FROST & SULLIVAN

Attn. Greg Walker

Continental Automated Buildings Association

1173 Cyrville Road, Suite 210

Ottawa, ON, K1J 7S6

Connected Home Council (CHC) Landmark Research 2020

"Privacy and Cybersecurity in the Connected Home"

Closing Date: February 24, 2020, 4:00 PM ET

"Technical Proposal"

Submitted To:

Continental Automated Buildings Association (CABA)

From: Frost & Sullivan

24 February 2020

Table of Contents

1 CHECKLIST - RFP SECTION 13 - MANDATORY REQUIREMENTS REFERENCE

RFP Reference	Requirement (Bidder's proposal should repeat exactly as defined in the RFP)	Referenced Section/Page In Bidder's Proposal
13.1	Technical Proposal Page Limits Acknowledgement Technical Proposal – Introduction/Legal/Other (Include statements from Section 1.2) Max Pages 1 Technical Proposal – Personnel Biographies; Max Pages 2 Technical Proposal – About Research Organization (Experience, sample research, clients, etc.); Max Pages 2 Technical Proposal – Methodology (Sample size, target groups, timeline, etc.); Max Pages 2 Technical Proposal – Appendix A: Signed RFP; N/A Technical Proposal – Appendix B: Sample Research (Whole or partial research) Financial Proposal (Provided as a separate document, include statements from Section 1.2, reference Technical Proposal); Max Pages 2	Provided Below: Page #4: 1 page Section 6; Page 12&13 Section 4; Page 6&7 Section 5; Page 8, 9,10 Attached Attached Provided separately
13.2	Evidence of knowledge and experience of personnel of current theory and practice in the connected home research discipline by providing relevant biographies of all personnel who it is proposed will participate in the project. The vender's project leader must have a minimum of 10 years relevant experience.	Page 13; 30-35
13.3	Evidence of previous experience in the connected home discipline by providing examples of relevant projects prepared for three (3) separate clients within the preceding 48 months. References will be required from these three (3) clients, if requested by CABA.	Page 7
13.4	A summary of how the vendor proposes to perform the project and the relevant experience of the proposed Staff.	Pages 8, 9, 10, 14
13.5	Identify the sample size of both the interviews and surveys	Page 9
13.6	Acceptance of deliverables as identified in the Terms of Reference/Prospectus and proposed schedule.	Pages 4, 10
13.7	**The vendor must be a member of CABA or agree to become a member of CABA (US$850) (before the RFP is reviewed).**	Already Member of CABA
13.8	**RFP Signature** - Bidders must complete, sign (end of Section 18) and return this RFP form prior to the closing date.	Signed and attached with proposal delivery email
13.9	**Costs must be in $USD.** A fixed price including a full cost breakdown as per Section 17, "Financial Proposal" must be provided.	Provided in Financial Proposal
13.10	The Financial Proposal must be submitted as a separate package (PDF document) to the technical proposal **(NO FINANCIAL INFORMATION MAY APPEAR IN THE TECHNICAL PROPOSAL).**	Submitted Separately

2 Certifications

Frost & Sullivan hereby provides the following certifications:

- Certification items Nos. I to III – These are provided as requested by CABA in the RFP.

CERTIFICATION

I As per the RFP point # 1, sub point 1.2 (on page 2 of the RFP), Frost & Sullivan hereby agrees to the following:

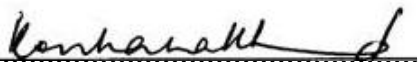
1.) We hereby offer to sell and/or supply to the Continental Automated Buildings Association (CABA), for terms and conditions set out herein, the supplies and/or services listed herein and/or any attached sheets at the price(s) set out therefore.
2.) We hereby certify that the price quoted is not in excess of the lowest price charged anyone else, including our most favored customer, for like services.

II Frost & Sullivan confirms acceptance of the deliverables and associated timeline as identified in the Terms of Reference and schedule outlined in Section 13 of the RFP (Please refer to page 10, Section 13 – Mandatory Requirements, Item # 13.6).

III As per RPF point # 9, sub points 9.1 & 9.2 (on page 5 of the RPF), Frost & Sullivan certifies the following:

9.1 We hereby certify that all the information provided in all the attached biographies/resumes, particularly as this information pertains to education achievements, experience and work history, has been verified by us to be true and accurate. Furthermore we hereby certify that, should we be awarded a contract and unless CABA is notified in writing to the contrary, the personnel offered in our proposal shall be available to perform the tasks described herein, as and when required by the project authority. CABA and the Steering Committee must approve all new personnel working on the research that were not listed in the RFP submission.

9.2 We hereby recognize and certify that CABA will be the owner of the final deliverables and that no revenue-sharing arrangements on subsequent report

Signature……  ……
(Authorized Representative of Frost & Sullivan)

Name – Konkana Khaund

Date – February 24, 2020

3 Introduction and Background

The Continental Automated Buildings Association (CABA) is an industry association dedicated to the advancement of intelligent home and building technologies. As part of its key responsibilities CABA undertakes cross-industry collaborative research under the CABA Research Program. Such research is funded and performed under the aegis of its leading industry councils focused at home and building technologies. The Connected Home Council (CHC) is a core working council of CABA, instituted to lead the advancement of technologies, industry initiatives and knowledge base with regards to an automated and connected home. The CHC has expressed interest in pursuing a landmark research project, specifically looking at the issues of privacy and cybersecurity in the context of connected homes, and evaluating the risks and susceptibilities associated with it. Given that cybersecurity vulnerabilities are already entrenched within the connected home, and further aggravated each day with IoT and connected devices becoming more ubiquitous, the CHC members therefore need to evaluate cyber risk mitigation prospects and privacy infringement issues for the industry and the consumers they serve.

Frost & Sullivan has been tracking the connected home market for over a decade. Our extensive research over the years has witnessed a simply automated or digitally-advanced home environment progress within a considerably short period of time into a communication-rich living space. This has enabled a host of smart experiences for the consumer ranging from energy management, interactive home devices, connected appliances, integrated entertainment and real time security solutions. However, it has also allowed unprecedented access to a variety of service providers, their networks and pervasive technologies to infiltrate the home.

As Frost & Sullivan's past research with CAB have demonstrated, the connected home encompasses both, an internal and external communication network, enabled by the Internet-of-Things (IoT) to activate various lifestyle supporting functions. This characteristic provides the very basis for cybersecurity and privacy infringement vulnerabilities for the connected home consumers and their associated, as it offers direct access to technology and service providers to have power over various systems and devices within the home. Although meant to enable connected experiences, such access opens the home to potential vulnerabilities of cyberspace, and makes it a victim of breakdowns and failure inflicted by such adversaries on service providers' networks. Systems that were installed to provide security and comfort can lead to serious breach of consumer privacy, service disruptions, theft of personal information and threat to anonymity, leaving not only the homeowner but also the solution providers powerless over such events. While consumers question the advantages of "connectedness" at the cost of such risks, the industry also is also burdened with extreme scrutiny of their solutions and privacy commitment. Unless the issue of cybersecurity and privacy is dealt with in a comprehensive manner market prospects for connected home solutions providers can be negatively impacted. For CHC members, the fundamental questions that therefore arise are:

- What is the magnitude of this threat and how can it be managed or eliminated?
- What are the challenges of implementing cybersecurity and privacy protection measures?
- How do various stakeholders manage the responsibility and accountability issues associated with it?
- Can industry participants keep pace with an ever evolving connected home space?
- What business cases can support greater provisioning of privacy protection and cybersecurity measures for connected home consumers?
- What should industry participants do to turn this industry challenge into specific opportunities?

Frost & Sullivan is pleased to put forward this proposal to assist CHC in its endeavors to address these fundamental questions. We believe our project design will help CHC members in formulating an actionable strategy to address the complexities of connected home cybersecurity, and offer recommendations on how to make cyber defense and privacy protection measures an integral part of the connected home industry.

4 About Frost & Sullivan

Frost & Sullivan, a global research and consulting organization, is uniquely positioned to not only identify growth opportunities but to also empower and inspire our clients to create visionary growth strategies for their future, enabled by our extraordinary depth and breadth of thought leadership, research, tools, events and experience that assist our clients by making their goals into a reality. Our understanding of the interplay between industry convergence, mega trends, technologies and market trends provides our clients with new business models and expansion opportunities. We are organized, positioned and trained to assist our clients in the development of their transformational growth strategies. We work with clients to not only help them survive the present, but adapt and thrive for the future. Our unparalleled breadth of services combines collaborative growth partnership research and consulting, technology and IP solutions, strategy, brand and demand solutions.

Frost & Sullivan's Global Presence, Coverage and Perspectives

More than 1,800 Consultants and Analysts in 40+ Offices Provide Perspective, Coverage & Service

Our Industry and Market Coverage

- Comprehensive understanding of all industry and market opportunities
- Analysis of potential competition from outside Client's industry
- Identification of growth opportunities in areas other than Client's current industry

10,000 active clients globally in more than 300 industry sectors and markets

Our Clientele

- Emerging and Global 1000 companies
- Leading industry associations
- Universities, business and tech schools
- The investment community

Frost & Sullivan's Expertise in Connected Homes, Cybersecurity and Digital Transformation

The connected home energy segment is undergoing rapid transformation from a static and conventional environment to a dynamic one with the impact of IoT. Connected concepts and platforms are making a steady headway into the home, although connectivity challenges and cybersecurity issues continue to impact adoption. In spite of these growing concerns, IoT devices and new connected concepts for the home are showing a rapid growth in the last decade spurring user sophistication and creating a burgeoning connected solutions ecosystem. Services to the industry are rapidly evolving to leverage the influx of information from the influence of IoT, creating new solutions and business models. And all of this is driven by the increasing need for consumers' convenience, safety and security, which, has also made this space increasingly vulnerable and risk prone. In keeping with the changing trends Frost & Sullivan's research has always taken a holistic view of the connected home and personal security industry encompassing all key aspects. From exploring market commercialization prospects, new business models, industry convergence, and initiatives to disseminating though leadership in areas of connected living, cybersecurity and privacy–our experience profile and recognized brand equity gives us a distinct edge.

Frost & Sullivan's Domain Expertise on Connected Homes

Frost & Sullivan's Unique Qualifications to Partner with CABA
Industry leading research and consulting experience in connected homes – over 15 years' experience of each senior project team member
Recognized project partner for CABA and individual CHC members – 5 landmark research projects delivered to CABA including "Impact of Smart Grid on the Connected Home"; White paper on Cybersecurity and Intelligent Buildings; several high-value consulting projects to CHC members
Leading authority on cybersecurity research – unmatched breadth of research and consulting projects delivered to over 25 industry sectors; 50+ reports published; Average 5 publication a year
Retained as INTERPOL's Knowledge partner on physical, electronic and cybersecurity research
Leader in Homeland Security Research on conventional and cybersecurity areas for over a decade – key clients include Dept. Of Defence, major internet security companies, research labs
Recognized though leader and knowledge partner on connected environments, buildings and cybersecurity - ASIS International, Consumer Electronics Show, SIA

Sample of Past Experience

Provided below is a representative list of our expertise in the connected homes and energy sectors that would directly benefit CABA in working with Frost & Sullivan on this project.

Project	Project Highlights and Outcome
Cybersecurity in the Connected Home CABA-CHC, 2015-16	• The project involved uncovering both consumer and industry perceptions around cyber risks, security concerns and the adequacy of various counter measures in dealing with cyber threats within the connected home. • It evaluated the roles and responsibilities of various stakeholders of the connected home industry value chain in dealing with cyber threats and the best practices that are being adopted by various entities in that direction. • Finally the project looked at recommendations for industry participants to follow in countering cyber threats going forward. The findings were tabled before the project steering committee in early 2016.
Connected Home IoT Energy Roadmap CABA-CHC, 2018	• The project involves establishing innovations, trends and opportunities pertaining to home energy solutions, their market readiness and ability to deliver to consumers' needs and priorities • It looks at identifying market evolution and transitions in home energy management and energy efficiency solutions impacted by IoT, connectivity and convergence, and delivery business models • It addresses consumer adoption issues and challenges for various home energy technologies and market demand indicators, including the role of the utility industry in influencing the roadmap • Finally it will look at evaluating interdependencies among the connected home energy solution provider ecosystems and strategic recommendation on implications to stakeholder groups
Impact of Smart Grid on the Connected Home CABA-CHC, 2012	• The project assessed critical needs such as the consumer's need for easy-to-use interfaces and simplified options to control, monitor, and remotely manage the connected home. • It confirmed that competitive advantages will depend upon the vendors' ability to offer solutions that have multi-faceted features and can meet scalable needs for the customer. • Findings proved that the ability of a connected home to integrate with the smart grid is a beneficial proposition both for home owners and utilities. • Recommendations made to the steering committee included hands-on approaches such as creating work stream-oriented sub-committees to pursue technology developments and standards, among others.
Home Energy Management Roadmap and Ideal Persona Evaluation Client: Tier 1 Global energy management player, 2016	• The project involved understanding the niches and market levers that can be targeted to predict the value of a fully intuitive and autonomous home and the role of home energy management and connected devices to deliver to it. • The project also explored consumer's concerns for privacy infringement and cyber protection in the event of exchanging home energy data with third parties, and vendor's responsibilities towards providing fully security-defined updated devices on an ongoing basis to consumers • It included determination of motivators and adoption challenges, and market evolution paths for ecosystem partnerships along the implementation roadmap. • It also established the future course of activity including determination of persona types, and identification of technology disruptors that will help client achieve their project goals.
Market Prospects and Future Roadmap for Smart Home Energy System Client: Internet Technology Leader and Smart Home Operating System Provider, 2012	• The project included uncovering the market potential for innovative smart thermostats and home energy management devices as intuitive products for enabling connected home energy monitoring and management. • Frost & Sullivan undertook a detailed market research exercise in North America to understand the demand for such products in the context of the anticipated growth in connected home devices and home energy management. • The research identified specific niches that the product could capitalize on, and developed a growth roadmap based on the latent demand that could propel its potential growth within the connected homes market over the next five years.

Sample of Relevant Research Expertise

Addressing Cyber Risks in the Connected Home, A Voice-of-customer Research by Frost & Sullivan, 2019
Transformational Trends in Cybersecurity in the Home Energy Management Solutions Industry (2018)
Opportunities for Internet of Things (IoT) in Connected Homes and Buildings, 2015, 2017, 2019
Technology Convergence with IoT and impact on Urbanization, Construction and Mega Cities, 2016
North American Energy Management Services, 2015, 1016, 2017, 2019
Connected Homes: Winning Solutions and Applications, 2015
Connected Homes: Supplier Strategies and Business Models, 2016
DC power distribution markets for home and building energy management, 2015
Home of the Future – connected home consumer demand review on connectivity, security and energy integration, 2015
Connected Home Consumer Preferences: A Market Ready for Solutions, May 2014
Connected Living, Apr 2014
Next Steps for Smart and Connected Homes, Feb 2015
Cybersecurity in Smart Buildings, Sep 2015
The Future of Lighting – Role of IoT and LaaS in Home and Buildings, Feb 2016
Connected Lighting and LED Integration in Smart Buildings, Dec 2015

5 Technical Proposal Methodology and Deliverables

Frost & Sullivan will extensively utilize our repository of industry research and databases pertaining to connected homes, cybersecurity and privacy, IoT and related domains for a good head start on this project. To uncover the underlying trends and issues associated with energy aspects as it related to the home environment Frost & Sullivan will start with certain key predictions and hypotheses about the concept. The research process will aim at proving these, as well as determining the potential changes to be expected over the span of the next decade in formulating the ideal cyber defense plan for the connected home. The predictions and hypotheses relevant to this research and the action items that will address these are listed in the exhibits below.

Our Understanding of Scope, Study Hypotheses and Key Domain Areas for Research

KEY HYPOTHESES
Expanding scope of critical vulnerability areas due to increasing IoT device penetration
Current cyber defined solutions lack a rigid implementation framework
Lack of defined measurements and business cases for investment in counter measures
Inadequacy of education efforts & training for consumers and service providers
Vendors' lack of commitment to upgrade systematically to security defined solutions
Limited success with privacy and cybersecurity regulation, certification and consortia-led initiatives

SCOPE & DOMAIN AREAS

- State of Privacy and Cybersecurity in the Home
- Stakeholder Analysis
- Best Practices Overview
- Value Proposition Optimization
- Future Direction and Recommendations

Frost & Sullivan's Approach & Project Fulfillment Plan

FROST & SULLIVAN'S APPROACH

Following our past history of successful landmark research projects with CABA, we propose the following approach:

Engage & Organize	Deploy a consensus-based approach to lay out engagement processes and extract best value by mobilizing both, the project team, and the steering committee.
Evaluate & Affirm	Apply proven research and investigative methodologies to affirm and corroborate fact-based analysis.
Collaborate & Deliver	Mutually collaborate with the steering committee, CABA and external industry experts to deliver best-in-class outcomes.

PROJECT FULFILLMENT PLAN

PROJECT INITIATION	PROJECT PLANNING; SURVEY AND RESEARCH DESIGN COLLABORATION; PROJECT MANAGEMENT PLAN
RESEARCH PHASE	INTERVIEWS; SURVEY; SECONDARY RESEARCH; PANEL DISCUSSIONS; ANALYSIS & REVIEWS; EXPERT ADVISORY PANEL GUIDANCE
REPORT CREATION	COLLABORATIVELY DESIGN AND DEVELOP FORM FACTOR OF FINAL DELIVERABLES; MILESTONE PLANNING; RECOMMENDATIONS REVIEW
FINAL DELIVERY	DRAFT & FINAL REPORT DELIVERY; EDITORIAL AND PAGINATION SUPPORT; WEBINARS; PROMOTION AT INDUSTRY EVENTS

Expert Advisory Panel

Frost & Sullivan will recruit the following experts as part of the proposed Expert Advisory Panel. This specially enlisted panel of experts will offer supervisory guidance, critique and external input to enrich the project outcomes.

Expert Advisory Panel Members	Profile	Role, Responsibilities & Deliverables
 Dr Ann Cavoukian  Dr Michelle Chibba  Jarad Carleton	Dr Ann Cavoukian, Executive Director at Global Privacy & Security by Design Centre, Ryerson College, University of Toronto Dr Michelle Chibba, Internationally Acclaimed Cybersecurity & Privacy Proponent Jarad Carleton, Global Program Leader, Cybersecurity, Frost & Sullivan	• Review project design and methodology with project team • By invitation on 2 update sessions during the duration of the project, liaise with the steering committee to provide external guidance • Supervise survey design and suggest directional changes, as warranted • Provide inputs on future direction for the industry in developing an ideal cybersecurity and privacy protection framework for connected homes • Guide the formulation of strategic recommendations of the study

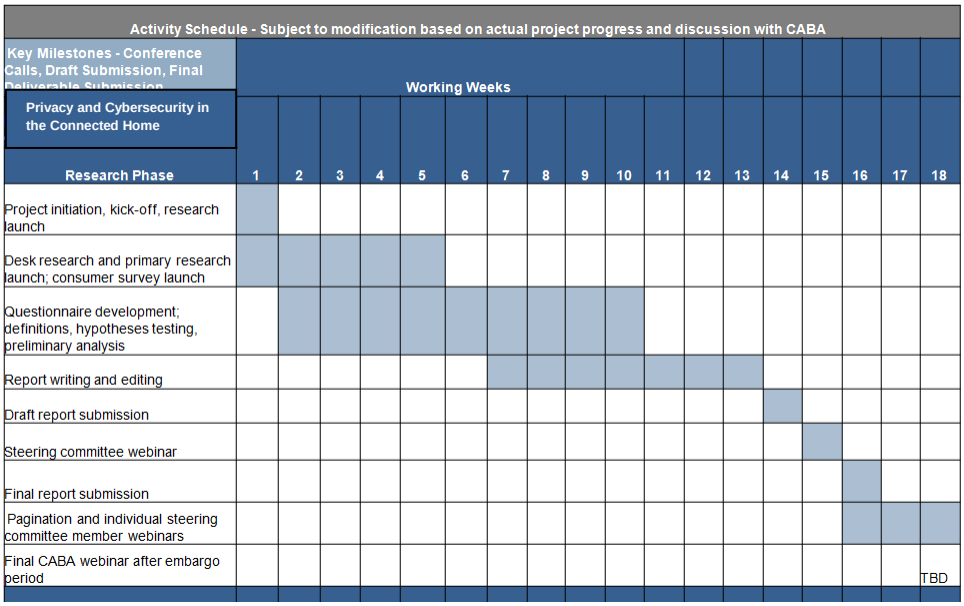
Sample Size, Target Groups and Research Methodology

The exhibit below provides a detailed description of the sample categorization, interview technique and research methodology to be deployed and the target groups to be included in this research.

Item	Component	Description	Target Group Profile	Sample Size	Research Technique
A	**Homeowners/Consumers**	Consumers of connected homes/smart devices/smart home technologies	Occupant/Homeowner in US and Canada	1000-1200	End user survey through online panels and survey methods
B	**Connected Home Technology Vendors & Service Providers**	Vendors/suppliers of technology solutions such as home energy management systems and platforms, energy consuming devices and systems such as HVACR, Lighting, Security, Energy Display and Monitoring, Telecom and Connectivity, Cabling, Wireless solutions, IoT solutions, Managed services, Analytics, Dashboards, Remote monitoring, Could hosted technologies and platforms, End-to-end IoT providers, Cybersecurity Solution providers, Ongoing services and support, third party product assimilators and integrators	Vice Presidents, Directors, Product/Sales Manager, CIOs, CTOs, Alliance Partners, Third Party Service Personal, MDU Building Super, Facility Manager	60-75	Analyst Interviews with Industry Stakeholders
C	**Cybersecurity Solution Providers & Privacy Advocates**	Security & cybersecurity solution vendors, service providers, privacy experts and architects, consultants	Sr VPs, Directors, Chief Architects, Chief Consultants, expert advisors, think tanks, regulators	25-30	By Invitation Panel/Forum based Analyst Discussion Techniques
D	**Industry Influencers**	Codes and Standard Development Organizations for connected environments and IoT, Cyber Policy and Privacy Law Influencers, Regulators, Industry Associations, Academic Influencers, Think Tanks	Technical Committee Heads, Academic Professors, Association Governing Body Stakeholders, Government Leaders, Policy Analysts	20-25	Analyst Interviews with Industry Stakeholders
Overall Sample Size (A+B+C+D)				**1,110-1,330**	

Timeline: Activity Schedule

The proposed timeline for this project is depicted below. Actual milestones may vary based on progress and discussion with CABA and steering committee members. Total time frame is expected to be 18 working weeks.



Deliverables

Frost & Sullivan will provide CABA with the following deliverables and webinars as requested in the RFP. The outline of report and content will be created once the steering committee is formed and the project is formally kicked off.

Reports, Presentations and Data	Webinars
Delivery of six (6) draft documents in a format that CABA will provide, including the following: (1) Full report (Microsoft Word format) (2) Executive summary (Microsoft Word format) (3) Full report presentation (Microsoft PowerPoint format) (4) Executive summary presentation (Microsoft PowerPoint format (5) Raw Data (6) Four (4) or more infographics of key data from the research Delivery of six (6) final documents, including the following: (1) Full report (Microsoft Word and PDF format) (2) Executive summary (Microsoft Word and PDF format) (3) Full report presentation (Microsoft PowerPoint format) (4) Executive summary presentation (Microsoft PowerPoint format) (5) Raw Data (6) Four (4) or more infographics of key data from the research	• One (1) introductory webinar (1 hour) for prospective funders • Kick-off webinar (1 hour) to the Steering Committee to outline the research purpose, scope, objectives, approach, and timelines. The webinar will be hosted and recorded, with contact information of attendees to be shared with CABA. • Regular Steering Committee webinar meetings (1 hour), when deemed necessary (approximately every 3-4 weeks), to communicate; progress, preliminary findings, approvals of research methodologies, and next steps. The webinar will be hosted and recorded, with contact information of attendees to be shared with CABA. • Respond to requests by individual Steering Committee members for additional information via conference or webinar calls. Any new CABA contacts that join Steering Committee meetings or any of the webinars will be provided to CABA (name, email, etc.). • "Final Webinar" (2 hours), provided by the vendor, will be presented to all the funders (unlimited attendance) after the final documents have been delivered. This webinar will be hosted and recorded by the vendor. Contact information of webinar attendees will be recorded by vendor and shared with CABA. Vendor must use the PowerPoint template provided by CABA. • "Organization Webinars" (1 hour) for each organization on the Steering Committee, unlimited attendance per organization. These webinars will be presented after the final documents have been delivered to the funders. Steering Committee members have one (1) month to arrange for these presentations with the vendor. These webinars will be hosted and recorded by the vendor. Contact information of webinar attendees will be recorded by vendor and shared with CABA. • An event presentation(s) on the Research Project will take place following the embargo period. This presentation(s) will take place at one or more industry events, an invite will be provided by CABA. All costs associated with the presentation(s) shall be the responsibility of the vendor. • "Industry Webinar" (1 hour) will be provided following the embargo period. The embargo period ends four (4) months after the Final Webinar. This webinar will be recorded and all contact info (name, email, etc.) of those registered will be shared with CABA. This webinar also includes a 60 second clip promoting the research which will be used for promotional purposes.
• Frost & Sullivan will provide a fully paginated final report to CABA as per CABA's guidelines • All webinar costs will be borne by Frost & Sullivan.	

Scope of Work: Proposed outline of deliverable content

The scope of work as understood from the RFP includes the following. Frost & Sullivan acknowledges that the steering committee will have the ability to collaborate on ratifying the scope at the kick-off stage of the study.

Scope Items	Description
State of Privacy and Cybersecurity in the Home	• Trends and evolutions of privacy and cybersecurity threats and solutions. • An overview of connected devices, systems and current trends in the home. • An outline of the convergence of systems and devices related to the home. • Issues related to security in wired versus wireless home systems. • The role cloud technology plays in connected home privacy and cybersecurity. • The role of service providers (telcos, cablecos and satellite companies). • The balance of security, privacy and functionality. • The key players and emerging players in the industry.
Stakeholder Analysis	• The connected ecosystem and overview of various stakeholders and domains. • The responsibility of privacy and cybersecurity by manufacturers, service providers and end-users. • Evaluations of privacy and cybersecurity risks and solutions for the home owner. • Evaluation of privacy and cybersecurity risks and solutions for home service providers and technology manufacturers. • Perceived security risk versus actual security risks. Role of convergence of systems. • Best practices for preventing and dealing with cybersecurity attacks and privacy concerns. • Detailed examination of consumer behaviors, risk aversion behavior, spending, reliance on alternate solutions, perceptions, cybersecurity issues and challenges.
Best Practices Overview	• Review of current standards and certification processes related to cybersecurity and privacy protection endorsed by the industry: review of gaps and future needs • Current best practices in cybersecurity and privacy protection followed by homeowners, vendors, service providers and partners • Assimilation of best practices to establish base line cybersecurity and privacy measures for each stakeholder group • Cybersecurity framework overview: critical examination of various cybersecurity frameworks currently available for the industry to follow at national and global level to assemble key learning, e.g., NIST, CSA, FCC • Privacy Framework Review: evaluation of currently available guidelines on privacy protection nationally and globally, e.g. “Privacy-by-design”; “International Privacy Implementation Directive”, GDPR
Value Proposition Optimization	• Level of security risk (high, medium, low) and specific strategies to mitigate privacy and security risks at each level of the industry ecosystem. • Risks and rewards of effectively dealing with privacy and cybersecurity issues in the home. • Business case analysis and opportunities for home service providers, technology manufacturers and other industry players. • Devising the ideal-plan-of-action for industry participants: identifying risk, responsibility and accountability for each stakeholder category
Future Direction and Recommendations	• Inhibitors to industry growth. • The growth and progression of the privacy and cybersecurity and the Internet of Things (IoT). • Risk-benefit analysis for various privacy and cybersecurity solutions. • Evolutions of industry standards. • Barriers towards adoptions of privacy and cybersecurity solutions. • Industry awareness of privacy and cybersecurity issues in the home. • Detailed examination of the opportunities that exist for organization in the connected home market.

6 Personnel Biographies

Frost & Sullivan proposes the following project team structure and responsibilities for success of this project.

Project Team Organization		Responsibilities (both for CABA and Frost & Sullivan)
Client Project Steering Committee	Frost & Sullivan Roberta Gamble, Partner Konkana Khaund, Director of Consulting Expert Advisory Panel Dr Ann Cavoukian, Executive Director at Global Privacy & Security by Design Centre, Ryerson College, University of Toronto & Formerly Privacy Commissioner of Ontario Dr Michelle Chibba, Internationally Acclaimed Cybersecurity & Privacy Proponent Jarad Carleton, Global Program Leader, Cybersecurity, Frost & Sullivan	• Provide supervision for the engagement • Approve initiatives • Eliminate roadblocks, facilitate client organization buy-in • Make decisions for engagement progress
Project Lead		
Client Project Steering Committee	Frost & Sullivan Konkana Khaund, Director of Consulting	• Manage day-to-day tasks • Lead creation of deliverables • Monitor progress against plan • Review weekly status
Project Team		
Client Project Steering Committee	Frost & Sullivan Core team Konkana Khaund, Director of Consulting Dr Romualdo Rodrigues, Director of Consulting Seth Cutler, Principal Consultant Maria Benintende, Sr Consultant Pratik Paul, Sr Consultant Other consultants and analysts to be added as required	• Provide deep industry expertise • Offer strategic insights into project planning and conduct research • Produce deliverables and recommendations

Brief Team Member Profiles

The exhibit below provides brief profile highlights of each team member. Detailed bios are provided in the appendix.

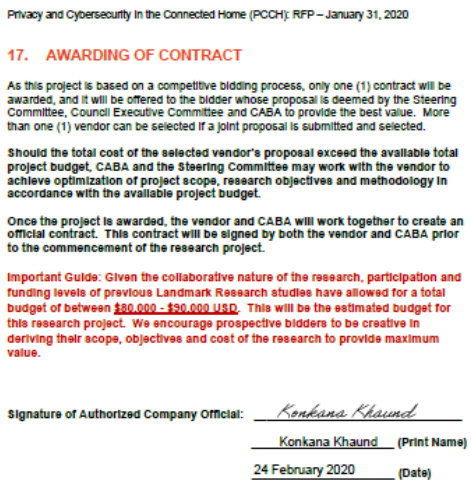
Team Member Credentials	Profile Highlights
Roberta Gamble, Partner & VP Role in this project: Project Supervisor and Quality Assurance Executive	• Over 19 years of consulting experience in energy, home and buildings and power sectors • Extensively involved in the home and building technology, cybersecurity and consumer privacy, power and energy sector, with focus on both traditional and alterative solution markets including Smart homes, connected living, smart buildings, IoT, environmental technologies, and converged industry solutions; renewables, in particular solar and wind industry; T&D markets with a focus on smart grid and metering
Konkana Khaund, Director of Consulting Role in this project: Project Manager and Team Lead	• Over 18 years of experience in research and consulting in home and building technologies, environmental technologies, and urban infrastructure sectors • Extensively involved in smart homes and building solutions, urban infrastructure development, energy management, Internet-of-Things (IoT) and cybersecurity, building automation and control, smart cities, sustainable solutions, energy efficient technologies and solutions, climate technologies, HVACR and lighting
Jarad Carleton, Global Program Leader, Cybersecurity, Frost & Sullivan Role in this project: Expert Advisory Panelist	• Over 20 years of strategy research and consulting for the Fortune 500 and Global 1000 in North America, Latin America, Europe, and Asia Pacific. Expertise in: Cybersecurity; Market Intelligence; Strategic Business Planning; Market Messaging • Industry Expertise: Information & Cybersecurity Technology across multiple industries. A partial list of focus areas: Cybersecurity, Privacy, Digital Trust, Mobile Privacy and Security, Encrypted voice and SMS
Dr Romualdo Rodrigues, Director of Consulting, Consumer Research Role in this project: Team Member, Consumer Research Specialist	• Over 15 years of experience as a quantitative market research and marketing strategy consultant, including hand-on experience on six CABA projects delivered to IBC and CHC • Experience covers consumer and professional industry end user research; brand research – consumer and B2B; advertising and message optimization; product features configuration and pricing optimization; market segmentation and positioning research; predictive modeling; advanced multivariate analysis; choice modeling using various methods (ACBC, CBC, MaxDiff, etc); marketing strategy formulation based on quantitative research insights
Seth Cutler, Principal Consultant Role in this project: Team Member	• Over 11 years of industry expertise, which include research and consulting • Worked in several strategic project in smart homes and buildings, urbanization, econometrics, disruptive technologies and business models; energy efficiency technologies; water and wastewater process and reuse technologies; sustainable developments
Pratik Paul, Sr Consultant Role in this project: Team Member	• Over 10 years of professional expertise, which include market research, advisory, and project management; particular expertise in technology penetration evaluations, sourcing strategy recommendations, connected home, smart cities research; visionary innovation research, analytics and business process implementation • Extensive track-record of leading flagship consulting projects, with in-depth knowledge of key trends and issues affecting the connected industry segments
Maria Benintende, Sr Consultant Role in this project: Team Member	• Consultant in the Energy and Environment team covering Home and Building Management Technologies, with over 10 years of industry experience • Extensively worked in a wide range of sectors including home automation, smart grid and smart buildings, cloud technologies; physical security and surveillance; oil & gas and power; biofuels and renewable; environmental services

Appendix

- **Appendix A – Signed RFP**
- **Appendix B – Sample of Past Research**
- **Appendix C – Team Member Bios**

Appendix A – Signed RFP

The complete signed RFP is send to CABA via email. A snapshot of the signature page is provided here.



Privacy and Cybersecurity in the Connected Home (PCCH): RFP – January 31, 2020

17. AWARDING OF CONTRACT

As this project is based on a competitive bidding process, only one (1) contract will be awarded, and it will be offered to the bidder whose proposal is deemed by the Steering Committee, Council Executive Committee and CABA to provide the best value. More than one (1) vendor can be selected if a joint proposal is submitted and selected.

Should the total cost of the selected vendor's proposal exceed the available total project budget, CABA and the Steering Committee may work with the vendor to achieve optimization of project scope, research objectives and methodology in accordance with the available project budget.

Once the project is awarded, the vendor and CABA will work together to create an official contract. This contract will be signed by both the vendor and CABA prior to the commencement of the research project.

Important Guide: Given the collaborative nature of the research, participation and funding levels of previous Landmark Research studies have allowed for a total budget of between $80,000 - $90,000 USD. This will be the estimated budget for this research project. We encourage prospective bidders to be creative in deriving their scope, objectives and cost of the research to provide maximum value.

Signature of Authorized Company Official: Konkana Khaund

Konkana Khaund (Print Name)

24 February 2020 (Date)

Appendix B – Sample of Past Research

As a sample of Frost & Sullivan's past research, an abridged version of the executive summary of the project "Cybersecurity in the Connected Home" that was undertaken on behalf of the CHC, CABA in 2016 is provided here.

Cybersecurity and the Connected Home

Recognizing the risk, adopting best practices, harnessing the potential

Executive Summary

Project Background and Introduction

The Continental Automated Buildings Association (CABA) is a not-for-profit industry association dedicated to the advancement of connected home and intelligent building technologies. The Connected Home Council (CHC), a core working council of the Continental Automated Buildings Association (CABA), commissioned this landmark research project, titled "Cybersecurity and the Connected Home,"[1] to evaluate the issue of cybersecurity in the context of connected homes, and explore the risks and susceptibilities associated with it. Given that 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, 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. This executive summary offers a concise snapshot of the entire research project in a distilled manner, concentrating on the high-level and critical aspects of the findings. For easy reference, the key sections of the executive summary correlate to individual chapters in the body of the main report: chapters 1-5.

Connected homes are a fast-growing market segment, driven by ubiquitous connectivity, smart mobility, and the Internet of Things (IoT). However, the emphasis on connectivity and convenience to enrich consumer lifestyle experiences has exposed the connected home environment to the increasing incidence of cyber threats. This research confirms growing consumer concerns about connectedness and the critical need for industry participants to counter skepticism with an actionable strategy combining secure solution development and deployment practices, organizational and industry-led best practices, and, more importantly, an ongoing plan for mitigating cyber threats for their businesses and end customers.

CABA and Frost & Sullivan hope this report will drive attention to this key industry challenge and encourage effective dialogue among industry participants for creating awareness and exploring collective initiatives for addressing cybersecurity.

About the Report

CABA commissioned Frost & Sullivan to undertake this research project on behalf of the Connected Home Council (CHC), a working group of CABA. The project was funded by CABA and members of the CHC to understand the state of cybersecurity vulnerabilities in the connected home and its impact on industry participants. The research commenced in November 2015, was conducted over an 18-week time period, and completed with a final webinar session mid 2016.

The outcomes of this collaborative research offers insights into the extent of risk perceived within the connected home, potential counter measures and best practices that are being adopted to address this growing concern by industry participants. The findings will help vendors and service providers to consider better incorporation of cybersecurity measures into their value proposition to build consumer confidence on their products and solutions. The report will also help drive focus and awareness to this pertinent industry issue, as well as, aspects of consumer privacy and protection that needs factoring into countermeasures and policy. The complete report is available for the project funding members only.

Role of the Steering Committee

The Steering Committee represents a cross-section of vendors, service providers, industry associations, utilities, and experts in the connected home, automation, and smart devices marketplace. Representatives from each organization joined Frost & Sullivan and CABA on regular collaboration calls to guide the research scope and ensure that it met project objectives. Figure ES 1 shows the 11 companies and organizations that supported the project as Steering Committee members and funders.

Figure ES 1: Project Steering Committee and Funders

Overview and Focus Areas

Connected homes are prime examples of innovative applications of technology meant to enable enriched lifestyle experiences for consumers, and have made significant market progress in recent years. This progression has enabled a host of smart experiences for consumer–energy management, interactive home devices, connected appliances and real time security solutions, among other experiences. However, this step forward has also allowed unprecedented access to a variety of service providers, thus, opening the home to potential vulnerabilities of cyberspace. The pervasiveness of technology means that the expanded ecosystem of all suppliers, service providers, and the consumer, will share in the burden of dealing with post event casualties in a cyber attack.

Despite reservations surrounding connectedness, there is no doubting the emerging and fast growing market of connected homes as it expands to include connected living, combining connected home, workspace and the city. The ability to address the issues around cyber risks and vulnerabilities will ultimately determine whether or not industry participants can successfully respond to this threat, and also pursue their respective business strategies within this growing market. 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

Key Objectives

The key objectives of the research encompassed the following:

- **Assess Potential of Risk:** Extent of the threat; implications for stakeholders; awareness and perceptions of the threat; shared impacts and responsibilities
- **Evaluate Adequacy of Response:** Adequacy of cybersecurity built into current solutions; responsibility sharing; relevance of standards, regulations, and training
- **Create an Optimal Value Proposition:** Best practices in risk profiling and mitigation; internal challenges in cybersecurity initiatives, compliance, and cost of inaction
- **Chart Implementation Path:** Incorporation of cybersecurity elements; awareness creation, standards development; and roadmap projection

Methodology

Frost & Sullivan used a combination of primary and secondary research methodologies to compile information for this project. This included both qualitative research and quantitative tools for analysis and projection of key issues.

Primary Research Process

Primary research formed the basis of this project, with two major components: an industry-focused research module and a consumer research module. The description of each is provided below in Table ES 1.

Table ES 1: Primary Research Methodology Description

Component	Organization/Entity	Interviewee Profile	Interview Sample Target	Interview Technique
Industry-focused Primary Research *Group A*	Cconnected home solution manufacturers, product and service integrators, managed service and third-party service providers, over-the-top (OTT) service providers, utilities, agencies/associations	Solution developers, research and development specialists, chief technology officers, product and sales management staff, chief engineers, technology architects, utility personnel, association heads	n=45-50	Analyst interviews with industry stakeholders
Industry-focused Primary Research *Group B*	Cybersecurity-related industry participants, information technology (IT) and Internet security solution providers	Research and development specialists, chief technology officers, product and sales management staff, alliance partners, third-party service personnel	n=25-30	Analyst interviews with industry stakeholders
Industry-focused Primary Research	Research institutes, government regulators, compliance enforcement bodies, not-for-profit organizations involved in	Academic experts, technical committee heads, privacy commissioners,	n=15-20	Analyst interviews with industry stakeholders

Group C	consumer protection and privacy, others as required	administrators, policy heads		
Total Sample Target			**n=85-100**	
Interviews Accomplished (Average Across Groups A, B, and C)			**77 percent**	
Consumer Research	Residential consumers	Consumers of connected home solutions (qualified using a preset criteria) in the United States (U.S.) and Canada	n=1,263 U.S.-84 percent Canada-16 percent	Consumer survey using online panels

Frost & Sullivan adopted extensively structured and high-profile discussion techniques with target participants for the industry-focused primary research, involving single or multiple senior level personnel and Frost & Sullivan's team of analysts and consultants to engage in insightful deliberations on the subject. This resulted in maximum value output in terms of information exchange and excellent validation of findings from the consumer research survey. Similarly findings of the consumer survey were triangulated with insights from the industry-focused primary research process.

Research Instruments: Questionnaire/Discussion Guide

The discussion guides for both modules of the primary research process were developed by Frost & Sullivan in consultation with the steering committee. Draft discussion guides were reviewed at the early stages of the project and feedback was mutually exchanged between the project team and the steering committee. Thereafter, the discussion guides were run through a soft launch process for market testing. Subsequently, the two research modules were launched. The sample for both research modules were generated using Frost & Sullivan's vast repository of contact sources and databases. The industry-focused primary research accomplished an average 77 percent fulfillment of the target sample. The data obtained from these discussions were analyzed and distilled into the commentary of the report. The online consumer survey was launched and remained active for a period of six weeks in the field. A total of 1,263 responses were collected against an original target of 1,200. The data from these responses were then analyzed using various qualitative and quantitative tools for interpretation in the report.

Secondary Research

Secondary research comprised the balance of the research effort and included published sources such as those from government bodies, think tanks, industry associations, Internet sources, the CABA Research Library, and Frost & Sullivan's repository of research publications and decision support databases. This information was used to enrich and externalize the primary data. A listing of all works cited is in the appendix. References are cited on the first instance of occurrence. Dates associated with reference materials are provided where available.

Any reference to "Frost & Sullivan's research findings, industry interactions, and discussions" in this report is made in the context of primary research findings obtained from this project "Cybersecurity and the Connected Home," unless otherwise stated. However, the analysis and interpretation of data in this report are those of Frost & Sullivan's consulting team.

Definitions and Consumer Survey Qualification Criteria

For the purpose of this research, a connected home is defined as "a residential environment where owners/occupiers use smart devices, appliances, communication features, controls, centralized hubs, and other functionalities that are enabled by information technology that anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment, among other functions."[2] This definition helped in defining a rapidly evolving concept with a broad stroke, thus providing study participants a degree of flexibility in envisioning and discussing it. Based on this definition, the connected home landscape encompasses participants from all leading product and solution categories, including integrated platforms, connected home devices, smart phones and tablets, home controls, security products, media, telemetry, entertainment, energy management, mobility, network technologies, utilities, and IT and Internet security technologies.

Participants in the consumer survey were offered the same definition of a connected home; however, for easy understanding and screening purposes, a battery of screening questions was asked as part of the qualification criteria before allowing them to proceed with the survey. The respondent screening and qualification process entailed the following qualifiers:

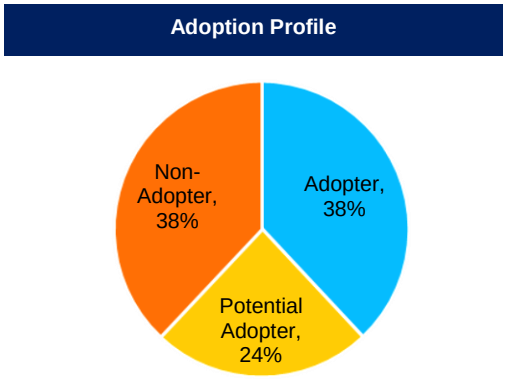
- Had to be 18 years or older
- Had Internet access
- Resided in either the U.S. or Canada
- Played a role in the decision-making process for investments in connected home solutions, consumer electronics, and communication technologies

Qualified respondents were further categorized by the following:

- Geographic distribution—urban, suburban, rural
- Type of dwelling unit—detached, semi-detached, townhouse, apartment, condominium
- Adoption profile—adopters, potential adopters, non-adopters

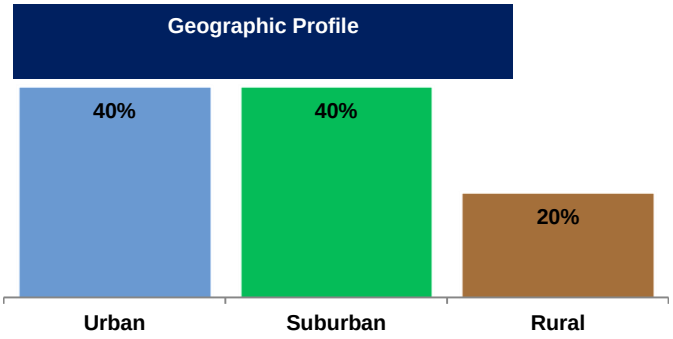
Figures ES 2 and ES 3 respectively show the sample's adoption profile and geographic distribution.

Figure ES 2: Adoption Profile of the Sample



Q: N/A; Profile derived from classification questions. (n=1263)

Figure ES 3: Geographic Distribution of the Sample



Q: Please select the option that describes your geographic location of residence. (n=1263)

Layout of the Report

The report is structured into five chapters with an executive summary outlining the overall objectives, research areas and findings, Chapters 1-5 and an appendix. Table ES 2 provides a brief layout of the report to help navigate its contents.

Table ES 2: Cybersecurity and the Connected Home: Layout of the Report

Sections	Title	Content
Preface	Executive Summary	Background and Introduction; Objectives, Methodology and Definition, Overview of Top Findings
Chapter 1	Cybersecurity and the Connected Home–An Overview	Introduction to the Concept of Connected Homes; Influence of IoT; Issue of Cybersecurity and its Implications; Current and Potential Threat Scenario; Measures and Options for Stakeholders; Balancing Functionality and Cybersecurity
Chapter 2	Consumer Perception Analysis	Introduction and Methodology, Sample Classification; Adoption Potential Analysis; Consumers' Benefits and Concerns; Expectations from Vendors and Service Providers; Cybersecurity Protection-Adequacy Review; Key Takeaways
Chapter 3	Review Cybersecurity Domain Issues	Issues and Challenges in Cybersecurity Adoption; Core Issues-legislation, standards, certifications, design processes; Cybersecurity Framework; Consumer Privacy
Chapter 4	Optimal Cybersecurity Value Proposition	Rational Risk Evaluation; Interdependency in Risk Sharing; Best practices for Stakeholders; Cybersecurity Response Plan
Chapter 5	Conclusions and Recommendations	Conclusions of the Research; Key Recommendations; Next Steps in Implementation
Addendum	Appendix	Glossary of Terms; References; Consumer Research Discussion Guide

Summary of Key Findings

The key findings of this research as discussed through Chapters 1-5 are outlined subsequently. Discussion under each heading represents a synopsis of the chapter corresponding to it in the report. For example, ES-CH 1 corresponds to executive summary of Chapter 1.

ES-CH 1Cybersecurity and the Connected Home–An Overview

The Evolving World of Connected Homes

Defining the Connected Home

The concept of a connected home is defined as follows: “A residential dwelling unit that uses both technology and processes to create a smart environment that is safe, responsive, adaptive, and comfortable for its occupants.” This definition was adopted through Frost & Sullivan’s interactions with the connected home industry for this research, and builds upon previous Frost & Sullivan and CABA projects in the connected home arena.

Expanding on this definition, a connected home is characterized by the presence of devices, communication services, and applications that interconnect and communicate with one another to enable an environment that is responsive and adaptive to the consumer’s needs and comforts. Such communication helps occupants make intelligent decisions regarding a connected home’s functions, both at the present moment, and to dictate such functions at a future time.

The degree of connectedness varies by the sophistication of the connected network that is ultimately the backbone of this evolving concept. The connected home has a wide scope, from one or more personal devices connected to a home area network to a comprehensive, home-wide integrated platform that eliminates all silos. Over the last decade, a simply automated or digitally advanced home environment has progressed into a communication-rich living space. Functions such as energy management, media and entertainment, and home security gained early acceptance with the concept of home automation. The incorporation of connectivity into these automated or digital components significantly changed the demand dynamics, enabling users to manage multiple aspects of the home and their lifestyle from any location.

The Connected Home and IoT

The connected home embraces both an internal and external communication network. The overlay of smart devices with an IP network neutralizes the complexities of navigating the internal and external networks of the connected home. IoT, in simple terms, refers to connecting smart devices or machines, with sensor-aided intelligence, to the Internet. Activities centering on IoT are delivering increasingly unique advantages and novel challenges. Advantages include real-time access, vast data generation and analytics, and interconnectivity of devices, applications, and platforms to support interdependent functions. These advantages by themselves, however, offer little value unless the data and networks are simultaneously shared, thus permitting access to multiple service providers to tap into a connected home’s network, systems, and devices. This unprecedented access is where cyber risks in the connected home originate.

Figures ES 7 and ES 8 provide a list of best practices for industry participants to pursue in addressing cybersecurity.

Figure ES 7: Best Practices: Vendors and 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

Figure ES 8: Best Practices: 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

ES-CH 2 Consumer Perception Analysis

The consumer research survey provided important insights into the overall state of the connected home market, the extent of penetration of connected devices and solutions, the future potential of these devices, and, above all, the impact of a connected lifestyle on increasing consumers' exposure to cyber risks. The top findings and strategic messages that can be drawn from the survey are highlighted below in Figure ES 9.

Figure ES 9: Top Consumer Research Findings and Messages

Significant Market Potential

- Connected homes represent a fast-growing market, with **38 percent** of homes in North America as **adopters**; another 24 percent is aspiring to be adopters within two years.
- Market penetration of major products is less than 20 percent (security, entertainment, etc.) and represents **potential to grow** by **15–20 percent** within the next two years.
- Connected home technologies are increasingly exposed to cyber risks with the breadth of devices that need to be secured.

High Incidence of Cyber Breaches

- In the past three years, 62 percent of adopters have experienced a cyber breach; 29 percent of adopters experienced cyber breaches over the last 12 months.
- Adopters are about **2-times more likely** than potential adopters and **3-times more likely** than non-adopters to have experienced cybersecurity incidents.
- Adopters' need for cybersecurity support is growing with the acquisition of additional connected devices and solutions.

Growing Mix of Connected Devices

- Adopters use **a broader mix of connected devices**, with an average of **at least five** devices.
- They also have higher confidence in the security of devices to control their connected home.
- Because this confidence reinforces their willingness to use more devices, the need to protect adopters from the cyber vulnerabilities becomes more pressing.

Increased use of Cybersecurity Measures

- **Adopters use** more firewalls and **a broader set of measures** to protect their homes from cybersecurity risks.
- Among adopters, **66 percent use firewalls and install timely anti-spyware** and security updates.
- Only **42 percent of adopters** had **insurance cover** for cyber risks.
- They also proactively asked vendors and service providers about risks and ways to mitigate them. This characteristic can be leveraged to offer comprehensive cybersecurity solutions.

Inadequate Cybersecurity Protection from Vendors

- Opinions were divided regarding the adequacy of cybersecurity protection from vendors.
- Among adopters, **30 percent felt the protection was inadequate.**
- Adopters perceived home security service providers and home automation specialists to be the most-trusted providers of cybersecurity.
- These channel preferences could serve as a basis to **formulate a multi-channel or multi-vendor strategy** to efficiently promote cybersecurity solutions for connected homes.

ES-CH 3Review Cybersecurity Domain Issues

Addressing cybersecurity concerns involves navigating a myriad of critical issues and challenges for all stakeholders involved. On one end of the spectrum are consumers, whose propensity for a connected lifestyle warrants growing risk. The process of minimizing these risks entails efforts by consumers and the ecosystem of connected home vendors and suppliers that are responsible for potentially increasing that risk. The measures that consumers can adopt to secure their devices and connected network are far simpler. However, their successful implementation depends largely on the ecosystem of stakeholders being able to successfully adopt their share of cybersecurity measures, and creating products and solutions that offer the assurance of cybersecurity to the consumer. In this regard, some key issues and challenges for the industry stakeholders are shown in Table ES 3.

Table ES 3: Cybersecurity Domain Issues and Challenges

Issues	Challenges	Impact
Incorporating cybersecurity into product design	• Anticipating the severity of cyber attacks • Pre-empting the sophistication of hackers • Evaluating the unknowns	• Ongoing trial and error process • Ample scope for adversaries to win • Uncertainty of guaranteeing cybersecurity • Declining consumer confidence
Technical ability and innovation	• Keeping pace with technology advancements • Maintaining a qualified resource pool • Keeping up with latest malware and other malicious instruments	• Ill-equipped technology • Mismatch of technical improvements and security requirements
Cybersecurity investment	• Proving the business case • Incorporating it into the business plan • Discounting the importance of best practices	• Remain behind the curve in secure system development • Recipe for product failure • Revenue loss; negative brand image
Cybersecurity outsourcing	• Limited control over processes and outcomes • Cost implications	• Compliance issues • Lack of accountability
Standards and protocols	• Insufficient cybersecurity-focused elements • Broad framework • Takes years for development and testing	• Frequently overlooked or not applied fully • Compliance cannot be enforced
Certification	• Consensus on elements to certify • Multiple efforts can create confusions	• Enforcement difficulties • No accountability for not being certified
Regulation and policy	• Takes years to develop • Biased towards certain stakeholders • Lack of comprehensive safeguards	• Loopholes allow sub-standard practices • No safeguards for victims
Education and training	• No institutionalized options • Training costs can be a deterrent	• Workforce lagging behind in knowledge of cybersecurity

Incorporating Cybersecurity into Product Design

Product design has been cited as the root cause of cybersecurity vulnerabilities for the connected home. Inadequate cybersecurity built into the design, in a bid to hasten the time to market, has been a major contributing factor in system breaches, as corroborated by this research. However, this also creates a far bigger issue in that, these products will always struggle to combat cyber threats in terms of their design capability.

Technical Ability and Innovation

Keeping pace with cyber threats implies that vendors and service providers must continue to enhance their technical capabilities and expand on innovations to address cyber threats successfully or, at the very minimum, offer the

consumer an assured level of protection against major losses. This is incumbent upon an organization's technical resource pool, and the importance of keeping it updated with increasingly qualified manpower.

Cybersecurity Investments

Cybersecurity-focused business units are a relatively new phenomenon in most organizations. It is often challenging for these personnel to secure proper investments to launch company-wide cybersecurity initiatives, including product hardening and testing processes. Proposing cybersecurity investments is often met with criticism and delayed responses from management. This challenges the adoption and implementation of key best practices that could otherwise allow the organization to offer secure products and solutions to their consumers.

Cybersecurity Outsourcing

Where in-house resources and investments may prove challenging, outsourcing cybersecurity tasks to third party specialists will offer organizations plausible ways of building cyber resilience. For mid-sized, and start-up organizations, this route to adopting cybersecurity processes may prove to be more feasible in the short run, as opposed to incurring upfront investments to set up their own cybersecurity task forces and processes. However, the option does come with challenges in terms of inability to enforce compliance on third parties, or limited accountability of these entities in dealing with breach-related events.

Standards and Protocols

This is an area of the connected home industry that is rife with activity. There are a multitude of standards and protocols that connected home technologies are developed on, and compatible with. Ubiquitous connectivity and the need for interoperability demand that solutions work with various standards and protocols. However, cybersecurity adds a layer of complexity to this issue, as this would require minimum common standards for cybersecurity compliance built into the various standards and protocols. This would require consensus building across numerous technology alliances and standards bodies to ensure that prescriptive cybersecurity requirements are codified into these standards.

Regulations and Policy

Regulation and policy is a domain issue that will generate considerable interest and ongoing debate. Cybersecurity legislation and rule making is at the preliminary stages in North America.[3] So far, the various bills that have been introduced have met with vehement criticism, and broadly lack the framework for comprehensively addressing cybersecurity.

Education and Training

There is a lack of proper institutionalized cybersecurity training programs for organizations to improve their knowledge and skill sets. Training costs can also be prohibitive. This discourages technical personnel, installers and service providers from availing of such training, unless the organizations they are affiliated with incur the expense, thus resulting in under qualified processionals.

ES-CH 4Optimal Cybersecurity Value Proposition

In evaluating an optimal value proposition incorporating cybersecurity, the following elements need to be considered: the rational evaluation of risk; the interdependency in risk sharing; the best practices to adopt against cyber threats; and finally a comprehensive and appropriate response plan.

Rational Risk Evaluation—Actual versus Notional Risks

Understanding cyber risks in the connected home space calls for the delineation of actual risks from notional ones. While it is common for the industry and consumers to define risk with a broad stroke, not all risks identified within the connected home domain should be classified with the same intensity. Consumers' lack of awareness in evaluating

risks often leads them to worry about benign risks instead of the more dangerous ones requiring greater focus and priority. To analyze this issue, a select group of popular connected home devices were rated for their actual versus notional risks, both from a consumer and industry standpoint[4], as shown in Table ES 4.

Table ES 4: Connected Home Cyber Risks: Actual versus Notional

Connected Home Technology	Notional Risk	Actual Risk
Smart Thermostats/Home Energy Management	**Easy to hack; device data loss; personal information loss; access to other systems**	Temporary system failure/remote access denied if hacked; usually no compromise of personal data
Security Cameras		Major compromise of personal information including video feeds
Home Monitoring		Temporary system failure; access to other systems; low possibility of personal data breach
Smart Meters		Easy to hack; minimal access to other systems; low risk of personal information loss
Media and Entertainment		Compromise of personal information if hacked; temporary failure

Consumer awareness of what is really at stake will help instill confidence in connected home systems, and, subsequently, in service providers and vendors. Based on this, vendors can also determine the level of device security and attention to consumer privacy and data security they need to commit to. However, this does not imply that a less risk-prone device needs less protection. Adding security and privacy into design by default is a practice that needs to be adopted, no matter the degree of vulnerability and subsequent damage associated with the compromise of a particular system or device. The takeaway here clearly is “plan for the worst.”

Cybersecurity Response Plan

The response plan for connected home vendors and service providers in dealing with cybersecurity will encompass crucial elements targeted at recognizing the risks, creating remedial methods, extending those methods to work with partners and the internal organization, training, and collaborating with industry peers to plan for contingencies.

Recognizing Ownership and Accountability

Recognizing and acknowledging the risks that vendors’ own systems and services can be subject to within the connected home environment, either through inherent glitches or through breaches in other participants’ systems and services, is crucial. With that acknowledgement comes the shouldering of accountability. Proactive damage assessment and planning for restoration that will be required for consumers, partners, as well as partners’ organizations should be charted out.

Independent Evaluation of Partner Processes

Putting processes in place to conduct partner scrutiny is a critical step. Proper security planning for testing products and components from third parties, developing guidelines for partners to follow, and creating checks and balances to ensure process compliance are key elements of this exercise.

Enterprise Initiatives, Training, and Documentation

Enterprise initiatives would involve incorporating periodic security audits to ensure that measures are followed correctly by product, R&D, and other internal teams, in addition to checking partners' security measures. Incorporating training modules are necessary to ensure that teams are up to date on the latest cybersecurity procedures, codes, and other compliance mechanisms.

Industry Collaboration and Contingency Planning

Planning for cybersecurity is a gradually unfolding process for all ecosystem participants in the connected home industry. Given the fact that every participant is engaged in creating their own action plan, it would tremendously help participants to come together in planning for contingencies for the industry as a whole. While it is expected that this may not be willingly agreed to, given the sensitive nature of the cybersecurity strategy that organizations are adopting, there are broad principles that can be deliberated upon and planned together for mutual benefit.

ES-CH 5Conclusions and Recommendations

The top findings of this research validate some of the early hypotheses around the nature and causes of cybersecurity risk within the connected home, and the triggers that aggravate it to reach unmanageable proportions. If not addressed appropriately and timely, the growing concerns and loss of consumer confidence in connected solutions could impede market growth. Education and awareness creation will help drive focus to the right practices that both consumers and the industry can adopt to address cyber risks.

The key recommendations of this research include following:

- Secure solutions and services by designing security and privacy as defaults
- Engage with consumers to offer product security knowledge, educate them on secure practices and general cybersecurity safeguards
- Examine partner strategies, lay down stringent guidelines and expect satisfactory compliance before embedding their solutions
- Pursue enterprise cybersecurity initiatives, incorporate advice of cybersecurity champions
- Collaborate on industry initiatives around education, training, standards and policy

Appendix C – Team Member Bios

Roberta Gamble, Partner and VP,

Frost & Sullivan, North America

Functional Expertise:

Over 19 years of consulting experience in energy, home and buildings and power sectors including:

- Third-party business plan verification
- Acquisition target research and due diligence
- Geographical expansion strategy
- New market exploration

Industry Expertise:

Fifteen-plus years in the home and building technology, power and energy sector, with focus on both traditional and alterative solution markets including:

- Smart homes, connected living, smart buildings, IoT, environmental technologies, and converged industry solutions
- Gas and steam turbine markets, as well as power plant services markets
- Generator sets and other distributed generation solutions
- Renewables, in particular solar and wind industry
- T&D markets with a focus on smart grid and metering

What I bring to the Team:

Years of industry contacts and connections, understanding market trends from the participant's point of view

- Extensive client interaction and strategic project management
- Oversight of a diverse and global team of analysts and consultants
- Fluent in Italian
- Oft quoted and interviewed in national publications including the New York Times, Chicago Tribune, and NPR

Career Highlights:

- Director of Frost & Sullivan Building Technology, Energy and Environment business unit since 2006, analyst and management roles since 2000
- Previous related experience at Siemens Power Corporation
- Long term client relationships with major industry players, including
    - CABA
    - GE
    - Caterpillar
    - Cummins
    - Schneider Electric

Education:

Bachelors in International Studies and in Economics from University of Wisconsin, Milwaukee

Konkana Khaund, Director of Consulting, Energy & Environment

Frost & Sullivan, North America

Functional Expertise

Over 18 years of experience in research and consulting in home and building technologies, environmental technologies, and urban infrastructure sectors, covering:

- Management and supervision of global research on connected homes and intelligent buildings, urban infrastructure and smart cities
- Markets, Technologies and Industry Research , including market commercialization prospects and best practices
- Project feasibility studies, acquisition target research and due diligence
- Geographical expansion strategies and new market exploration

Industry Expertise

Seventeen plus years in the energy, environment and building technology sectors, with focus on both traditional and sustainable solutions including:

- Smart homes and building solutions, urban infrastructure development, energy management, connected homes, cloud technologies, Internet-of-Things (IoT) and cybersecurity, building automation and control, smart cities, sustainable solutions, energy efficient technologies and solutions, climate technologies, HVACR and data centers
- Water and waste water, waste management and remediation, environmental quality solutions
- Emerging segments such as carbon markets, capture technologies, environmental monitoring and diagnostics
- Associated service markets and vertical industry segments
- Thought leadership promotion through active participation in industry association-led activities and collaborative research programs

What I bring to the Team

- Long standing industry association, understanding of market trends and behaviour from stakeholder's viewpoint
- Extensive client interaction experience, including strategic project execution and management
- Broad perspective of people, regions and industry sectors with work experience in North American and Asia
- Frequent presenter at major industry events such as Smart Grid Modernization Summit – Connected Homes think tank, Intelligent & Green Buildings Summit, Realcomm, Niagara Summit, Growth Innovation & Leadership Conference (Frost & Sullivan), leading industry webinars and forums
- Often featured, quoted and interviewed in national publications and newswires such as Bloomberg, the Wall Street Journal, CNN.com, Business Week, Forbes.com San Francisco Chronicle, Green Biz, Associated Press, New York Times and Chicago Tribune
- Serves on the advisory board of Realcomm/IB-Con ; member of the Intelligent Integrated Buildings Council, the Connected Home Council and White Paper Committee of the Continental Automated Buildings Association

Career Highlights

- Industry Manager with Frost & Sullivan's Energy & Environment Practice since 2011; Sr. Industry Analyst and Program Manager with the same practice from 2008-10; Research Analyst, Building Technologies, 2006-08
- Senior Consultant with CBRE South Asia Pte Ltd as core member of the Strategic Consulting Group, 1998-2005
- Established relationships with major industry players and organizations, including Philips, GE, Schneider Electric, Emerson, Cisco, Intel, AT&T, Samsung, IBM, Ingersoll Rand/Trane, Johnson Controls, Siemens Building Technologies, United Technologies Corporation, Honeywell, US Green Building Council, Continental Automated Buildings Association, Realcomm.

Education

- Masters Degree in Economics (Specialization – Econometrics and Development Economics); BA – Economics (Hons), Delhi University, India

Jarad Carleton, Global Program Leader, Cybersecurity

Information & Communication Technologies, Frost & Sullivan

Functional Expertise

- Over 20 years of strategy research and consulting for the Fortune 500 and Global 1000 in North America, Latin America, Europe, and Asia Pacific. Expertise in:
- Cybersecurity
- Market Intelligence
- Strategic Business Planning
- Market Messaging

Industry Expertise

- Information & Cybersecurity Technology across multiple industries. A partial list of focus areas:
- Cybersecurity, Privacy, Digital Trust
- Mobile Privacy and Security
- Encrypted voice and SMS

What I bring to the Team

- Leadership for the cybersecurity research practice in Europe
- Global project management and interaction with Sr. executive teams
- Thought leadership that clients use for strategic business planning, shaping market perceptions, and lobbying government to shape national policy
- Direct and effective communicator in-person, in webinars, videos, and with senior executive teams

Career Highlights

- Led high profile strategic projects with leading firms including:
- CA Technologies (Broadcom)
- Segasec
- Secureworks
- Kudelski Security
- Cisco Systems
- WatchGuard
- RSA
- Digicert
- RiskIQ

Education

- MBA – International Management from Thunderbird, School of Global Management, Glendale, AZ
- BA – Psychology from the University of California, Davis, CA
- German A1 Certificate – Goethe Institut, Munich, Germany
- German A2 Certificate – Österreichisches Sprachdiplom Deutsch, Saalfelden, Austria
- Advanced Spanish Language Certificate – Cuauhnáhuac Escuela, Cuernavaca, México

Romualdo Rodriguez, Consulting Director,
Consumer Research Group
Frost & Sullivan, North America

Functional Expertise

Over 15 years of experience as a quantitative market research and marketing strategy consultant, including hand-on experience on **six CABA projects** delivered to IBC and CHC
Experience covers:

- Consumer and professional industry end user research
- Brand research – consumer and B2B
- Advertising and message optimization
- Product features configuration and pricing optimization
- Market segmentation and positioning research
- Predictive modeling
- Advanced multivariate analysis
- Choice modeling using various methods (ACBC, CBC, MaxDiff, etc)
- Marketing strategy formulation based on quantitative research insights

Industry Expertise

Experience in quantitative market research for the following sectors and categories

- Brands of Fortune 500 companies
- Global research for automotive, transport, energy, technology, healthcare sectors
- Above-brand research to uncover category drivers

What I bring to the Team

- Ability to leverage experience with automotive and transport market in particular
- Ability to bridge business objectives and quantitative research objectives
- Ability to provide relevant marketing strategy framework and analytics framework.
- Ability to apply creativity and innovation to both research design and research presentation.
- Ability to derive and integrate key insights at a strategic level.

Career Highlights

- Strategist, Quantitative Research, In-Sync
- Director, Advanced Analytics, Customer Research, Frost & Sullivan

Education:

- Ph.D. in Business Administration (focus: Business Strategy)
- Master in Business Administration
- BSC Marketing Management
  - AB Behavioral Science (minor: Sociology)

Seth Cutler, Principal Consultant, Energy & Environment
Frost & Sullivan, North America

Functional Expertise

Over 10 years of industry expertise, which include research and consulting, with particular expertise in:

- Smart Homes And Buildings, Urbanization, Econometrics,
- Disruptive technologies and business models
- Energy Efficiency Technologies
- Water and wastewater process and reuse technologies
- Sustainable Developments

Industry Expertise

Experience base covering broad range of sectors, leveraging long-standing working relationships:

- With leading industry participants' senior executives of connected homes and buildings supply chain
- Utilities, Municipal and Urban Development
- Industrial Water and Wastewater Treatment -process and reuse technologies in home and buildings, and industrial segments; IoT enabled smart water environment
- Sustainable developments and cities with technology converge and IoT

What I bring to the Team

- Strong focus on Mega Trends and disruptive technologies
- International professional experience
- Stakeholder engagement
- Analytical focus

Career Highlights

Extensive expertise in the consulting industry including:

- Principal Consultant with Frost & Sullivan's Energy and Environment Team, 2012-Present
- Associate Consultant with Frost & Sullivan's Energy and Environment Team, 2011
- Consultant with CEB, Arlington, Virginia, 2009-11
- Associate with Regeneris Consulting, London, England, 2008
- Analyst with London East Research Institute, London, England, 2007-08

Education

- MA Cities, Culture & Social Change from King's College London, England
- MA Human Geography from the University of St Andrews, Scotland

Pratik Paul, Principal Consultant, Energy & Environment

Frost & Sullivan, North America

Functional Expertise

- Over **10 years** of professional expertise, which include Market Research, Advisory, Business Development and Project Management; Particular expertise in:
  - Market Research and Sourcing Strategy recommendations
  - Connected Home; AI & ML; Visionary Innovation Research
  - Analytics and Business Process Implementation

Industry Expertise

- Experience base covering a broad range of sectors, leveraging long-standing working relationships with leading participants in the following industries
  - Artificial Intelligence (AI), Machine Learning (ML), Connected Homes, IoT and the Embedded Ecosystem
  - Temperature Controls, transportation and logistics, thermal power plants and associated buildings
  - Industrial Durables (Metal Products and Injection-Molded Plastics) across multiple industries
  - High-Technology and Discrete Manufacturing

What I bring to the Team

- Strong ideation skills backed by analytical ability
- Data-driven approach to provide focused information and solutions
- Wide experience in managing large scale connected home research projects
- Vast knowledge of the smart and connected technology solutions markets and its opportunities and challenges
- Close relationships with key stakeholders in connected home and digital transformation industry segments

Career Highlights

- Extensive expertise in Market Research, Advisory, Project Management and Bid-Management functions in the following firms.
  - Continental Automated Buildings Association
  - Consumer Technology Association
  - The CSA Group
  - Emerson
  - Philips Lighting
  - Larsen and Toubro Ltd.
  - Infosys BPO Ltd.
  - Beroe Inc.

Education

- Masters in Business Administration from Symbiosis International University, Pune, India
- Bachelors in Technology from Amrita University, Coimbatore, India