Privacy and Cybersecurity in the Connected Home

LANDMARK RESEARCH PROJECT

EXECUTIVE SUMMARY

CABA AND THE FOLLOWING CABA MEMBERS FUNDED THIS RESEARCH:

CABA™ Continental Automated Buildings Association

Connect to what's next™

Disclaimer

This report was prepared for CABA by Frost & Sullivan.

FROST & SULLIVAN

Frost & Sullivan has provided the information in this report for informational purposes only. Qualitative and quantitative market information is based primarily on interviews and secondary sources, and is subject to fluctuations. Intelligent building 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 or recommendation. 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. Frost & Sullivan hereby disclaims liability for any loss or damage caused by errors or omissions in this report.

This paper is funded by CABA and CABA members Acuity Brands, Inc., CommScope, Inc., Community Smart Living, Inc. (powered by Netex), the Consumer Technology Association (CTA), CSA Group, National Research Council of Canada, Resideo Technologies, Inc., SnapAV and UL LLC. It represents the opinions of the authors, and is the product of professional research. It is not meant to represent the position or opinions of CABA, Acuity Brands, Inc., CommScope, Inc., Community Smart Living, Inc. (powered by Netex), the Consumer Technology Association (CTA), CSA Group, National Research Council of Canada, Resideo Technologies, Inc., SnapAV and UL LLC, nor the official position of any staff members.

Citation
Khaund, K. & Victor, D. (March 2021). *Privacy and Cybersecurity in the Connected Home*. Continental Automated Buildings Association (CABA).

Keywords: Connected Devices, Connected Homes, Cybersecurity, Internet of Things (IoT), Privacy.

Acknowledgements

Frost & Sullivan wish to acknowledge the support of Continental Automated Buildings Association (CABA) staff: Greg Walker, Senior Director, Research Operations, for his project management and liaison efforts; Ron Zimmer, President & CEO, for his recognition and promotion of this important topic; and CABA's Marketing and Business Development team for fundraising in support of this study. CABA would like to acknowledge Joanna Odrowaz for her editing of the report. In addition, the Steering Committee contributed valuable time and expertise to the project—through virtual group sessions, offline sessions with the research team, and reviews of the research processes, discussion guides, and earlier drafts of this report. These organizations and individuals are listed in alphabetical order below.

Steering Committee

Acuity Brands, Inc.
Jeff Spencer
Yan Rodriguez
Jazib Frahim

CommScope, Inc.
Shawn Liu

Community Smart Living Inc. (powered by Netex)
Jay Wax
Jason Kotler

Consumer Technology Association (CTA)
Steven Koenig
Mike Bergman

CSA Group
Nicki Islic

National Research Council Canada (NRC)
Amaya Arcelus
Heather Molyneaux
Hélène Fournier

Resideo Technologies, Inc.
David Kaufman

SnapAV/Control4
Eric Harper
Alex Mann
Glenn Clapp

UL LLC
Gonda Lamberink

TABLE OF CONTENTS

FIGURES

TABLES

EXCUTIVE SUMMARY

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 Frost & Sullivan to undertake this landmark research project to obtain a comprehensive understanding of the cyber risks and susceptibilities associated with connected-home technologies.

Cybersecurity vulnerabilities are already present within the connected home, and further aggravated with Internet of Things (IoT) and connected devices becoming more ubiquitous. It was therefore critical to explore the potential risks of cyber breaches and infringement on consumer privacy, and the long-term consequences for industry participants. The connected home represents a communication-rich living space, enabling smart experiences for the consumer, including energy management, interactive home devices, connected appliances, integrated entertainment, and real- time security solutions. It is an environment that also allows for unprecedented access to a variety of service providers and their networks, and the infiltration of pervasive technologies. Connected homes function via an internal and an external communication network, enabled by IoT, which helps activate various lifestyle-supporting functions. This characteristic is the basis for cybersecurity and privacy infringements and vulnerabilities as it gives technology and service providers direct access to systems and devices within the home. The systems installed to provide security and comfort can lead to serious breaches of consumer privacy, service disruptions, theft of personal information, and threats to anonymity.

While consumers question the advantages of connectedness at the cost of such risks, the industry is subjected to scrutiny of its commitment to solutions and privacy. Unless the issue of cybersecurity and privacy is dealt with comprehensively, market prospects for connected-home solutions will be negatively affected.

This research project focused on the following areas:

- Understanding the implications of cybersecurity and privacy compromises and ways of managing it
- Reviewing the challenges of implementing cybersecurity and privacy protection measures
- Evaluating the perceptions of various industry stakeholders and their level of accountability in managing these challenges
- Reviewing best practices that can be prioritized to address cyber risks and consumer privacy concerns

This report provides an analysis and evaluation of these focus areas, including a review of industry trends and challenges as well as consumers' cybersecurity and privacy concerns.

ES 1 ROLE OF THE STEERING COMMITTEE

The Steering Committee represents a cross-section of vendors, service providers, industry associations, and experts in connected-home technologies, automation, and smart devices. Representatives from each organization collaborated with Frost & Sullivan and CABA to guide the research scope and ensure that project objectives were met. Figure ES 1 shows the nine companies and organizations that supported the research project as Steering Committee members and funders.

Figure ES 1: Project Steering Committee and Funders

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 375 organizations involved in the design, manufacture, installation, and retailing of products relating to home automation and building automation. Public organizations, including utilities and government agencies 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 **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 360-degree coverage includes industry convergence, disruptive technologies, competitive intelligence, visionary innovation research, breakthrough best practices, changing customer dynamics, and emerging economies. To learn more, visit **www.frost.com**.

The Project Consulting Team

Frost & Sullivan led this research project for CABA. The core consulting team and report contributors were Konkana Khaund, Director of Consulting, and Dennis Marcel Victor, Senior Consultant.

ES 2 RESEARCH OVERVIEW

Connected homes are characterized by immersive applications of technology and innovations that enable lifestyle-enriching experiences. Connected-living technologies have made significant market progress and registered promising revenue growth in recent years. The connected-home industry has seen the arrival of numerous smart solutions in areas such as energy management, interactive home devices, voice-enabled tools, connected appliances, and real-time monitoring and intuitive functioning. This acceptance has allowed unprecedented access to a variety of service providers, opening the connected home to potential vulnerabilities. With connected-living technologies becoming pervasive, it is inevitable that the expanding ecosystem of suppliers and service providers as well as growing numbers of consumers will have to deal with the consequences of cyber breaches, privacy loss, and resulting financial implications.

ES 2.1 Key Objectives

The key objectives of the research included:

- Understanding the challenges imposed by compromised cybersecurity and privacy on connected-home industry stakeholders
- Evaluating the role of current cybersecurity response frameworks endorsed by the industry and the relevance of applicable standards and guidelines
- Reviewing value propositions and best practices around cybersecurity and consumer privacy and their effectiveness
- Assessing ways the connected-home industry can incorporate cybersecurity and privacy-protecting elements based on consumers' expectations

ES 3 METHODOLOGY

This project used a combination of primary and secondary research methodologies to compile information. Both qualitative research and quantitative tools were used for analysis and projection of key issues.

ES 3.1 Primary Research Process

There were two major components to this primary research project: an industry-focused research module and a consumer research module. These are described in Table ES 1.

Table ES 1: Description of the Primary Research Methodology

Item	Component	Description	Target Group Profile	Sample Size/ Actual Size	Research Technique
A	Consumers	Consumers of connected homes/smart devices/energy efficient home technologies	Occupants/ homeowners in U.S. and Canada	N=1,000-1,200 97% of target achieved	End-user survey through online panels and survey methods
B	Connected home technology vendors and service providers	Vendors/suppliers of connected home technology solutions; IoT solution providers; managed service providers; third party assimilators and integrators	Business unit decision makers, product and sales management professionals, alliance partners	N=60-75 70% of target achieved	Analyst interviews with industry stake-holders
C	Cybersecurity solution providers and privacy advocates	Vendors and service providers engaged in developing and marketing cybersecurity solution; advocates and industry influencers dealing with consumer privacy issues	Vice presidents, directors, marketing professionals in these organizations; consumer privacy advocates, academics, regulators	N=25-30 80% of target achieved	Virtual forum and interviews led by analysts
D	Industry influencers	Codes- and standard-development organizations for connected environments and IoT, regulators, industry associations, academic influencers	Association heads, working committee members for regulatory bodies, academics	N=20-25 75% of target achieved	Analyst interviews with industry stake-holders
Overall Sample Size (A+B+C+D) = 1,110-1,330					

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

The industry-focused primary research used structured discussion techniques with target participants. This provided excellent validation of findings from the consumer research survey. Findings from the consumer survey were triangulated through the corroboration of insights from the industry-focused primary research process.

ES 3.2 Research Instruments: Questionnaire/Discussion Guide

The discussion guides for both modules of the primary research process were jointly developed by Frost & Sullivan and the members of the Steering Committee. The project team and the Steering Committee reviewed the draft discussion guides early in the research project. The survey logic was tested using a soft launch process, and the two research modules were launched. The samples for both research modules were generated using Frost & Sullivan's repository of contact sources and databases.

The industry-focused primary research reached 75 percent of the target sample. The data from these discussions was analyzed and distilled into the commentary of the report. The online consumer survey was launched and remained active for seven weeks in the field. A total of 1,164 responses were collected against an original target of 1,200, resulting in a 96 percent target achievement. The data from these responses were analyzed using various qualitative and quantitative tools for interpretation in the report.

ES 3.3 Secondary Research

Information from published sources 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 was used to enrich and externalize the primary research findings. References are cited the first time they are used. Dates associated with reference materials are provided where available.

References to Frost & Sullivan research findings, industry interactions, and discussions are made in the context of the primary research findings for this project, unless otherwise stated. The analysis and interpretation of data in this report are those of Frost & Sullivan's consulting team.

ES 3.4 Definitions and Consumer Survey Qualification Criteria

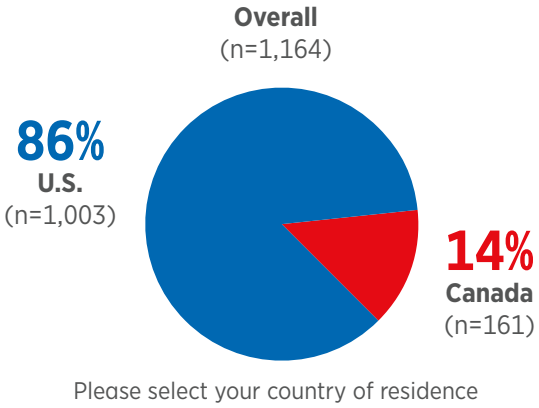
Following past landmark research projects on connected homes, a connected home is defined as "a residential environment where owners/occupiers use smart devices, appliances, communication features, controls, centralized hubs, and other functionalities that are enabled by information technology that anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, energy savings, and security, among other functions." The presence of two or more connected devices was a baseline requirement to qualify as a connected home. This broad definition provided the study participants with a degree of flexibility in envisioning and discussing the concept of the connected home.

Potential participants were asked a number of screening questions to determine:

- If they were 18 years or older
- If they lived in the United States or Canada
- The number of people living in the house
- The average gross household income per year
- If they played a role in making decisions about purchasing the household's connected-home solutions
- The communication and connectivity services in the home

Of the qualified respondents, 86 percent lived in the U.S. and 14 percent in Canada, as shown in Figure ES 2.

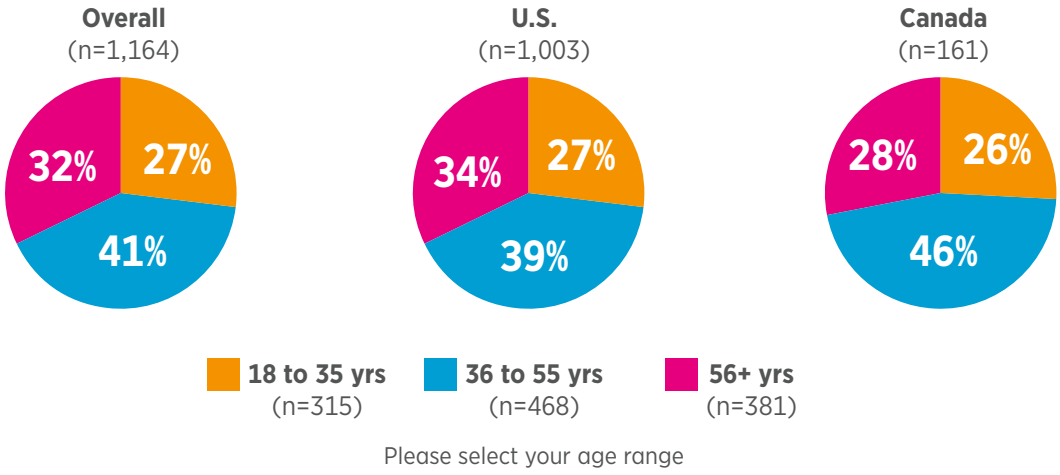
Figure ES 2: Consumer Survey Respondents' Country of Residence



Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

Respondents were approximately equally distributed between three age groups, as shown in Figure ES 3.

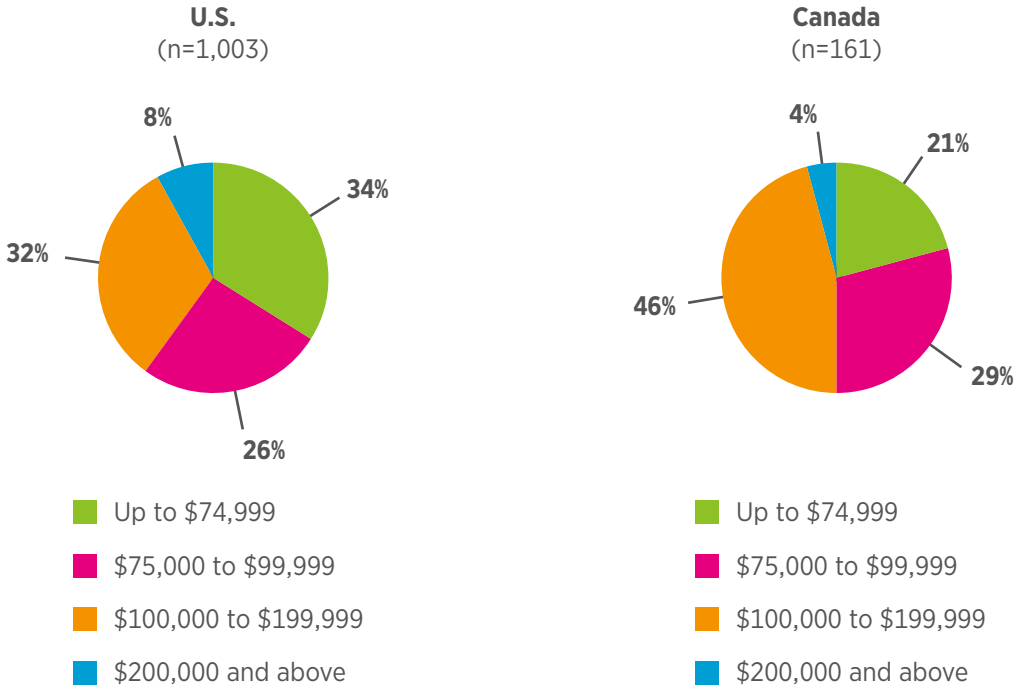
Figure ES 3: Consumer Survey Respondents' Age



Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

Figures ES 4 and ES 5, respectively, show the respondents' household income and description of their households.

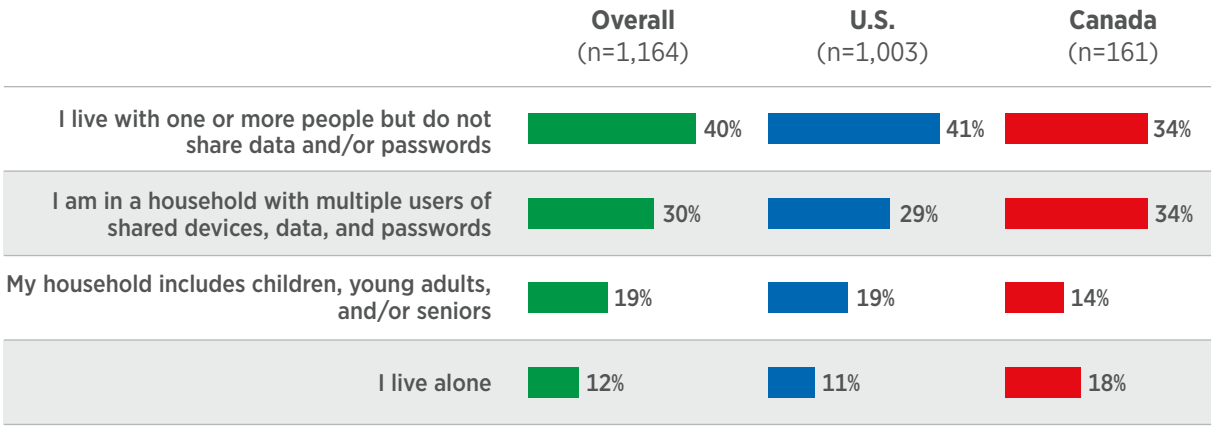
Figure ES 4: Consumer Survey Respondents' Household Income



What is your approximate household income; i.e., combined total earnings of household members before taxes?

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

Figure ES 5: Consumer Survey Respondents' Description of their Household



How would you describe your household?

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

ES 4 LAYOUT OF THE REPORT

Table ES 2 shows the layout of the report, which includes an executive summary, five chapters and two appendixes. The appendixes include a list of abbreviations and a list of references.

Table ES 2: Report Layout

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

Sections	Title	Content
Executive Summary		Background and introduction; objectives, methodology and definition, overview of top findings
Chapter 1	State of Privacy and Cybersecurity in the Connected Home	State of the connected-home industry, industry stakeholders, domain issues, current and potential threat scenario; best practices review
Chapter 2	Consumer Perception Analysis	Methodology, sample classification; adoption potential analysis; consumers' benefits and trust factors; expectations from vendors and service providers; key takeaways
Chapter 3	Cybersecurity and Privacy Frameworks Review	Core issues including cybersecurity and privacy framework implementation, legislation, standards, certifications, consensus development on core issues and initiatives
Chapter 4	Cybersecurity Value Proposition Review	Devising the ideal response plan for industry participants: identifying risk, responsibility and accountability of stakeholders
Chapter 5	Conclusions and Recommendations	Conclusions of the research and key recommendations
Appendix A		Glossary of terms
Appendix B		References

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

ES 5 SUMMARY OF KEY FINDINGS

The research findings discussed in Chapters 1 to 5 are summarized here. Each heading represents the corresponding chapter. For example, ES-CH 1 corresponds to executive summary of Chapter 1.

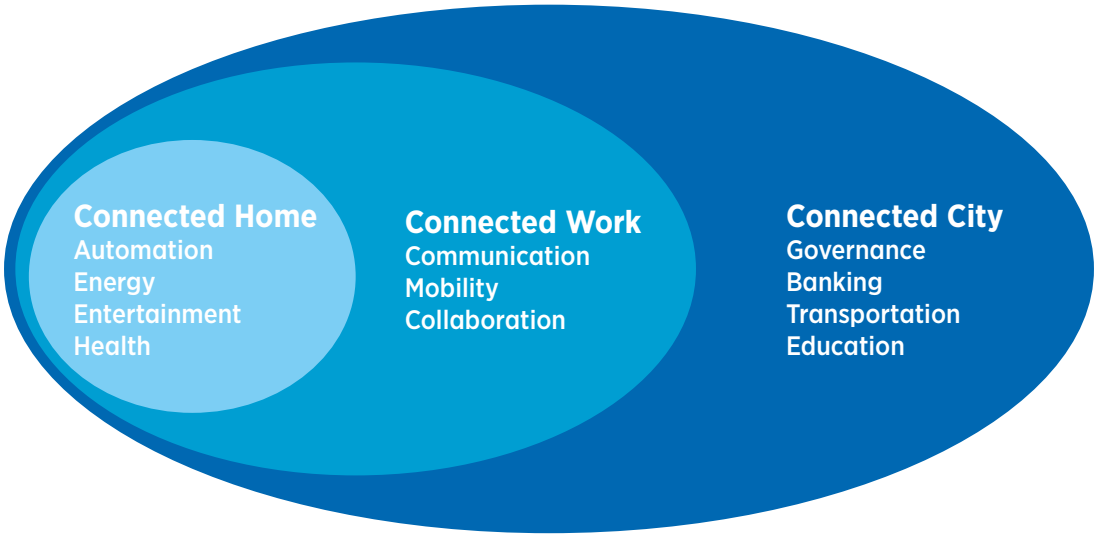
ES 5.1 ES-CH1: State of Privacy and Cybersecurity in the Connected Home

In the last decade, the connected-home market has been transformed in the way technology is used and augmented. A connected home has devices, communication services, and applications that interconnect and communicate to enable a responsive and adaptive environment that helps the occupants make smart lifestyle-supporting decisions. The extent of connectedness varies by the sophistication of the network that forms the backbone of the connected home. The primary drivers for market growth are the increasing acceptance

of new products and the safety and comfort they offer. This trend is likely to continue as consumers start to perceive novel products, from virtual voice assistants to wearable health devices, as standard.

Figure ES 6 shows a model of a broader connected lifestyle that consumers are embracing today.

Figure ES 6: The Concept of Connected Living



Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

Focusing and prioritizing smart functionalities, interoperability, smart connectivity, apps, and user experiences have dominated the strategic decisions of connected-home vendors and service providers. And topping it all has been the rushed time-to-market to capture market share and penetration. Ongoing research and research undertaken for this project show that market participants factored in cybersecurity and privacy reactively. As the rate of device penetration grew, so did concerns to do with privacy infringements and cyber breaches, resulting in financial losses, among others. These concerns have posed a serious threat to the market prospects of connected-home solutions. As the problem grows with the market entry of new devices and the growing technology stack of the connected home, threats to market derailment cannot be ignored.

The growing ecosystem and expanding technology stack are increasing the potential for various vendors and service providers to inflict security breaches on each other's networks. Data security and privacy are critical for consumers as they do not want their personal data or credentials stolen. A major concern restraining the adoption of connected devices is the compromise of private information. Technological advancements in smart devices, and associated services catering to such devices, are generating additional privacy challenges. Sensors embedded in smart and connected devices collect vast amounts of data, which are processed and analyzed to provide a service to the users. This, with the increasing deployment of IoT devices in the home, exposes consumers to new privacy and security risks. Research for this project shows that most industry studies of barriers to adoption and acceptance of connected-home solutions have, so far, been directed at understanding technological issues

associated with such solutions, including cybersecurity concerns. However, the issue of privacy remains largely unconsidered. More importantly, the construct of privacy concerns has not yet been part of scientific research on this topic.

Findings from the customer research undertaken for this project indicate that 71 percent of product security breaches could be due to glitches and security issues embedded in vendors' and service providers' solutions. When the same study was undertaken in 2015, the share of breaches attributed to service provider glitches was only 54 percent. This substantial increase, 31 percent over five years, indicates that it is challenging for vendors and service providers to keep pace with cybersecurity innovations and release fully tested and hardened devices.

ES 5.2 ES-CH2: Consumer Perception Analysis

Part of the project involved gathering consumers' insights into their privacy concerns, perceptions of vendors' and devices' trustworthiness, and cybersecurity vulnerabilities associated with the connected-home solutions they currently use or are planning to acquire. The findings of the consumer research module helped in the real-world application of data from industry research and secondary sources.

The top takeaways of the consumer research module are shown in Figure ES 7.

Figure ES 7: Top Takeaways of the Consumer Research Module

Adoption Overview

- With 89% having adopted some form of smart home solution, connected-home products and solutions represent a rapidly evolving and growing segment.
- Personal connected devices and entertainment options still dominate the market, leaving significant room for all other categories to increase share.

Cyber Breaches and Privacy Infringement

- While 13% of respondents said they had had a breach in their smart home systems, this happened to 20% of those between 18 and 34 years old.
- Over 70% of breaches and security issues were attributed to service provider's errors and glitches embedded in vendors' and service providers' solutions.

Consumers' Technology Awareness

- Over 80% of respondents across North America agree with or are neutral on the need to use unique, complex passwords for multiple devices. About half were also aware of privacy guidelines (49%) and could confidently select relevant devices for their household (54%).
- However, the perception was that vendors and service providers levels of privacy protection were very low, particularly for appliance manufacturers.

Consumers' Trust and Confidence in Vendors

- Adopters aged 18-25 years were more trusting of their vendors and service providers. Trust and confidence diminished in the higher age groups.
- In the higher age groups, concerns over data breaches and personal identity protection increased, and these respondents were more reluctant to engage with vendors and service providers whose solutions required multiple third-party access and intrusions.

Consumers' Expectations of Vendors and Products

- Consumers want to be able to choose to opt out of sharing information.
- A label or other indication of built-in privacy protection is a critical requirement, with 69% agreeing that this should be visible on the product.
- Over 60% of respondents agreed they need better disclosure on how their information will be used and why is it collected.

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

ES 5.3 ES-CH3: Cybersecurity and Privacy Frameworks Review

Addressing cybersecurity and privacy infringements in the connected home requires efforts in the areas of regulations, guidelines, and policy to address the interests of all stakeholders. Regulations and policy are key domain issues in the connected-home industry and related IoT segments.

Cybersecurity legislation is still in nascent stages in North America and remains rather shortsighted. So far, new legislation has been correcting loopholes in past legislation or trying to cope with requirements that were not previously addressed because of the rapid evolution of IoT innovations and the entry of new connected solutions into the marketplace. These changes and innovations pose a growing threat to cybersecurity and privacy, accelerating the need for dynamic guidelines, frameworks, testing criteria and regulatory policy.

The survey conducted for this research project found that consumers preferred more visible and transparent product labeling and certification. The lack of clarity in certifying products as cyber secure or as guaranteeing consumers' privacy is an ongoing issue. First, the elements that need to be certified vary by product. Second, there is no industry-approved guideline that describes which details or configurations will confer cybersecurity. Finally, multiple agencies—industry associations, not-for-profit bodies, and standards organizations from other industries—can spearhead certifications, leading to further confusion in determining which product elements are cyber secure.

This research evaluated some of the existing frameworks and guidelines on privacy and cybersecurity. Although these frameworks and guidelines have considered cybersecurity more or less comprehensively, privacy has been relatively less explored. Besides, strict regulations and policy frameworks neither offer enforceability nor safeguard vulnerable consumers. Those frameworks that advocate for cybersecurity and privacy needs to be baked into connected-design concepts have found greater acceptance among advocates and vendor organizations.

ES 5.4 ES-CH4: Cybersecurity Value Proposition Review

The severity of cyberattacks is expected to grow as hackers' sophistication increases and new devices enter the connected-home marketplace. Privacy concerns are likely to grow proportionally. The connected-home industry will need to safeguard their solutions to avoid the resulting fallout. Incorporating predictive capabilities to counter such adversarial tactics will be critical when proposing optimal cybersecurity that delivers greater privacy protection. Given the fundamental complexities of the situation, it is imperative that the entire spectrum of industry participants reach a consensus on cybersecurity measures.

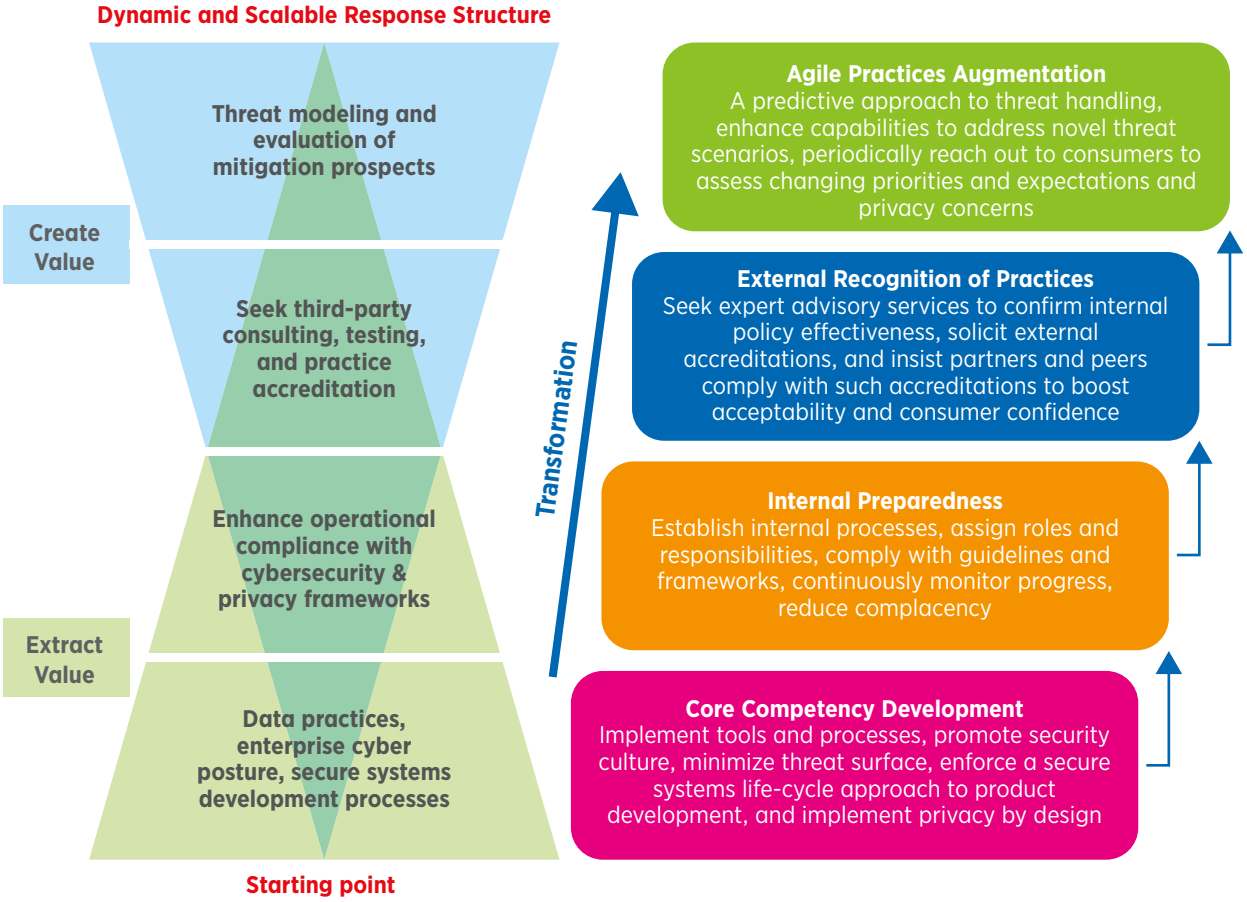
A proposal with optimal value that incorporates privacy protection and cybersecurity of connected-home solutions would need to incorporate the following key elements:

- Accounting for interdependencies in risk mitigation
- Consensus development on best practices
- A dynamic response plan with countermeasures

A dynamic response is required to handle the continually evolving cyber threats to connected homes. Privacy is also a changing concept as consumers are introduced to novel experiences with emerging technologies and service experiences. It is likely that expectations from vendors will change as consumers weigh functionality, usefulness, and compromises to their privacy and anonymity. For vendors and service providers, it is important to chart out a dynamic and scalable response plan that can cope with their growth needs and consumers' evolving demands for new connected products and solutions.

Figure ES 8 illustrates a proposed privacy and cybersecurity response plan for connected-home solution providers, as informed by the findings of this research.

Figure ES 8: Connected-Home Privacy and Cybersecurity Response Plan



Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

ES 5.5 ES-CH5: Conclusions and Recommendations

This project found that cybersecurity and privacy issues, which continue to be an issue in the connected home, have the potential to worsen given the increase in number of new devices ownership and growing demand for gadgets. Adoption by new demographic segments, such as older adults and children, and large numbers of young adults raises concerns around the many ways that the connected home is vulnerable.

A measured approach to assessing cyber risks and privacy infringement challenges is necessary given that the profile and intensity of such risks will continue to grow with the increase in device ownership and market penetration. Growing consumer sophistication and vigilance regarding the use of their devices and their growing expectations of cybersecurity and privacy is encouraging. As a result, solution providers will have to enhance their compliance levels.

What remains to be seen is how much of this compliance can be institutionalized and mandated. Interdependencies and crossover impacts will continue to challenge regulators, assimilators, integrators, aggregators, and above all consumers. Adopting some of the best practices described in this research will help support the compliance agenda and fast-track the consensus needed to address cybersecurity and privacy challenges. Figure ES 9 illustrates the key conclusion from this research.

Figure ES 9: Privacy and Cybersecurity in the Connected Home: Key Conclusions

Privacy and Cybersecurity in the Connected Home: Key Conclusions	
Strong adoption potential with a high threat exposure	With 89% adoption, connected-home products and solutions represent a rapidly growing segment; personal connected devices and entertainment options still dominate the market, leaving room for all other categories to increase share. Cyber vulnerabilities and privacy infringement are also on the incline.
Increased device ownership and breach potential	Connected-device ownership is growing. Nine out of every 10 adopters own some form of connected device, and, on average, own at least five connected devices that are potentially breachable. Not surprisingly, 29% of adopters experienced cyber breaches over the last 12 months.
Growing consumer sophistication and vigilance	Consumers' sophistication and vigilance with regard to connected-home solutions is increasing. Over 80% of North American survey respondents said they used unique, complex passwords for multiple devices and 49% were aware of privacy guidelines. However, consumers perceived the levels of privacy protection given by vendors and service providers to be very low.
Compliance, standards and interoperability Issues	Instituting prescriptive cybersecurity requirements and minimum privacy provisions in products requires collaboration between alliances and standards development bodies to ensure interoperability and cyber compliance is achieved consistently. However, developing alliances is a challenging proposition.
Dynamic response plan for cyber vigilance	Adopting an approach in data and device security that is driven by best practices, combined with well-rounded strategies such as enterprise cybersecurity and life-cycle approaches, is critical for success. However, privacy needs to be baked into the original concept plan through comprehensive privacy-by-design principles.

Source: CABA Privacy and Cybersecurity in the Connected Home 2021 Report

A key recommendation for industry participants from this research is to treat cybersecurity and privacy protection as the norm. It is critical to put the consumer at the center of the discussion and build solutions that keep consumers' needs and priorities in mind. Aside from functionality and user experience, privacy needs to be factored into the process. Designing for security is important to achieving cybersecurity compliance and avoid costly consequences. Mandating stringent guidelines for partners and component suppliers is also critical. All of this is possible by having a dynamic cybersecurity regimen in place. This can be achieved by following a comprehensive enterprise-wide cyber response plan.

APPENDIX A: GLOSSARY

ANSI: American National Standards Institute

API: application programming interface

AV2: Home Plug AV2 specification from the HomePlug Powerline Alliance

BoPL: broadband over power line

CABA: Continental Automated Buildings Association

CAGR: compound annual growth rate

CCPA: California Consumer Privacy Act

CHC: Connected Home Council

CISA: Cybersecurity Information Sharing Act

CPRA: California Privacy Rights Act

CSA Group: CSA Group Testing & Certification Inc., operating as CSA Group

CTIA: Cellular Telecommunications Industry Association

DLTS: Datagram Transport Layer Security

DoD: Department of Defense

ECDH: Elliptic-curve Diffie–Hellman

EU: European Union

ENISA: European Union Agency for Cybersecurity

FCC: Federal Communications Commission

FIPS: Federal Information Processing Standards

FTC: Federal Trade Commission

GDPR: General Data Protection Regulation

G.hn: specification for home networking with data rates up to 2 Gbit/s

IEC: International Electrotechnical Commission

IEEE: Institute of Electrical and Electronics Engineers

IoT: Internet of Things

IT: information technology

IP: Internet protocol

ISA: International Society of Automation

ISO: International Organization for Standardization

ISP: Internet service provider

ITU: International Telecommunication Union

ITU-T: ITU Telecommunication Standardization Sector

LTE: Long-Term Evolution standard for wireless broadband technology

MoCA: Multimedia over Coax Alliance technology

NIST: National Institute of Standards and Technology

OCF: Open Connectivity Foundation

OTT: over-the-top (services)

PbD: privacy by design

PC: personal computer

SHIELD: Stop Hacks and Improve Electronic Data

SSL: secure socket layer

UL: Underwriters Laboratories

UL CAP: UL Cybersecurity Assurance Program

APPENDIX B: REFERENCES

1 Frost & Sullivan. (2019). *Future of Smart and Connected Homes, Forecast to 2025*. https://www.researchandmarkets.com/reports/4846382/future- of-smart-and-connected-homes-forecast-to

2 Frost & Sullivan. (2014). *Connected Living, Forecast to 2025*.

3 Frost & Sullivan. (2019). *Future of Smart and Connected Homes, Forecast to 2025*.

4 Frost & Sullivan. (2019) *Future of Smart and Connected Homes, Forecast to 2025*.

5 Koetsier, J. (2020, February 17). *Amazon, Google Own U.S., Europe In Smart Speakers as Sales Up 70%. But Baidu And Xiaomi Grew Over 100%*. Forbes. https://www.forbes.com/sites/johnkoetsier/2020/02/17/amazon-google- own-us-europe-in-smart-speakers-as-sales-up-70-but-baidu-and- xiaomi-grew-over-100/?sh=6d308c7d15c4

6 Frost & Sullivan. (2019) *Future of Smart and Connected Homes, Forecast to 2025*.

7 Frost & Sullivan. (2014). *Connected Living, Forecast to 2025*.

8 Sonny, A., & Yusuf, Z. (2018, October 1). *Mapping the Smart-Home Market*. Boston Consulting Group. https://www.bcg.com/it- it/publications/2018/mapping-smart-home-market

9 Raymond, M. (n.d.). *Usage and Buying Trends in Smart Home Devices: GoodFirms Research*. https://www.goodfirms.co/resources/buying-smart- home-devices-statistics

10 Frost & Sullivan. (2019) *Future of Smart and Connected Homes, Forecast to 2025*.

11 Fouse, D. (2020, June 29). *Cybercrime Is on The Rise: How Communications Can Help State and City Governments*. Forbes. https://www.forbes.com/sites/forbesagencycouncil/2020/06/29/cybercrim e-is-on-the-risehow-communications-can-help-state-and-city- governments/?sh=71fbf626501e

12 International Telecommunication Union. (n.d.). *Internet of Things Global Standards Initiative*. https://www.itu.int/en/ITU- T/gsi/iot/Pages/default.aspx

13 Malhotra, N.K., Kim, S. S., Agarwal, J. (2004, December 1). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 311–416. https://doi.org/10.1287/isre.1040.0032

14 Guhr, N., Werth, O., Blacha, P.P.H., Breitner, M.H. Privacy concerns in the smart home context. *SN Applied Sciences*. 2, 247 (2020). https://doi.org/10.1007/s42452-020-2025-8

15 Statt, N. (2020, July 16). *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*. The Verge. https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates- twitter-hack-bitcoin-scam-compromised

16 Owaida, A. (2020, April 16). *Half a million Zoom accounts for sale on the dark web. ESET: Enjoy Safer Technology*. https://www.welivesecurity.com/2020/04/16/half-million-zoom- accounts-sale-dark-web/

17 Davis, J. (2020, July 7). *Magellan Health Data Breach Victim Tally Reaches 365K Patients*. Health IT Security. https://healthitsecurity.com/news/magellan- health-data-breach-victim-tally-reaches-365k-patients

18 Ferreras, J. (2019, July 29). *Capital One data breach hits about 6 million people in Canada, 100 million in U.S. Global News*. https://globalnews.ca/news/5700226/capital-one-data-breach-canada/

19 Cimpanu C. (2020, March 31). *Marriott discloses new data breach impacting 5.2 million hotel guests*. Zero Day. https://www.zdnet.com/article/marriott- discloses-new-data-breach-impacting-5-2-million-hotel-guests/

20 Garcia, S. E. (2019, December 30). *Data Breach at Wyze Labs Exposes Information of 2.4 Million Customers*. The New York Times. https://www.nytimes.com/2019/12/30/business/wyze-security-camera- breach.html

21 Whittaker, Z. (2020, June 9). *Nintendo now says 300,000 accounts breached by hackers*. Tech Crunch. https://techcrunch.com/2020/06/09/nintendo- accounts-affected-breach/

22 CNN Newsource. (2019, December 13). *A hacker accessed a family's Ring security camera and told their 8-year-old daughter he was Santa Claus*. https://www.thedenverchannel.com/news/national/a-hacker-accessed-a- familys-ring-security-camera-and-told-their-8-year-old-daughter-he- was-santa-claus

23 Paul, K. (2020, December 23). Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs. *The Guardian*. https://www.theguardian.com/technology/2020/dec/23/amazon-ring- camera-hack-lawsuit-threats

24 Peterson, H. (2019, September 25). Wisconsin couple describes the chilling moment that a hacker cranked up their heat and started talking to them through a Google Nest camera in their kitchen. *Business Insider*. https://www.businessinsider.in/retail/wisconsin-couple-describes- the-chilling-moment-that-a-hacker-cranked-up-their-heat-and- started-talking-to-them-through-a-google-nest-camera-in-their- kitchen/articleshow/71300897.cms

25 Whittaker, Z. (2020, June 1). After a spate of device hacks, Google beefs up Nest security protections. *Tech Crunch*. https://techcrunch.com/2020/06/01/google-nest-advanced-protection/

26 Kumar, M. (2020, February 5). *Flaw in Philips Smart Light Bulbs Exposes Your WiFi Network to Hackers*. The Hacker News. https://thehackernews.com/2020/02/philips-smart-light-bulb- hacking.html

27 ioXt. (n.d.). *ioXt Certification Program*. https://www.ioxtalliance.org/get- ioxt-certified

28 UL. (n.d.). *Underwriter Laboratories: Solutions for Connected Devices*. https://www.ul.com/services/solutions-connected-devices

29 CSA Group. (n.d.). *Cybersecurity*. https://www.csagroup.org/testing- certification/testing/cybersecurity

30 IAPP. (n.d.). *Privacy by Design Certification Program: Assessment Control Framework*. https://iapp.org/resources/article/privacy-by-design- certification-program-assessment-control-framework/

31 CABA. (2016). *Intelligent Buildings and Cybersecurity Report* (2016).

32 Federal Trade Commission. (2019, March 26). *FTC Seeks to Examine the Privacy Practices of Broadband Providers*. https://www.ftc.gov/news- events/press-releases/2019/03/ftc-seeks-examine-privacy-practices- broadband-providers

Privacy and Cybersecurity in the Connected Home

LANDMARK RESEARCH PROJECT

888.798.CABA (2222)
613.686.1814

Connect to what's next™

www.caba.org