CABA™

Cybersecurity and the Connected Home

RECOGNIZING THE RISK, ADOPTING BEST PRACTICES, HARNESSING THE POTENTIAL

EXECUTIVE SUMMARY

CABA AND THE FOLLOWING CABA MEMBERS FUNDED THIS RESEARCH:

EMERALD FUNDERS

American Family Insurance · Consumer Technology Association · CEDIA · hydro one · Intermatic · Leviton · Pella · Schneider Electric · Southern California Edison

DIAMOND FUNDERS

Honeywell · Hydro Québec

Disclaimer

Frost & Sullivan has provided the information in this report for informational purposes only. The information and findings have been obtained from sources believed to be reliable; however, CABA and Frost & Sullivan does not make any express or implied warranty or representation concerning such information, or claim that its use would not infringe any privately owned rights. Qualitative and quantitative market information is based primarily on interviews and secondary sources, and is subject to fluctuations. Connected home products, technologies, and processes evaluated in the report are representative of the market and not exhaustive. Any reference to a specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply an endorsement, recommendation, or favoring by CABA and Frost & Sullivan. Information provided in all segments is based on availability and the willingness of participants to share these within the scope, budget, and allocated time frame of the project. All directional statements about the expected future state of the industry are based on consensus-based industry dialogue with key stakeholders, anticipated trends, and best-effort understanding of the future course of the industry. CABA and Frost & Sullivan hereby disclaims liability for any loss or damage caused by errors or omissions in this report.

About CABA

The Continental Automated Buildings Association (CABA) is an international not-for-profit industry association, founded in 1988, dedicated to the advancement of connected home and building technologies. The organization is supported by an international membership of over 330 organizations involved in the design, manufacture, installation and retailing of products relating to home automation and building automation. Public organizations, including utilities and government are also members. CABA's mandate includes providing its members with networking and market research opportunities. CABA also encourages the development of industry standards and protocols, and leads cross-industry initiatives.

Citation

CABA Cybersecurity and the Connected Home: Recognizing the risk, adopting best practices, harnessing the potential; Gamble, R., Khaund, K., Singh, A., Vetter, S., Rodriguez, R., Wright, M., Continental Automated Buildings Association (CABA); May 2016

Keywords: Connected Home, Home Automation, Cybersecurity, Connected Devices, Internet of Things (IoT), Machine-to-Machine (M2M), Home Energy Management, Smart Home, Cyber Risks, Consumer Privacy, Home Security, Security Breach

Acknowledgements

This study was made possible thanks to the insights and support of the Continental Automated Buildings Association (CABA). The authors wish to acknowledge the support of CABA staff: Greg Walker, Research Director, for his management of the project; Ron Zimmer, President & CEO, for his recognition and promotion of this important topic; and George Grimes, Marketing and Business Development Consultant, for industry connections and fund raising in support of this study.

The Steering Committee contributed their time and industry expertise to the project at numerous Web conference meetings, offline sessions with the research team, and through interim and final review of the research processes, discussion guides, and this extensive report. The organizations and their representatives are:

Steering Committee

American Family Insurance

Ryan Rist, Director of Innovation
Eric Orthey, Innovation Consultant
Lauren Pemberton, Innovation Research Consultant

Consumer Technology Association (CTA)

Steve Koenig, Senior Director, Market Research

Hydro One Networks

Tom Semler, Manager of Conservation and Demand Management

Schneider Electric

Michael Pyle, Vice President of Cybersecurity, Partner Business
Jason Lien, Future Offer Manager, Small Buildings Systems, Partner Business

Pella Corporation

Larry Ehlinger, Director, Advanced Technologies

CEDIA

Dave Pedigo, Senior Director of Learning & Emerging Technologies
Steven Sumners, President and CEO, Sound Insights
Michael Maniscalco, Co-Founder and VP of Consumer Technology Association (CTA) Product, Ihiji

Intermatic Inc.

Elizabeth Jacobs, Vice President of Marketing
Barbara Farrah, Manager, Business Intelligence and Strategic Planning Group

Leviton Manufacturing Company, Inc.

Bob Becker, EVP and General Manager, Residential
Justin Berghoff, Director, Business Development & Product Management, Residential
Aaron Ard, Director, Software Engineering, Security & Automation

Southern California Edison

Jerine Ahmed, Senior Engineer, Design and Engineering Services Group

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

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 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. 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 concept of connected homes and the ecosystem that caters to it has expanded quite rapidly over the last five years. Encompassing players from home automation, security, energy management, information and communication technology, managed services, the utility industry and more, this is a highly evolving landscape of solution providers bringing innovative offerings in connectivity, smart devices, and smart mobility into the home. However, along with the growth in this innovative concept, there is an increasing expansion of cyber breaches, resulting from ubiquitous connectivity, data sharing and third-party access, which has led to risks and vulnerabilities within the connected home.

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 consider better incorporation of cybersecurity measures into their value proposition to build consumer confidence into 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.

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. The organizations that were on the Steering Committee include: American Family Insurance, Consumer Technology Association (CTA), CEDIA, Honeywell International, Hydro One Networks, Hydro-Québec, Intermatic Inc., Leviton, Pella Corporation, Schneider Electric and Southern California Edison. Representatives from each steering committee level 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 organizations that supported the project.

Figure ES 1: Project Funders

EMERALD FUNDERS
AMERICAN FAMILY INSURANCE
Consumer Technology Association
CEDIA
hydro one
INTERMATIC
LEVITON
Pella
Schneider Electric
SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL Company
DIAMOND FUNDERS
Honeywell
Hydro Québec

ABOUT CABA

The Continental Automated Buildings Association (CABA) is an international not-for-profit industry association, founded in 1988, dedicated to the advancement of connected home and building technologies. The organization is supported by an international membership of over 330 organizations involved in the design, manufacture, installation and retailing of products relating to home automation and building automation. Public organizations, including utilities and government are also members. CABA's mandate includes providing its members with networking and market research opportunities. CABA also encourages the development of industry standards and protocols, and leads cross-industry initiatives.

Please visit http://www.caba.org for more information.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation, and leadership. The company's consulting methodologies and strategic partnership initiatives provide clients with disciplined research and best-practice models to drive the generation, evaluation, and implementation of powerful growth strategies. The company leverages 50 years of experience in partnering with Global 1000 companies, emerging businesses, industry associations, and the investment community from over 40 offices on six continents. It collaborates with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. Frost & Sullivan’s integrated value proposition provides support to clients throughout all phases of their journey to visionary innovation including: research, analysis, strategy, vision, innovation, and implementation. The 360o coverage includes industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics, and emerging economies. To learn more, visit www.frost.com.

THE PROJECT CONSULTING TEAM

Frost & Sullivan’s Energy & Environment Group led the research project for CABA, with integral support from Frost & Sullivan’s Customer Research Group. The core consulting team and report contributors are:

Energy & Environment Group, Frost & Sullivan
Roberta Gamble, Partner
Konkana Khaund, Principal Consultant
Aanchal Singh, Senior Consultant

To learn more about Frost & Sullivan’s Energy & Environment Group: http://ww2.frost.com/research/industry/energy-environment

Customer Research Group, Frost & Sullivan
Sascha Vetter, Director of Research Operations
Romualdo Rodriguez, Ph.D., Consulting Director
Max Wright, Consultant

To learn more about Frost & Sullivan’s Customer Research Group:
http://ww2.frost.com/research/customer-research

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 the 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 include 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 encompass 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	Connected 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 Group C	Research institutes, government regulators, compliance enforcement bodies, not-for-profit organizations involved in consumer protection and privacy, others as required	Academic experts, technical committee heads, privacy commissioners, administrators, policy heads	n=15-20	Analyst interviews with industry stakeholders
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:

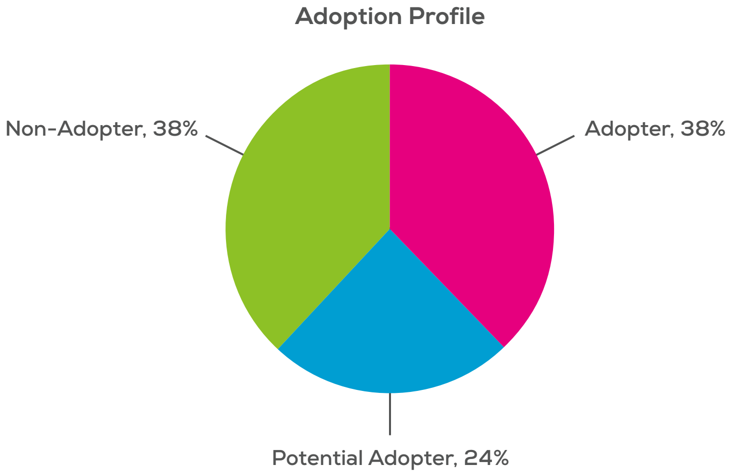
- Had to be 18 years or older
- Had Internet access
- Resided in either the U.S. or Canada
- Played a role in the decision-making process for investments in connected home solutions, consumer electronics, and communication technologies

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

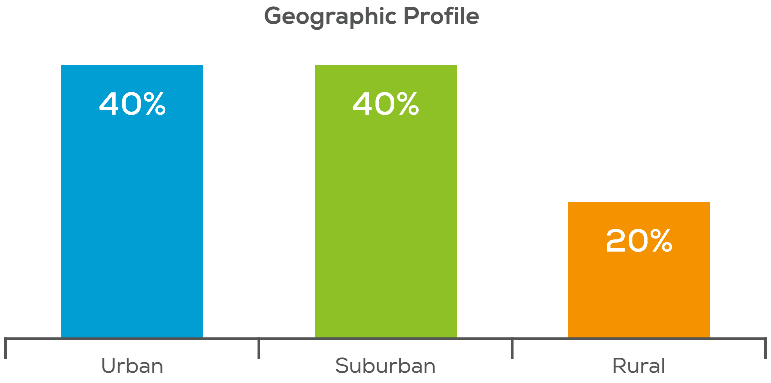
Figures ES 2 and ES 3 respectively show the sample's adoption profile and geographic distribution.

Figure ES 2: Adoption Profile of the Sample



Q: N/A; Profile derived from classification questions. (n=1,263)

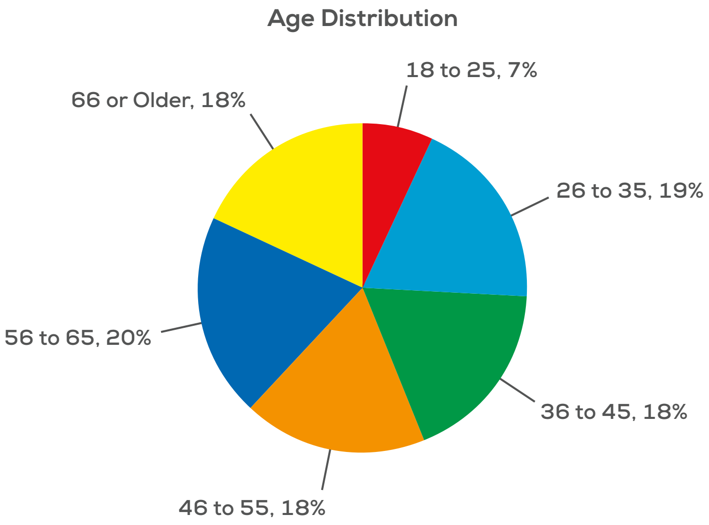
Figure ES 3: Geographic Distribution of the Sample



Q: Please select the option that describes your geographic location of residence. (n=1,263)

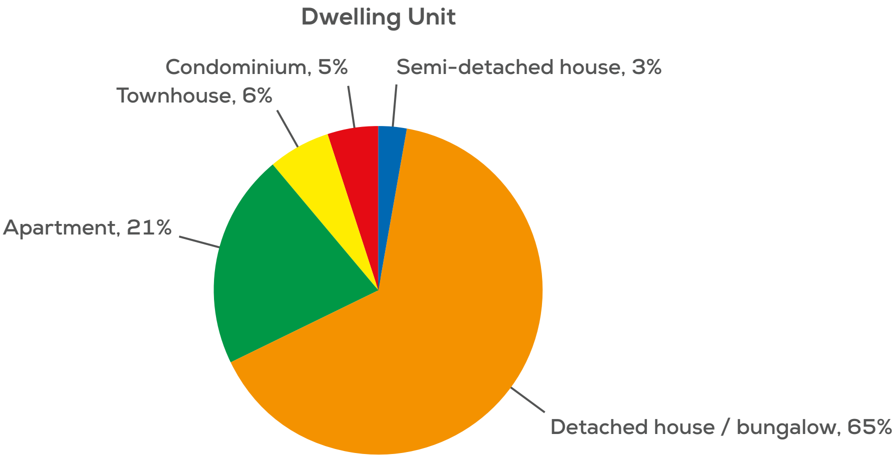
Figures ES 4 and ES 5 respectively show the sample's age distribution and type of dwelling unit.

Figure ES 4: Age Distribution of the Sample



Q: Please select your appropriate age group. (n=1,263)

Figure ES 5: Type of Dwelling Unit of the Sample



Q: Which of the following best describes your dwelling unit type? (n=1,263)

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 1: CYBERSECURITY 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.

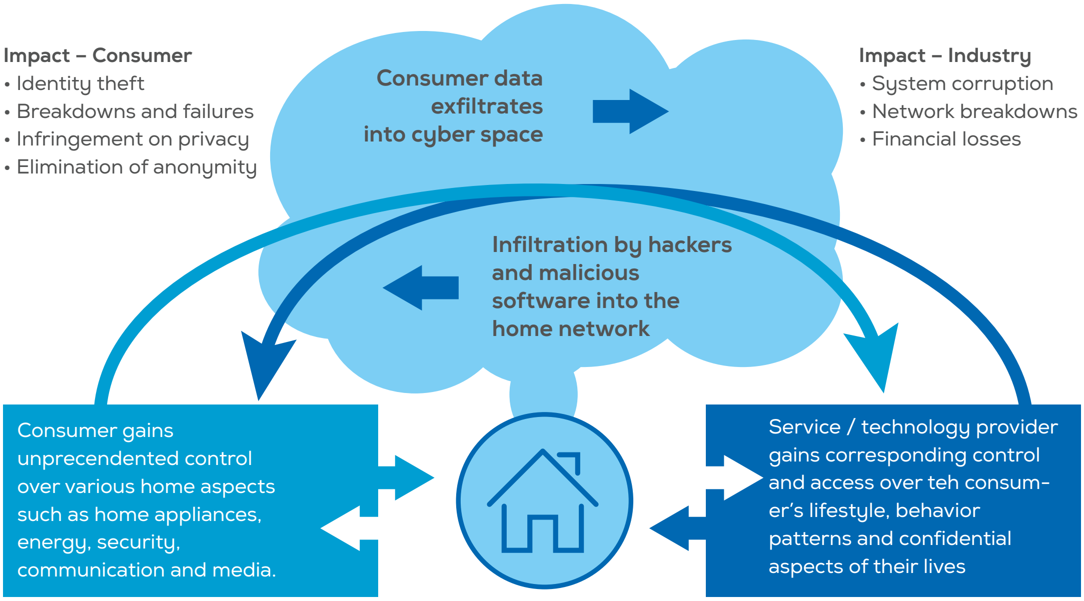
The degree of connectedness varies by the sophistication of the connected network that is ultimately the backbone of this evolving concept. The connected home has a wide scope, from one or more personal devices connected to a home area network to a comprehensive, home-wide integrated platform that eliminates 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 the Internet of Things (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 as shown in Figure ES 6.

Figure ES 6: 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.


Impact – Consumer
• Identity theft
• Breakdowns and failures
• Infringement on privacy
• Elimination of anonymity
Consumer data exfiltrates into cyber space
Impact – Industry
• System corruption
• Network breakdowns
• Financial losses
Infiltration by hackers and malicious software into the home network
Consumer gains unprecendented control over various home aspects such as home appliances, energy, security, communication and media.
Service / technology provider gains corresponding control and access over teh consumer's lifestyle, behavior patterns and confidential aspects of their lives

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

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 **two times more likely** than potential adopters and **three times more likely** than non-adopters to have experienced cybersecurity incidents, owing to their first hand exposure
- 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 five21 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 coverage** for cyber risks
- They also proactively ask 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 3: REVIEW 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

Issues	Challenges	Impact
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 larger 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 underqualified professionals.

ES-CH 4: OPTIMAL 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.

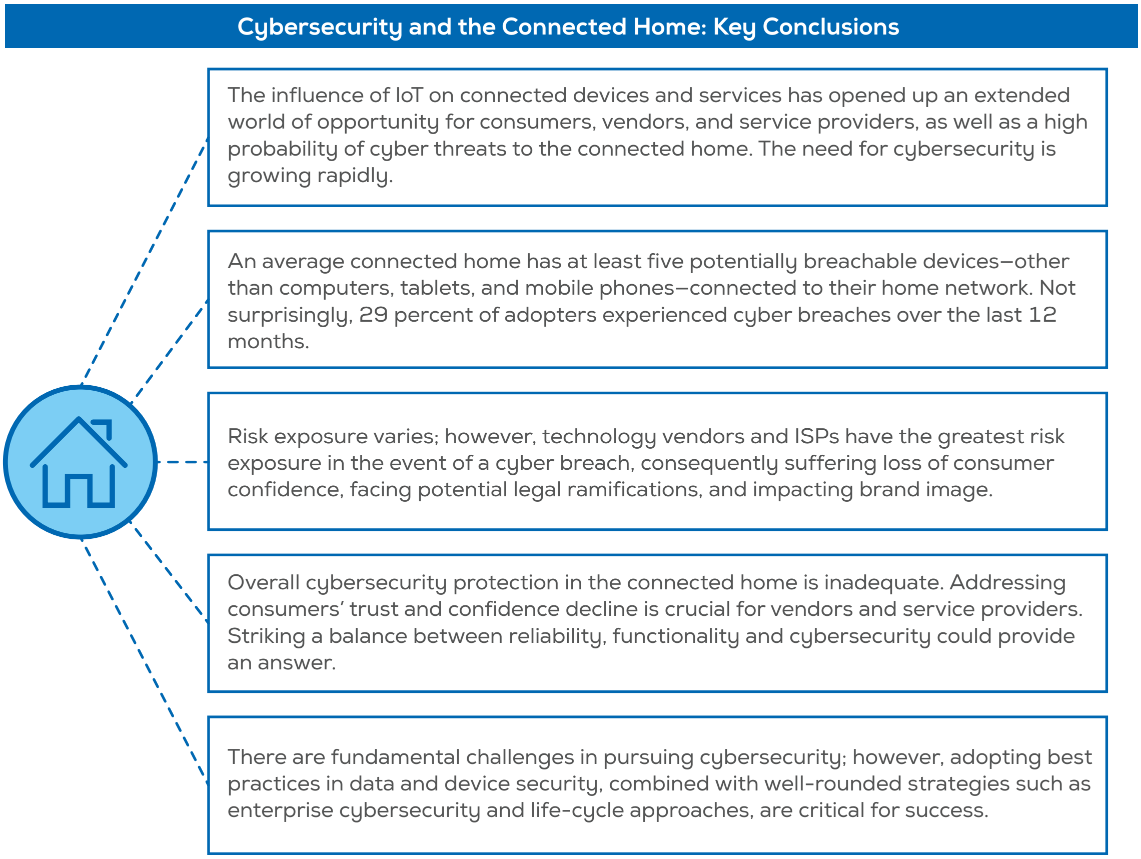
Industry Collaboration and Contingency Planning

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 5: CONCLUSIONS 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 conclusions of this research are summarized in Figure ES 10.

Figure ES 10: Cybersecurity and the Connected Home: Key Conclusions



Cybersecurity and the Connected Home: Key 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.

The key recommendations of this research include the 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, and incorporate advice of cybersecurity champions.
- Collaborate on industry initiatives around education, training, standards and policy.

CABA™

Cybersecurity and the Connected Home

RECOGNIZING THE RISK, ADOPTING BEST PRACTICES, HARNESSING THE POTENTIAL

888.798.CABA (2222)
613.686.1814 (x226)

Connect to what's next™

www.caba.org