameren
- Arkansas Electric Cooperatives Corporation
- Avista
- Burbank Water and Power
- BPA
- CenterPoint Energy
- Chevron
- ComEd
- Dominion
- Duke Energy
- Electric Reliability Council of Texas
- Entergy
- FP&L
- HECO
- Idaho Falls Power
- NIPSCO
- NRECA
- Orange & Rockland Utility
- Pacific Gas & Electric
- Peak RC
- PJM Interconnection
- Rochester Public Utilities
- Sacramento Municipal Utilities District
- San Diego Gas and Electric
- Southern Company
- Southern California Edison
- TVA
- Virgin Islands Water and Power Authority
- WAPA
- WGES

Solution Providers

- ABB
- Alstom Grid
- Applied Communication Services
- Applied Control Solutions
- Cigital, Inc.
- Critical Intelligence
- Eaton
- Enernex
- EPRI
- Foxguard Solutions
- GE
- Grid Protection Alliance
- Grimm
- Honeywell
- ID Quantique
- NexDefense
- *OPAL-RT*
- *Open Information Security Foundation*
- OSIsoft
- Parsons
- Power Standards Laboratory
- *Qubitekk*
- RTDS Technologies Inc.
- Schneider Electric
- SEL
- Siemens
- Telvent
- Utility Advisors
- Utility Integration Solutions
- ViaSat

Academia

- Arizona State University
- Carnegie Mellon University
- Dartmouth College
- Florida International University
- Georgia Institute of Technology
- Illinois Institute of Technology
- Iowa State University
- Lehigh University
- Massachusetts Institute of Technology
- Oregon State University
- Rutgers University
- Tennessee State University
- University of Arkansas
- University of Arkansas-Little Rock
- University of Buffalo - SUNY
- University of Illinois
- UC Davis
- UC Berkeley
- University of Houston
- University of Tennessee-Knoxville
- University of Texas at Austin
- Washington State University

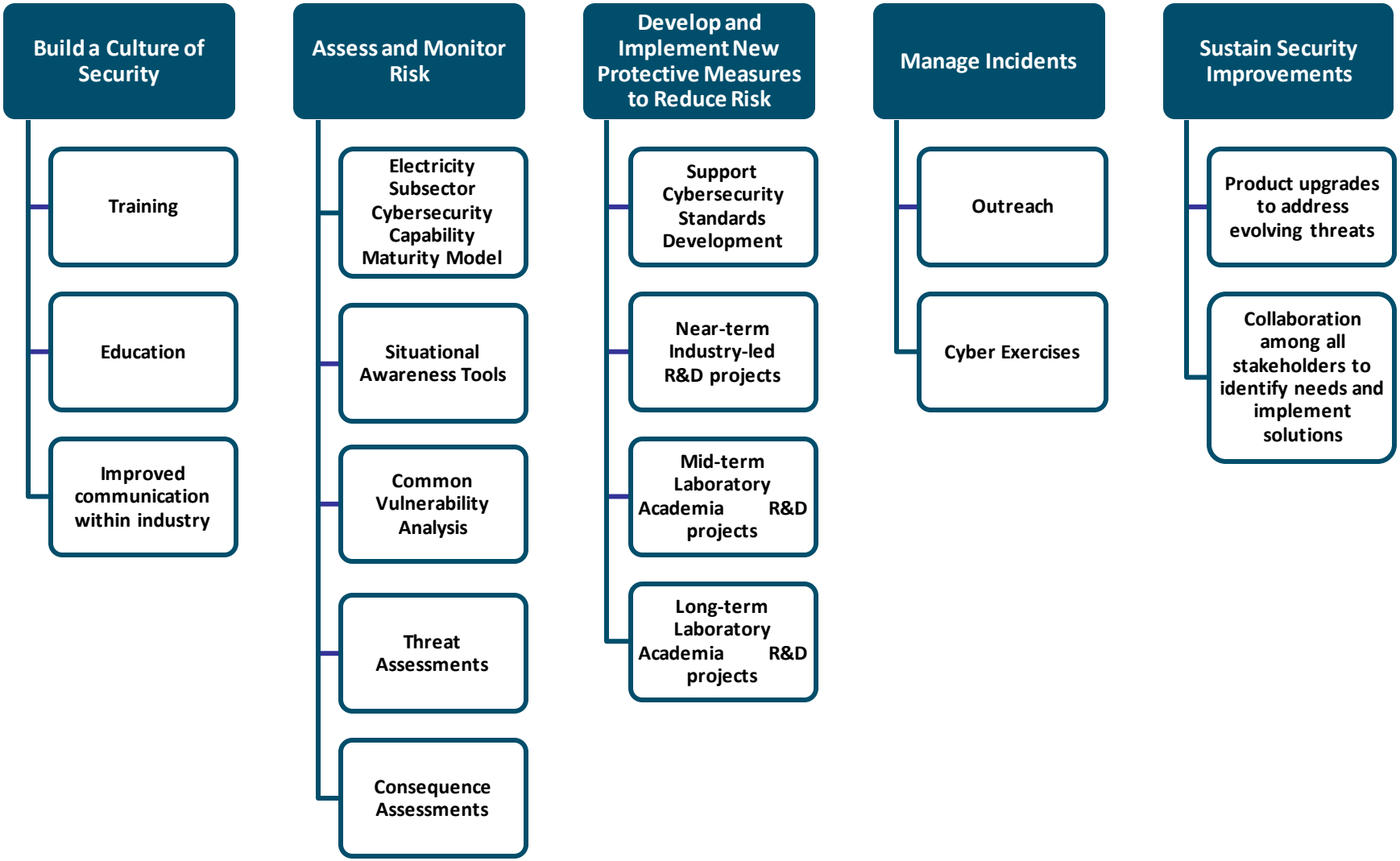
National Labs

- Argonne National Laboratory
- Brookhaven National Laboratory
- Idaho National Laboratory
- Oak Ridge National Laboratory
- Los Alamos National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- National Renewable Energy Lab
- Pacific Northwest National Laboratory
- Sandia National Laboratories

Other

- Energy Sector Control Systems Working Group
- International Society of Automation
- NESCOR
- Open Information Security Foundation

CEDS Alignment with the Roadmap



Roadmap Milestone Analysis

- The energy sector cybersecurity community, whether or not participating in the CEDS program, has made impressive advances relevant to the Roadmap milestones.
- As part of DOE National Laboratories energy sector stakeholder outreach activity, nine labs are working together to perform a Roadmap milestone analysis.
- Energy sector stakeholders interested in participating may reach out to a National Laboratory, using the contact information provided at the end of this presentation.

Near-Term (0-3 years) Roadmap Milestones

Build a Culture of Security	Assess and Monitor Risk	Develop and Implement New Protective Measures to Reduce Risk	Manage Incidents	Sustain Security Improvements
Executive engagement and support of cyber resilience efforts Industry-driven safe code development and software assurance awareness workforce training campaign launched	Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectu policies, and other system changes commercially ava	**Tools to identify cyber events across all levels of energy delivery system networks commercially available** Tools to support and implement cyber attack response decision making for the human operator commercially available	Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders Federal and state incentives available to accelerate investment in resilient energy delivery systems

The Exe-Guard Project led by SEL is an example of a technology that supports the achievement of this milestones

The Exe-Guard Project

SEL SCHWEITZER ENGINEERING LABORATORIES

Partners

Dominion Virginia Power
Sandia National Laboratory
Dartmouth University

Key Success:

SEL's Exe-Guard project is technology that helps prevent unexpected cyber-activity, specifically developed for energy delivery control systems. Providing malware protection while maintaining high reliability**. In December 2015**, the project team transferred the research result of the Exe-Guard project to the Open Source community.

In addition, Exe-Guard is fully commercialized in six products from SEL and there are plans for more products to be released with the technology integrated in the near future.

- SEL3620 - Ethernet Security Gateway
- SEL3622 - Ethernet Security Gateway (smaller form factor of SEL3620)
- SEL3610 - Port Server
- SEL3530 - Real-Time Automation Controller
- SEL3505 - Real-Time Automation Controller (smaller form factor of SEL3530)

Mid-Term (4-7 years)

Build a Culture of Security	Assess and Monitor Risk	Develop and Implement New Protective Measures to Reduce Risk	Manage Incidents	Sustain Security Improvements
Vendor systems and components using sophisticated secure coding and software assurance practices widely available Field-proven best practices for energy delivery systems security widely employed Compelling business case developed for investment in energy delivery systems security	Majority of asset owners baselining their security posture using energy subsector specific metrics	**<u>Scalable access control for all energy delivery system devices available</u>** Next-generation, interoperable, and upgradeable solu[illegible]s for secure serial an[illegible]able communications [illegible]een devices at all l[illegible] energy deliver[illegible] networks imp[illegible]	Incident reporting guidelines accepted and implemented by each energy subsector Real-time forensics capabilities commercially available Cyber event detection tools that evolve with the dynamic threat landscape commercially available	Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining

The <u>Role Based Access Control (RBAC)</u> Project led by Honeywell is an example of a technology that supports the achievement of this milestones

Role Based Access Control (RBAC)

Honeywell

Partners

Honeywell Laboratories
Honeywell Process Solutions
Idaho National Laboratory (INL)
University of Illinois at Urbana-Champaign

Key Success:

This project created role based access control (RBAC) technology for the Honeywell Experion® Process Knowledge System product suite, an energy delivery control system used extensively within the oil and gas industry. RBAC technology limits access to the least needed to perform a given task, which helps reduce the risk of unauthorized access, including by an insider. This technology accounts for roles that are specific to energy delivery operations, for instance, access required for different operating modes, such as normal, start-up, shut-down, and emergency operations. The RBAC technology has been implemented on Honeywell Experion systems since FY2014.

For more information:
https://www.honeywellprocess.com/en-US/explore/products/control-monitoring-and-safety-systems/integrated-control-and-safety-systems/experion-pks/pages/default.aspx

Long-Term (8-10 years) Roadmap Milestones

Build a Culture of Security	Assess and Monitor Risk	Develop and Implement New Protective Measures to Reduce Risk	Manage Incidents	Sustain Security Improvements
Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	**Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available**	Self-configuring energy delivery system network architectures widely available Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	Lessons learned from cyber incidents shared and implemented throughout the energy sector Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector

The Cybersecurity Intrusion Detection and Monitoring for Field Area Networks Project led by Applied Communication Sciences (now Vencore Labs) is an example of a technology that supports the achievement of this milestones

Cybersecurity Intrusion Detection and Monitoring for Field Area Networks

Partners

Sacramento Municipal Utility District
Hawaiian Electric Company

Key Success:

Applied Communication Sciences (now Vencore Labs) has developed innovative technology to provide anomaly and intrusion detection for Advanced metering infrastructure (AMI) and distribution automation (DA) wireless mesh networks. **As of June 2015**, this technology is operational at the Sacramento Municipal Utility District (SMUD), Hawaiian Electric, Commonwealth Edison (ComEd), and Baltimore Gas & Electric (BGE). SMUD has entered into an ongoing service agreement to use the SecureSmart service as "their eyes on network", relying upon ACS to monitor both their AMI and DA systems.

For more information:
http://energy.gov/sites/prod/files/2015/12/f27/Cybersecurity%20Intrusion%20Detection%20Security%20Monitoring%20fact%20sheet%20September%202014.pdf

Roadmap Milestone Analysis Participation

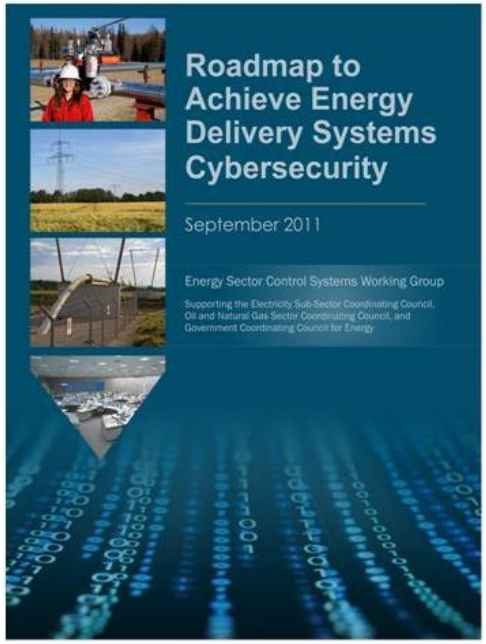
- Invitation to participate and collaborate with a National Laboratory.
- Summary of this activity will be available in September of 2016.
  - Report will celebrate progress, reveal areas that could benefit from increased emphasis, and inform various cybersecurity activities across the energy sector.

For More Information in Participating

- Argonne National Laboratory: Shabbir Shamsuddin
  - Email: shamsuddin@anl.gov
  - Phone: (630) 252-6273
- Brookhaven National Laboratory: Meng Yue
  - Email: yuemeng@bnl.gov
  - Phone: (631) 344-7140
- Idaho National Laboratory: Rita Foster
  - Email: rita.foster@inl.gov
  - Phone: (208) 526-3179
- Lawrence Berkeley National Laboratory: Sean Peisert
  - Email: sppeisert@lbl.gov
  - Phone: (510) 486-4706
- Lawrence Livermore National Laboratory: Jamie Van Randwyk
  - Email: vanrandwyk1@llnl.gov
  - Phone: (925) 423-5307
- National Renewable Energy Laboratory: Erfan Ibrahim
  - Email: erfan.Ibrahim@nrel.gov
    Phone: (303) 384-7433
- Oak Ridge National Laboratory: Peter Fuhr
  - Email: fuhrpl@ornl.gov
  - Phone: (865) 574-8529
- Pacific Northwest National Laboratory: Mark Morgan
  - Email: m.morgan@pnnl.gov
  - Phone: (509) 372-4128
- Sandia National Laboratory: Adrian Chavez
  - Email: adrchav@sandia.gov
  - Phone: (505) 284-6664

For More Information, Please Contact:

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability



Carol Hawk
Carol.Hawk@hq.doe.gov
202-586-3247

Visit:

http://energy.gov/oe/technology-development/control-systems-security

www.controlsystemsroadmap.net

CABA™ Continental Automated Buildings Association

Cybersecurity in Connected Homes and Intelligent Buildings

In participation with Frost & Sullivan

Connect to what's next™

www.caba.org

Today's Presentation

- ✓ *Cybersecurity and the Buildings Industry*
- ✓ *Understanding the Risk and Opportunities for Homes - Key Research*
- ✓ *Best Practices and Challenges for Vendors*
- ✓ *Research Conclusions*
- ✓ *Key Market Take-Aways*
- ✓ *The Roadmap Forward*

Source: Frost & Sullivan

Security Vulnerabilities in an Intelligent Building

As buildings become increasingly intelligent, they may become increasingly vulnerable

- Building Automation
- Energy Management and Demand Response (DR)
- Physical Security
- HVAC and Lighting
- Fire and Life Safety
- Elevators

Integrated Network

Integrated Network

- Real-time Monitoring and Controls
- Networks, Voice, and Data Communication
- Facility and Asset Management
- Parking, Signage, and Display

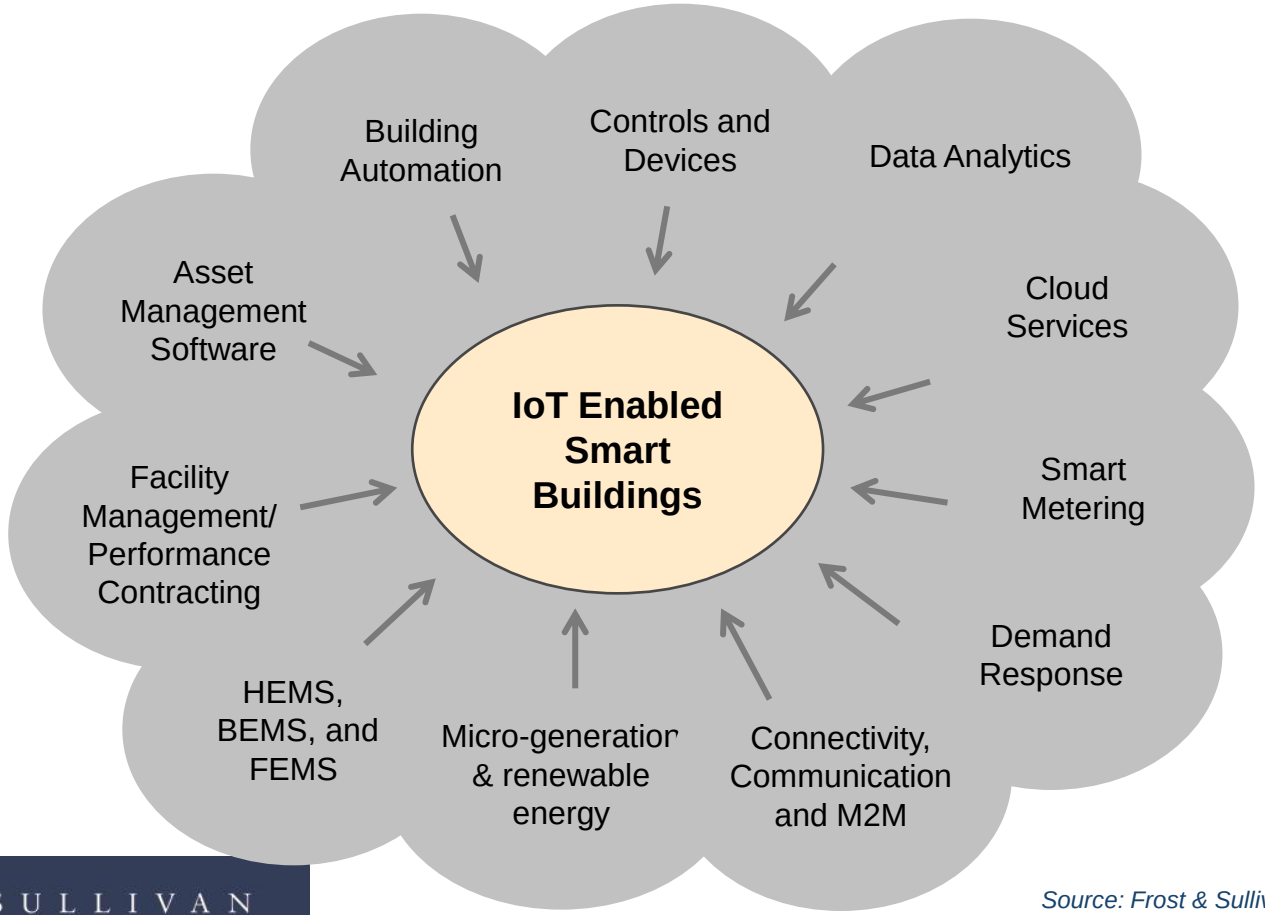
Source: Frost & Sullivan

FROST & SULLIVAN

CABA™ Continental Automated Buildings Association

IoT-influenced Cyber Risk Areas

The inseparable relationship of device and data brought together through aggregation in the cloud presents the next frontier of vulnerabilities



Source: Frost & Sullivan

FROST & SULLIVAN

CABA™ Continental Automated Buildings Association

Managing Vulnerabilities with IT and OT Convergence

Best Practice Framework

Stated Best Practices

1. Cross-learning of skills between OT and IT – Leading to multi-skilled people
2. OT should leverage traditional IT technologies to benefit from efficiencies and reliability.
3. OT controls plant control networks, IT controls anything outside the data management zone
4. Segmented operations, network and layered security approaches

Source: Frost & Sullivan

FROST & SULLIVAN

CABA™ Continental Automated Buildings Association

Cybersecurity Extends to Connected Homes

Cybersecurity vulnerabilities are already present within the connected home and could potentially impact further market penetration of connected home products and solutions. As a result of consumer skepticism and perceived risks, CABA and the Connected Home Council (CHC) members sought to understand the implications of this disruptive trend on their end customers, their value proposition, and, ultimately, their businesses.

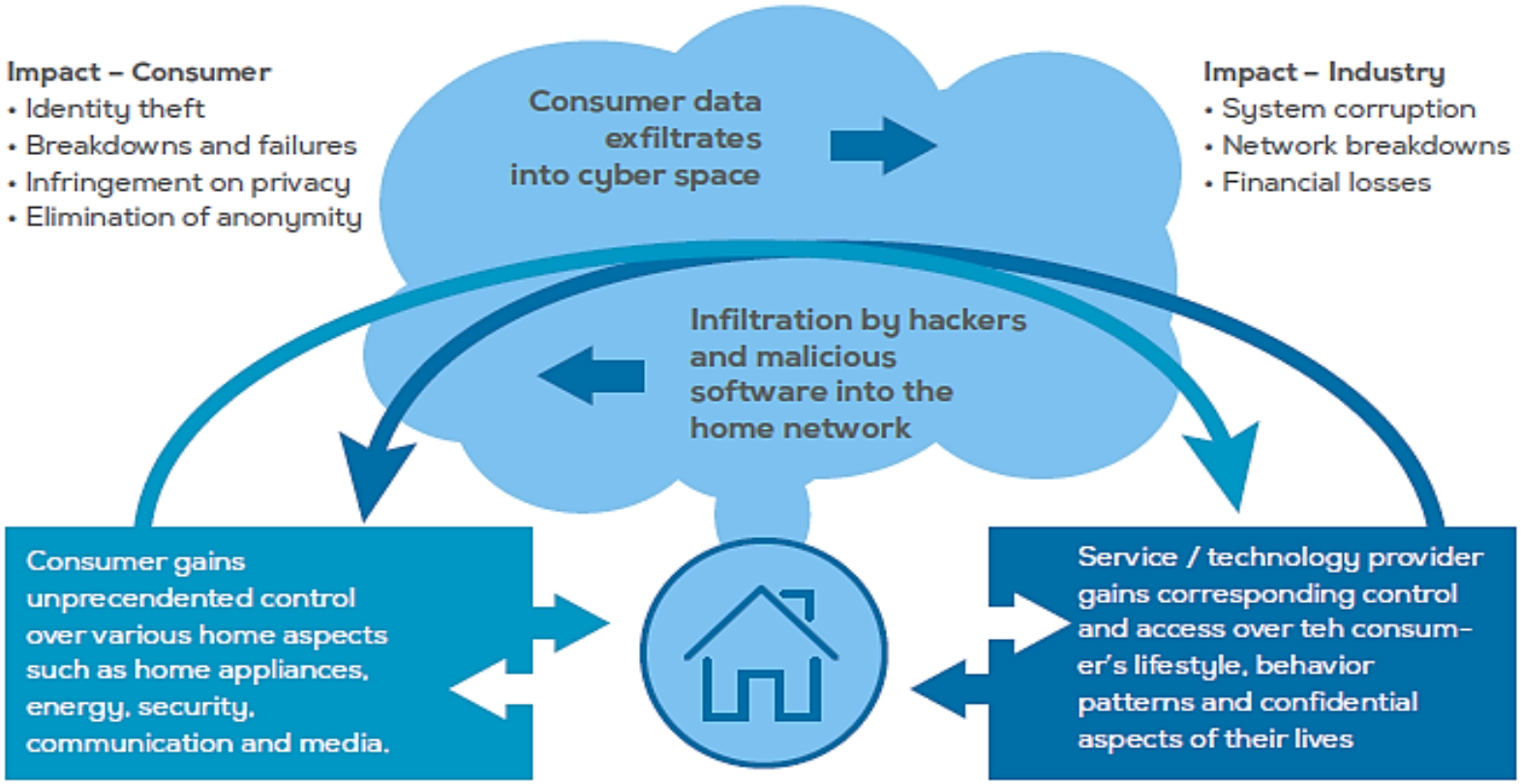
The research examined the issue of cybersecurity in the connected home from the perspective of consumers, vendors and service providers, industry associations, and think tanks. It referenced an existing body of literature in the public domain that pertains to this issue to corroborate findings obtained through consumer and industry research processes.

The key focus areas of the project included the following:

- Understanding consumers' and industry's perspectives on the extent of risk
- Exploring ways to address consumer's skepticism with effective communication
- Understanding process changes and strategic measures to be adopted internally
- Opportunities for collaborations and partnerships to address a common challenge

Connected Home and IoT: Snapshot of Open Access and Information Flow

Cloud penetration will remain limited unless security concerns are overcome, and consumers are comfortable with opening up their homes to the outside world via Internet-based services.



Connected home combines home controls, media, telemetry and personal communications into one integrated platform

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association

Cybersecurity Threat Components

Current Threat Scenario

Cybersecurity Breach Incidents	Impact Areas	Cyber Defense Components	Preventative Aspects
• Device and home network failure • Infection by viruses or malicious software • Infiltration by unauthorized outsiders • Nuisance tactics (email hacking) to life-threatening damages (hacking health device, or hijacking car controls) • Theft of information by solicitors/business prospectors in cyberspace • Unintentional damage caused by authorized third party service providers owing to cybersecurity compromises affecting their own infrastructure	• Connected Home Consumer • Remote access by consumer/ authorized third parties • IoT gateways • Physical access to connected devices, networks, apps • Product/service abstraction platforms • Wireless access • Temporary/guest plug-in devices and hardware	• Identity validation • Endpoint device security • Network security • Data security • Multi-layered security • Dynamic home security hub	• Access to home security systems • Access to connected home network integrating devices through the network • Disabling of home controls and sensor network • Access to communication technologies – home Wi-Fi hubs and Wi-Fi-enabled devices, broadband connections • Access to utility-installed devices such as metering solutions, in-home display, energy monitoring devices, SCADA devices • Hijacking the home control network for blackmail, inflicting damage to energy, security and control systems • Identity theft of the consumer, elimination of anonymity, disruption of privacy, even life threatening damage

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association

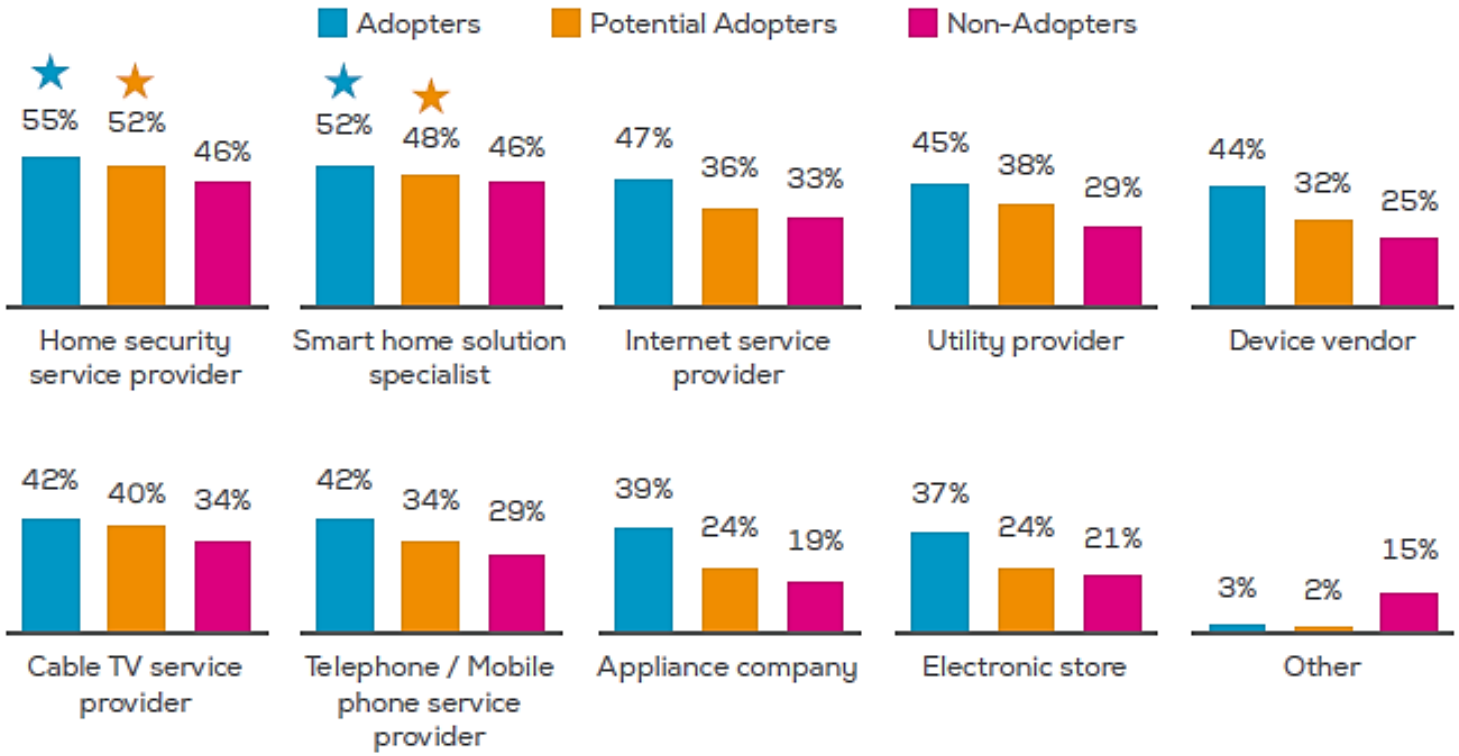
Top Concerns for Adopters

Adopters: Concerns of Connected Homes	
	Adopters (n=474)
High initial setup costs	66%
The costs (time, money, effort, risks) outweigh the benefits	58%
Potential access to personal information from the home network	65%
Security breaches on the smart home network	63%
High management / maintenance costs	61%
Risk of loss of privacy and personal integrity	65%
Security breaches of smart home cloud services	63%
Effect of electrical or power systems failure on the system	62%
Effect of system failure on the ability to manage the home	59%
Insecure smart home apps	61%
More likely to fail than manual systems (due to greater complexity)	56%

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association

Expectation of Cybersecurity from Vendors/Service Providers



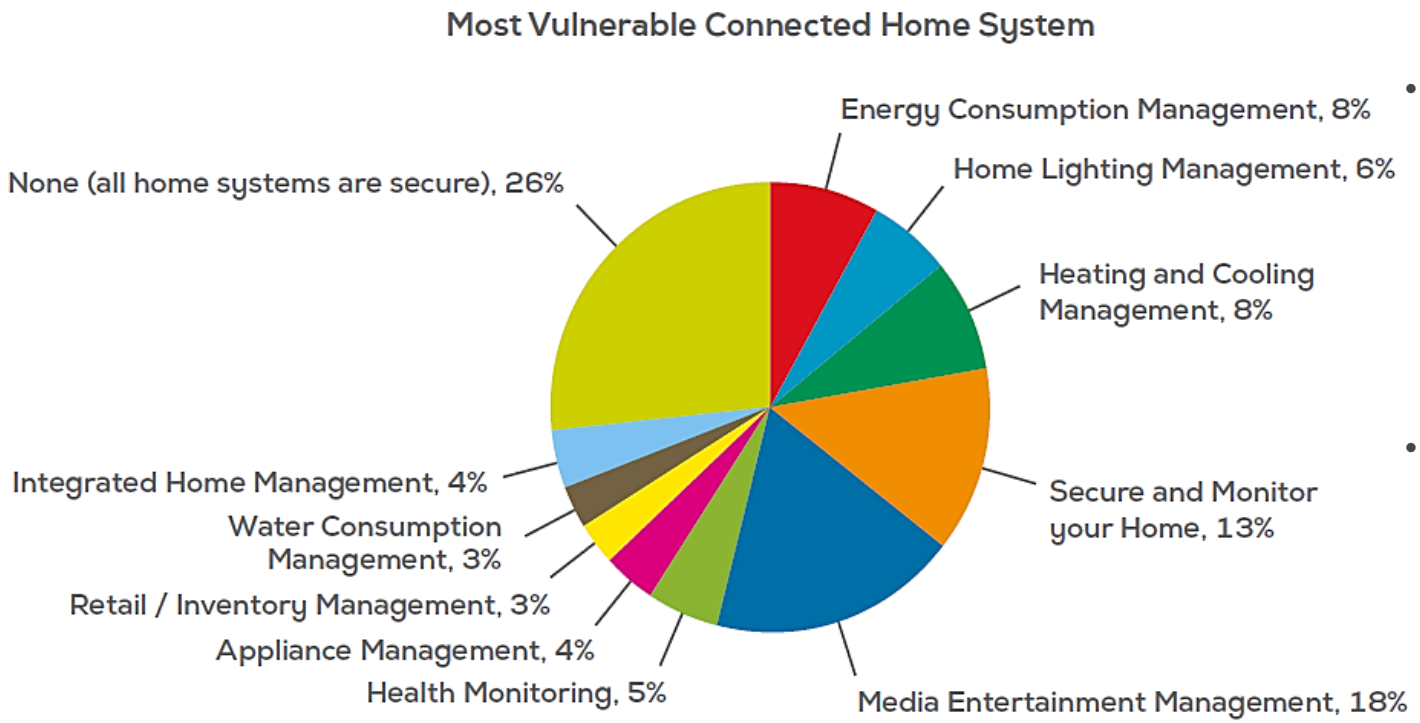
Q: Which of the following would be your likely source(s) for providing cybersecurity for your installed connected solutions?
Adopters (n=474); Potential Adopters (n=307); Non-Adopters (n=482)

Existing relationships and experience with connected home solution providers are instrumental in determining which vendors are trusted more than others in provisioning cybersecurity measures and overall home and data security, including privacy protection.

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association

Cyber Breach Concerns of Consumers



Q: In your opinion, which of your existing connected home systems is most vulnerable?

- The degree of vulnerability associated with various connected home systems is closely reflected in the market penetration trends of these systems.
- Media and entertainment topped the list, with 18 percent of adopters identifying these as the most vulnerable systems, followed by security at 13 percent.

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association

Best Practices for Stakeholders

Vendors & Consumers

- Hardwiring devices where possible
- Ensuring wireless devices have push notifications to the user when offline, indicating that updates are in waiting
- Enabling automatic firmware updates
- Mandating strong passwords
- Sending all data to the cloud using a secured connection
- Avoiding data storage on the device as it can be hacked
- Ensuring all communication uses bidirectional encryption and mandatorily checking certificates at both ends
- Using secure socket layer (SSL) pinning so the device is authenticated, rather than the network the device is on

Utilities/Service Providers

- Creating secure infrastructure by adopting available industry standards, no matter how broad they are
- Following minimum code of conduct laid down by industry regulatory bodies (e.g., FCC codes)
- Considering a "carrier-based firewall" initiative that can provide a smart filter to the home network
- Sending and storing all data in the cloud using a secured connection
- Offering consumer-friendly front-end for interfaces with strong in-built security and frequency of security updates
- Developing resource pool qualified in handling cyber risks

Research Conclusions

The influence of IoT on connected devices and services has opened up an extended world of opportunity for consumers, vendors, and service providers, as well as a high probability of cyber threats to the connected home. The need for cybersecurity is growing rapidly.

An average connected home has at least five potentially breachable devices—other than computers, tablets, and mobile phones—connected to their home network. Not surprisingly, 29 percent of adopters experienced cyber breaches over the last 12 months.

Risk exposure varies; however, technology vendors and ISPs have the greatest risk exposure in the event of a cyber breach, consequently suffering loss of consumer confidence, facing potential legal ramifications, and impacting brand image.

Overall cybersecurity protection in the connected home is inadequate. Addressing consumers' trust and confidence decline is crucial for vendors and service providers. Striking a balance between reliability, functionality and cybersecurity could provide an answer.

There are fundamental challenges in pursuing cybersecurity; however, adopting best practices in data and device security, combined with well-rounded strategies such as enterprise cybersecurity and life-cycle approaches, are critical for success.

Challenges to Market Participants

Internal Organization Challenges

- Communicating cyber defense capabilities of the value proposition
- Determining the right collaborations and partnerships
- Increasing customer/service partner awareness
- Establishing product distinction and brand recognition

External Industry Challenges

- Little knowledge of the full scale of cyber threats
- A fragmented industry with many influencers
- Instituting standards and compliance criteria
- Clear, concise messaging and industry-wide communication issues
- Understanding the end-user's pain points
- Lobbying for appropriate cyber governance policies and standards

Meanwhile the issue intensifies…

- IoT and Big Data continues to present new challenges
- Grim reality - ICS are no longer secure from hacking
- An ongoing and robust plan is critical

FROST & SULLIVAN

Source: Frost & Sullivan

CABA™ Continental Automated Buildings Association

Key Takeaways

1	***IoT is a game-changing opportunity*** for smart building participants, but ***could also pose the maximum threat*** if not pursued responsibly. While still in the early stages, cybersecurity concerns have the potential to ***derail an otherwise fast-growing smart buildings industry***.
2	As more ICS equipment becomes networked, ***the silos of IT and OT must work in collaboration*** to maintain uptime, integration, security, and real-time visibility.
3	In the future, more ***secure systems, devices, and advanced authentication techniques*** are expected to enter the smart buildings industry. The ability to ***segment the network into risk or trust zones*** is important.
4	The ***smart buildings industry has the ability to prevent, or at least minimize***, the damaging impact of cyber threats if it acts in a timely manner. The focus should be on creating and implementing a robust cybersecurity strategy, factoring in anticipated technology changes.

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association

Addressing Cybersecurity - Roadmap Milestones

Cybersecurity Implementation: Impact on the Connected Home Industry

Cybersecurity in Homes and Buildings

Consumers, Vendors, Service Providers

Reduce system vulnerability and potential breach; neutralize negative impacts

Ecosystem; Regulators; New Entrants

Create guidelines; standards and certifications; set minimum compliance criteria

Future of the Market

Sustain growth with countermeasure in place; review and update legislations and privacy policy

Milestones in Implementation

Internal cybersecurity – product hardening initiatives	Instituting standard/certifications	Review market predictions against risk evaluation
Insurance risk assessment and coverage	Policy recommendations/task forces	Conduct legislative reviews and updates
Partner initiatives/collaborations	Compliance mechanisms	Establish privacy framework

2016 — 2020 — 2025

FROST & SULLIVAN

CABA™ Continental Automated Buildings Association

Q &A

Thank You!

Roberta Gamble, Partner and Vice President

Energy & Environment, Frost & Sullivan

Roberta_gamble@frost.com

FROST & SULLIVAN

CABA™
Continental Automated Buildings Association