NISTIR 8333

Workshop Summary Report for "Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices" Virtual Workshop

Katerina N. Megas
Michael Fagan
Barbara Cuthill
Mary Raguso
John Wiltberger

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8333

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8333

Workshop Summary Report for "Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices" Virtual Workshop

Katerina N. Megas
Michael Fagan
Barbara Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

Mary Raguso
John Wiltberger
The MITRE Corporation
McLean, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8333

March 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8333
23 pages (March 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8333

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: iotsecurity@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This report provides a summary of the discussion and findings from the NIST *Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices* virtual workshop in October 2020. NIST Interagency Report (NISTIR) 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers,* and NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline,* provide general guidance on how manufacturers can approach their role of fulfilling their customers' cybersecurity needs and capabilities. As discussed in those documents, particular sectors and use cases may require more specific guidance than what is included in NISTIR 8259A's core baseline for Internet of Things (IoT) devices. To better understand the consumer home device sector, NIST collected observations on the cybersecurity device capabilities in a number of devices available in the first half of 2019. These observations were published in Draft NISTIR 8267, *Security Review of Consumer Home Internet of Things (IoT) Products*. The information in Draft NISTIR 8267 was foundational for the NIST *Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices* virtual workshop. The workshop gathered further community input on the concerns with consumer home IoT device cybersecurity.

Keywords

consumer home devices; cybersecurity baseline; Internet of Things (IoT); privacy; securable computing devices; security requirements.

Audience

The main audiences for this publication are IoT device manufacturers, consumer organizations, and other stakeholders in the consumer home IoT market. This publication may also help IoT device customers or integrators who are incorporating IoT devices intended for the home market into their residence or business, especially small business networks.

Acknowledgments

The authors wish to thank all contributors to this publication, including the participants in this workshop and other interactive sessions; the individuals and organizations from the public and private sectors, including manufacturers for various sectors and several manufacturer trade organizations who provided feedback on the preliminary public content; and colleagues at NIST, The MITRE Corporation, and Scarfone Cybersecurity who offered invaluable input and expertise.

Table of Contents

List of Appendices

1 Introduction

To better understand the consumer home Internet of Things (IoT) device sector, the National Institute of Standards and Technology (NIST) collected observations on the cybersecurity capabilities in a number of devices available in the first half of 2019. These technical observations were based on approaches to implementing the cybersecurity capabilities described in NIST Interagency Report (NISTIR) 8259A, *IoT Device Cybersecurity Capability Core Baseline* [1]. The observations were published in Draft NISTIR 8267, *Security Review of Consumer Home Internet of Things (IoT) Products* [2].

The information in Draft NISTIR 8267 and comments received during the public comment period were foundational for NIST's October 22, 2020 virtual workshop titled *Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices*. This workshop gathered further community input on the concerns with consumer home IoT device cybersecurity. It included stakeholders from industry, trade associations, consumer advocacy groups, international bodies, and academia. The purpose of this workshop was to obtain stakeholder feedback on topics related to future directions for NIST, including its National Cybersecurity Center of Excellence's (NCCoE) work in the consumer home IoT space, and to identify and discuss critical issues and barriers to implementing the core baseline in NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [1], in consumer IoT products.

1.1 About the NIST Cybersecurity for IoT Program

The mission of the NIST Cybersecurity for IoT program [3] is to cultivate trust in IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools. The Cybersecurity for IoT program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, consumer advocacy groups, international bodies, and academia, the program aims to fulfil this mission and foster an environment that sparks innovation on a global scale.

1.2 About the Cybersecurity Risks in Consumer Home IoT Devices Virtual Workshop

The free, publicly available virtual workshop featured an overview of NIST's Cybersecurity for IoT Program and panels that highlighted the many considerations impacting the cybersecurity of home IoT products. These considerations include unique cybersecurity challenges associated with home IoT products and unique barriers to implementing the core baseline in NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [1] in consumer IoT products. After the panels, attendees broke into small groups for facilitated discussions about the most critical issues impacting the implementation of stronger cybersecurity in consumer IoT devices. The workshop concluded with attendees reassembling to hear reports from each breakout facilitator—tying together any overriding themes and/or issues for future exploration.

The workshop agenda is presented in Table 1 and on the NIST event information page [4].

Table 1: Workshop Agenda

Time	Activity and Presenters
12:00 – 12:20 PM	**Welcome and introduction:** **Kat Megas,** Program Manager, NIST Cybersecurity for IoT Program **Mike Fagan**, Technical Lead, NIST Cybersecurity for IoT Program • Overview of NIST IoT Cybersecurity program, core baseline and profiling work • Overview of NCCoE work related to Consumer IoT Cybersecurity
12:20 – 1:20 PM	**Panel 1: What makes a consumer IoT device different?** • **Moderator: Barbara Cuthill**, Deputy Program Manager, Cybersecurity for IoT Program (NIST) • **Maarten Bron**, Managing Director, Riscure • **L. Jean Camp**, Professor, Indiana University Bloomington • **Mark Haney**, Laboratory for Telecommunication Sciences, University of Maryland • **Rebecca Herold**, The Privacy Professor Consultancy • **Andrew Tierney**, IoT Security Consultant, Pen Test Partners
1:20 – 1:30 PM	**Break**
1:30 – 2:30 PM	**Panel 2: What barriers exist to meeting the baseline in NISTIR 8259A *IoT device Cybersecurity Capability Core Baseline in Consumer Devices?*** • **Moderator: Mike Fagan,** Technical Lead, NIST Cybersecurity for IoT Program • **Mike Bergman**, Vice President of Technology and Standards, Consumer Technology Association • **Julie Haney**, Computer Scientist, Visualization and Usability Group, NIST • **Michelle Richardson**, Director of the Data and Privacy Project, Center for Democracy and Technology • **David Thaler**, Partner Software Architect, Microsoft
2:30 – 2:45 PM	**Break** Transition to Plenary Session
2:45 – 3:45 PM	**Breakout Sessions** Facilitated discussions on what tools and guidance are needed to build and support more secure consumer home IoT devices
3:45 – 4:00 PM	**Break** Transition to Plenary Session
4:00 – 4:20 PM	**Readout from Breakout Sessions** Facilitator Panel
4:20 – 4:30 PM	**Concluding Remarks: Kat Megas**, Program Manager, NIST Cybersecurity for IoT Program

The workshop drew approximately 338 participants, including attendees, panelists, and moderators, from 13 countries. These participants came from many types of organizations, including:

- Fourteen academic institutions from across the country
- Nine non-profit organizations, including consumer electronics and engineering, and business/trade associations
- Approximately 60 private sector businesses, including major corporations, IoT device manufacturers, small businesses, and high-technology firms

- Fourteen management consulting firms
- Sixteen federal, state, and local government organizations, including civil, defense, and intelligence agencies

NIST sought a wide range of workshop attendees involved in the consumer home IoT market to hear their views. Consumers have a broad range of technical expertise, but most are much less familiar with cybersecurity than the specialists employed by businesses and government. On the other hand, the market is exploding with new consumer IoT devices that incorporate a variety of ideas and approaches to implementing device functionality and cybersecurity. The NIST Cybersecurity for IoT program is attempting to identify the critical elements of this complex market that will make a substantial difference in the cybersecurity capabilities available in consumer home IoT devices.[1]

During the workshop panels, participants submitted questions and participated in a series of six polls as a mechanism to share feedback and influence the focus of panel discussions. The poll questions and results are presented in Appendix A. Since workshop attendees created a by-definition, self-selected survey group and poll responses were entirely voluntary, poll results should be not viewed as providing generalizable results for their questions. During the workshop breakouts, which consisted of significantly smaller groups of participants, facilitated discussions encouraged open conversation and the exchange of ideas.

Videos of each workshop segment are available on the event web page [4]. Based on the participant presentations and stakeholder feedback collected, this report provides a summary of key points, common themes, and a general discussion of possible follow-on activities for NIST's IoT program.

[1] The catalog of technical cybersecurity capabilities and non-technical supporting capabilities can be viewed on GitHub at https://pages.nist.gov/FederalProfile-8259A [5]. Feedback can be submitted by submitting issues to the repository at https://github.com/usnistgov/FederalProfile-8259A.

2 Summary and Key Takeaways

The following takeaways are the ideas, observations, and suggestions that NIST heard from workshop participants and that received significant support from attendees and/or panelists. This workshop was not a forum for developing consensus; rather, the takeaways represent recurrent themes which emerged during the event—not formal positions taken by attendees or participants. While this document seeks to thoroughly summarize discussions and viewpoints expressed by panelists and participants, it cannot capture every thought, opinion, and suggestion provided during the sessions. The takeaways do not represent specific NIST recommendations or guidance; rather, they provide important feedback to the program, and serve as a basis for future conversations with the community.

Takeaway 1: Creating a more secure IoT ecosystem for consumer devices can benefit all manufacturers and the "common good."

Workshop participants expressed their support for creating a more secure ecosystem for home IoT devices and believe this can benefit the "common good." Panelist **Michelle Richardson** said, "We encourage people to design for the masses. We need people to accept that security is a common good."

Workshop participants discussed some key issues and challenges with defining what this ecosystem might look like, such as:

- ***The Magnitude of the Home IoT Ecosystem***—Participants agreed that the sheer size of the home IoT ecosystem is a challenge in and of itself. Panelist **Mark Haney** explained, "A device may have security, but the host may be vulnerable. Many times, the host is a critical part of the IoT ecosystem. And that ecosystem is vast." Panelist **Maarten Bron** added, "When you compare consumer IoT to industrial IoT, the main difference is the sheer size of it. With such a large attack surface, the number of devices increases along with the potential for an attack…attackers study vulnerabilities…Once one device is hacked, it opens up attacks to others."
- ***Managing Security Breaches***—**Mark Haney** said, "Devices installed in homes rely on an ecosystem to collect information and make decisions about things in your home. A breach can result in a loss of consumer confidence in a company or technology." Haney cited self-driving cars as an example of this phenomenon, where the entire industry—not just the individual car manufacturer—experienced a loss in consumer confidence as reports questioning the safety of the technology began to surface. **Michelle Richardson** added, "There is a lack of consequences for poor design; that is changing. Find problems in systems before there's an actual breach and enforce against them."
- ***Meeting the Core Baseline***—Panelist **Mike Bergman** said the baseline "is a strong foundational document to build on—not something you live in...engineers need detailed technical requirements." Workshop participants agreed that having examples of, and more information about how different IoT devices can work together in the home IoT

ecosystem is beneficial, and that customers (retailers, enterprises, consumers) need assurances that a home IoT product meets NIST's core baseline.

- ***Varying Degrees of Knowledge***—The home IoT ecosystem is impacted by the fact that manufacturers have different degrees of in-house cybersecurity expertise, skills, and capabilities that can influence how much cybersecurity they are capable of building into home IoT devices.

Takeaway 2: Manufacturers are challenged by balancing the design and functionality of consumer IoT devices against maintaining a viable cost structure for their target market.

Manufacturers are in the business of creating products that meet their customers' needs and goals, which are constantly shifting against a backdrop of perceptions and realities that influence the home IoT market, including:

- There is a widely held perception among manufacturers that consumers place a higher value on the design/functionality/aesthetics/usability of home IoT devices and a lesser value on security. As a result, manufacturers have invested more resources into creating designs that are feature-rich and user-friendly and less on cybersecurity. **Maarten Bron** said, "Some research indicates that in general, consumers perceive value in functions/features of a device. For manufacturers, cybersecurity is knowledge/resource intense." Panelist **Rebecca Herold** observed that "manufacturers invest more into making the device look good and easy to use." **Bron** said that manufacturers do not know where to start in terms of "baking security" into home IoT devices, and cited NISTIRs and other European government agency documents as helpful references for manufacturers.
- Some workshop participants challenged the perception that consumers do not value security as much as they do usability and features. Panelist **Jean Camp** said, "We're asking consumers to evaluate risk with no basis to do so. If you give people a default that offers privacy and security, they will choose to pay more. One study showed that consumers will pay on average $17 more for a lightbulb that's private and secure." Panelist **Rebecca Herold** added, "Manufacturers assume that consumers don't care if security isn't built in because if they wanted it, they would ask for it. The problem with that belief is that most consumers assume security is already built in and turned on by default."
- Manufacturers' delays in adding security features (encryption, adding more powerful processors, locked down interfaces, strong password usage) to home IoT devices may result in increased costs, design changes, or have an impact on functionality. **Mark Haney** gave an example of having to charge a smart watch battery daily versus weekly. Panelist **Andrew Tierney** gave another example using multi-factor authentication (MFA): "MFA represents a massive security improvement and stops password phishing. However, because consumers don't want barriers, some companies are hurt by deploying MFA. Consumers will go elsewhere." These examples illustrate what can occur when

manufacturers add cybersecurity device capabilities that consume substantially more power, and how that can create usability issues.

- Manufacturers must ensure they have adequate hardware to accommodate the customer's needs, with the understanding that maintaining cybersecurity is an ongoing effort that requires them to supply hardware/software and other infrastructure. Panelist **Rob Coombs** commented that consumers should be informed how long a manufacturer intends to provide software updates for their devices.

Manufacturers must perpetually weigh the benefits of added security with the costs to implement these features and the effect that additional security features can have on device usability and aesthetics. Because manufacturers have gained many insights into their customers' preferences and behaviors over the years, they are better positioned to meet this challenge.

Takeaway 3: Manufacturers can benefit by having a recognized business model around a "connected device lifecycle" that covers the mechanical and information technology (IT) components of a home IoT device.

Workshop participants discussed some of the key challenges with creating a standard business model or connected device lifecycle that addresses the distinct lifecycles for both the mechanical and IT components of a home IoT device, as follows:

- Because some home IoT devices' mechanical components have longer lifecycles compared to their IT components, this results in a gap between the expected useful life of the mechanical components compared to the IT components within the same device.
- Because mechanical components often outlive their IT counterparts, manufacturers often drop IT infrastructures (how secure is it, how long will it last, who provides updates, who performs updates, etc.) because they do not have the technical expertise. Therefore, the IT becomes obsolete, and/or the costs become prohibitively expensive over time. Panelist **Mike Bergman** said, "Manufacturers don't have a business model to support a device that lasts 20 years…infrastructures get dropped because manufacturers can't maintain them."
- **Mark Haney** observed that companies struggle to maintain their host environments, and said, "You don't hear a lot about abandoned infrastructure. For instance, a $49 smart night light is no longer IoT capable because its infrastructure was orphaned. Over time, you lose functionality."
- Participants raised the issue of making subscriptions available to consumers. **Mike Bergman** explained that manufacturers have started to experiment with subscription models to enable more functionality and to extend the life of the IT infrastructure, but more work is needed in this area.
- Consumers are developing more familiarity with maintenance of IT components across their lifecycle. This familiarity will help consumers understand what is required for a viable IT infrastructure. This may be more aspirational at this point. Ideally, this will

result in informed consumers valuing the maintenance of a device's IT infrastructure as they do the maintenance of mechanical components.

Takeaway 4: Consumers cannot bear the sole responsibility of maintaining cybersecurity on IoT devices.

Workshop participants generally agreed that consumers are being overwhelmed with maintaining security for IoT devices. Participants shared their diverse views around their perceptions of the consumer's role in maintaining cybersecurity for their home IoT devices, including:

- Cybersecurity should fall on manufacturers and integrators rather than consumers. **Jean Camp** said, "Seventy-one percent of IoT medical devices suffer ransomware infections that are caused by the user. People are incapable of making an informed decision without information, but they get blamed when an attack happens."
- Associations, manufacturers, integrators, and other stakeholders can create minimum security standards that IoT devices should meet before coming to market.
- Consumers expect retailers to sell home IoT devices that meet a minimum cybersecurity standard.
- **Mike Bergman** stated that the continued availability of resources such as NISTIR 8259A can improve the cybersecurity of home IoT devices. While the situation has improved over the past five years, more resources and guidance are needed to strengthen the cybersecurity of home IoT devices.
- Manufacturers can build security into IoT devices that conforms to a detailed baseline. **Dave Thaler** noted that consumers do not view security as a feature for most devices and that if manufacturers are meeting the core baseline, they should convey the benefits of doing so to the consumer in terms the consumer can understand.

Takeaway 5: Software and patch updates are critical to maintaining security, but a consumer's ability to deploy them is limited.

In a home environment, the consumer is responsible for deploying software updates and patches. These deployments are at the core of home IoT cybersecurity and are critical since unpatched known vulnerabilities remain a common root cause of cybersecurity incidents.

Workshop participants agreed that the typical customer's ability to securely configure and launch updates/patches for a device is limited and shared these observations:

- Consumers often do not understand the benefit of conducting updates or do not recognize the urgency. **Jean Camp** said, "We can't blame people for making decisions about security when there's no information about privacy and security provided to them." And as **Julie Haney** pointed out, "Personal responsibility doesn't always involve taking action. A consumer who buys an IoT device hopes or assumes that it is secure."

Workshop participants agreed that more education can help consumers understand why updates/patches are important to maintaining the cybersecurity of a device, and the relationship among security, safety, and privacy.

- Even if a consumer is informed about cybersecurity, they may not be able to act on a manufacturer's recommendation to secure a device for a variety of reasons (e.g., lack of technical ability, unwilling to spend time on making updates, complexity of varied schedules and methods for updates, etc.) **Julie Haney** said, "We found that people have a fair number of concerns around security…even if the owners want to do something, they don't know how to go about it."
- From a manufacturer's perspective, because of the complexity and size of the home IoT space, they each handle software updates differently. As a result, consumers are having inconsistent experiences with deploying updates, which may explain why consumers express confusion or ambivalence around patching. One solution is for manufacturers to push updates directly to a home IoT device—shifting the burden from consumers by automating software updates/patches.

Takeaway 6: Privacy plays a role in the manufacture and consumption of home IoT devices but is not well understood by consumers.

Consumers value privacy; however, workshop respondents agreed that they lack awareness around how their privacy is impacted when an IoT device is deployed in their homes. Moreover, workshop participants agreed that consumers can better understand the issues around privacy and how it affects them more than they can cybersecurity. **Jean Camp** said, "Consumers are willing to pay more for security/privacy, but they need information about security/privacy to make informed decisions." Consumers are also more concerned with infringements on their privacy, but do not feel empowered or know what actions to take to protect themselves. **Julie Haney** put it simply: "People don't trust manufacturers to respect their privacy." All combined, these factors give consumers a sense of discomfort around home IoT devices.

Workshop participants identified some key issues pertaining to privacy and home IoT devices as follows:

- **Third Parties**—Manufacturers may not routinely include a privacy policy explaining to consumers how their data is collected from their IoT devices and then shared with third parties. Privacy policies that are provided tend not to be easy to find or in plain language. As a result, consumers are left unaware and uninformed about the role of third parties and how much access they have to their information. Workshop participants generally supported greater disclosure, as **Rebecca Herold** explained: "Consumer IoT devices collect a massive amount of data that is rarely stored within the device, but in a cloud server. That data is shared downstream with other third parties**.** Consumers don't know how many third parties have this data because a privacy policy is not presented with details on how the device is used. Privacy is an afterthought, not an integral part of the design." **Maarten Bron** shared this caveat: "When it comes to data—if you can't protect it, don't collect it."

- **Information**—As part of the process of setting up an IoT device, consumers will share personal information such as name, home address, and email address. Participants touched on what might happen to this information should the infrastructure be abandoned but could not reach any conclusions. At the present time, there is no single, predictable model for what happens to that information.

Takeaway 7: Consumer education about home IoT cybersecurity should be an ongoing, shared responsibility among stakeholders.

In the home IoT market, consumers have a range of expectations, assumptions, and levels of awareness around the cybersecurity of these devices. Workshop participants examined some of the challenges around consumer education and home IoT device cybersecurity, which echoed some of the key points raised throughout the workshop discussions, including:

- As the IoT devices market matures and consumers become more familiar with IoT devices, they may start demanding that manufacturers make security a higher priority.
- Consumers are being asked to evaluate risk without enough information to make informed decisions. This needs to change.
- Consumers assume that security is built into an IoT device, but that is not always the case. In addition, there is an unreasonable expectation for consumers to secure devices when they may not have the ability or enough information from the manufacturer to perform this function.
- When manufacturers supply consumers with information about a device's security and privacy risks, consumers are better positioned to make informed decisions on whether or not to make the purchase and what is required of them.
- Consumers need more information on what security features to look for when shopping for a home IoT device.
- Manufacturers support the notion of consumer education but face challenges such as servicing a diverse customer base with varying abilities and motivations to process technical information.
- For maximum effectiveness, information about a home IoT device's security should be clear, easy to implement, and visible—similar to how information is displayed on a nutrition label.
- If manufacturers build in a certain security standard by default, consumers should have information that is easy to understand and explains how to configure a device to their liking, e.g., turning certain functions on/off or opting in/out of certain settings.
- Some studies reveal that when consumers have information about security, they are willing to pay more for a device. Conversely, manufacturers will need to weigh how much building security in will cost and if their target market is willing to make the tradeoff (higher costs for more security).

- Consumers do not have a mechanism for recognizing which devices meet security baselines and which do not. Customers expect devices to be initially secure, but confidence mechanisms for establishing that security are not available.

3 Next Steps

The NIST Cybersecurity for IoT program has identified the following next steps taking into account the takeaways from the workshop, the feedback on draft NISTIR 8267, and ongoing efforts:

1. ***Survey the Options for Confidence Mechanisms for IoT Devices***. NIST should work with consumer groups, industry, standards bodies, and other stakeholders to survey options for confidence mechanisms that enable identification of cybersecurity device capabilities in consumer home IoT devices.
2. ***Address Software Update and Patching Complexity***. NIST could explore ways to work with consumer groups, industry, academia, and other interested stakeholders to address the complexity of software updating/patching and the limits of consumers' ability to manage updates/patches.
3. ***Consider a Consumer Home IoT Device Profile***. NIST could consider how a consumer home IoT device profile of the core baseline might be structured to address the specific concerns of this market.
4. ***Perform an Analysis of the Available Guidance for Consumer IoT Cybersecurity***. NIST could conduct an analysis to identify the standards, guidance, and tools currently available; how the standards and guidance overlap and where any critical gaps exist; and what would best support consumer IoT device manufacturers in implementing better security in IoT devices.
5. ***Determine appropriate revisions for the Product Security Survey***. NIST should consider revising NISTIR 8267, *Security Survey of Consumer Home Internet of Things (IoT) Products* with comments from the workshop.

References

[1] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[2] Fagan M, Yang M, Tan A, Randolph L, Scarfone K (2019) Security Review of Consumer Home Internet of Things (IoT) Products. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8267. https://doi.org/10.6028/NIST.IR.8267-draft

[3] National Institute of Standards and Technology (2020) *NIST Cybersecurity for IoT Program*. Available at https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[4] National Institute of Standards and Technology (2020) *Workshop on Cybersecurity Risks in Consumer Home IoT Products*. Available at https://www.nist.gov/news-events/events/2020/10/workshop-cybersecurity-risks-consumer-home-iot-products

[5] National Institute of Standards and Technology (2020) *Next Steps for the Cybersecurity for IoT Program in the Development of a Federal Profile of NISTIR 8259A*. Available at https://pages.nist.gov/FederalProfile-8259A

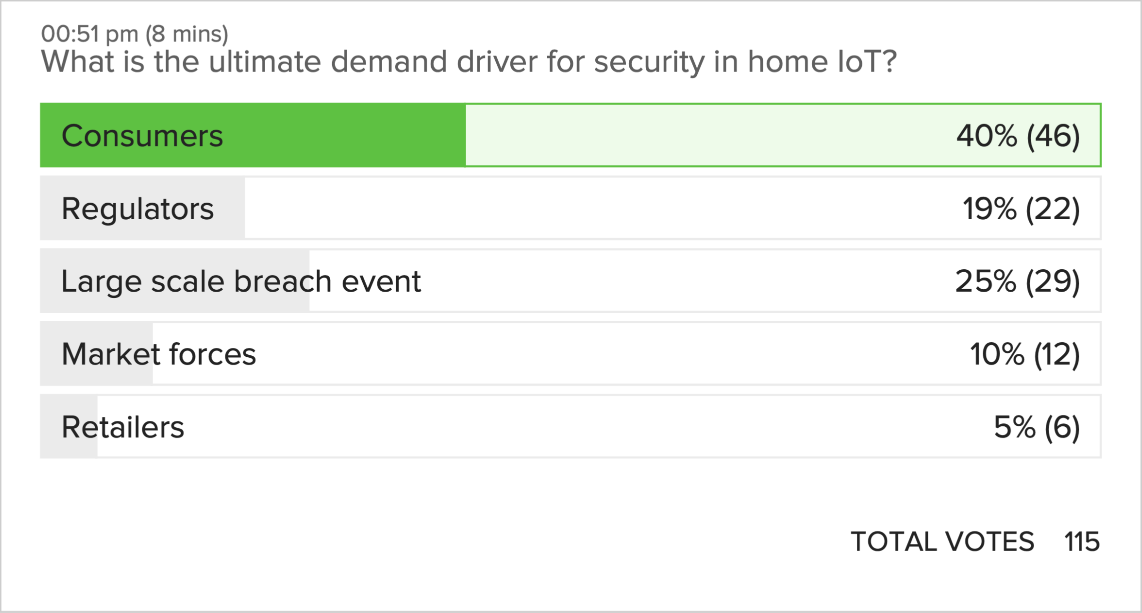
Appendix A—Poll Results

Six online polls were conducted during the workshop. The polls gathered participant viewpoints on a variety of topics related to the challenges of cybersecurity risks for consumer home IoT devices. Since workshop attendees created a by-definition, self-selected survey group and poll responses were entirely voluntary, poll results should be not viewed as providing generalizable results for their questions.

Note: the most popular result for each poll is highlighted in green and the shading provides a visual depiction of how popular each selection was.

Poll questions and results are provided below.

A.1 Ultimate Demand Driver for Security in Home IoT



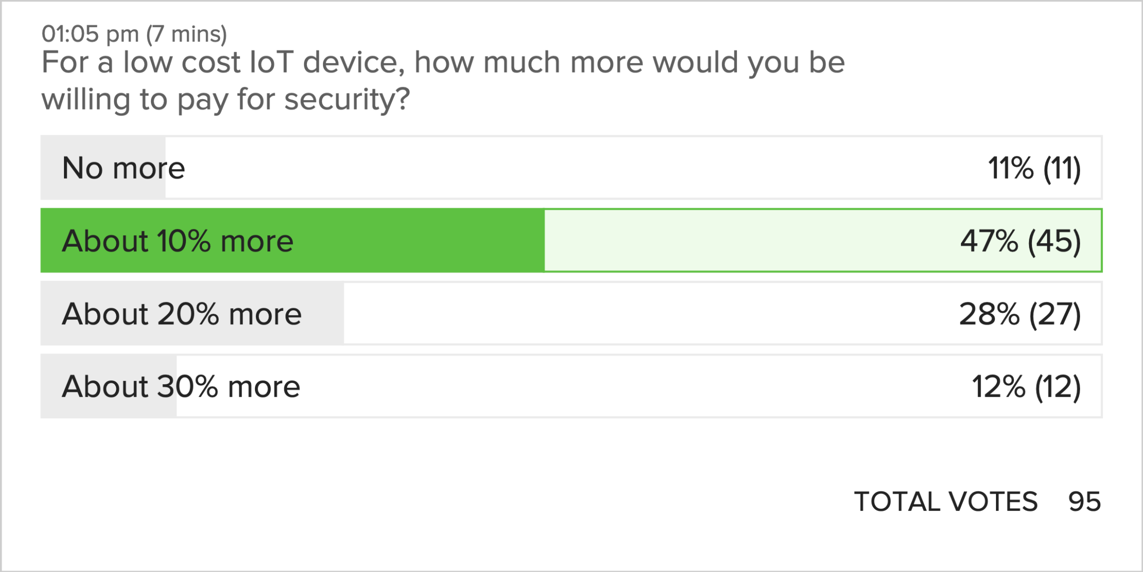
00:51 pm (8 mins)

What is the ultimate demand driver for security in home IoT?

Consumers	40% (46)
Regulators	19% (22)
Large scale breach event	25% (29)
Market forces	10% (12)
Retailers	5% (6)

TOTAL VOTES 115

A.2 Willingness to Pay More for Security in Low-Cost IoT Devices



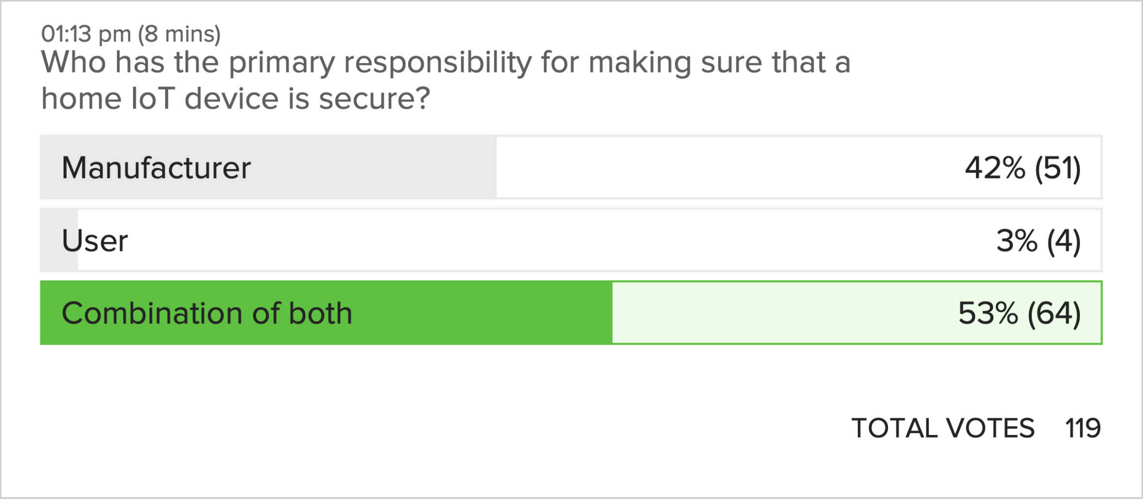
01:05 pm (7 mins)

For a low cost IoT device, how much more would you be willing to pay for security?

No more	11% (11)
About 10% more	47% (45)
About 20% more	28% (27)
About 30% more	12% (12)

TOTAL VOTES 95

A.3 Primary Responsibility for Home IoT Device Security



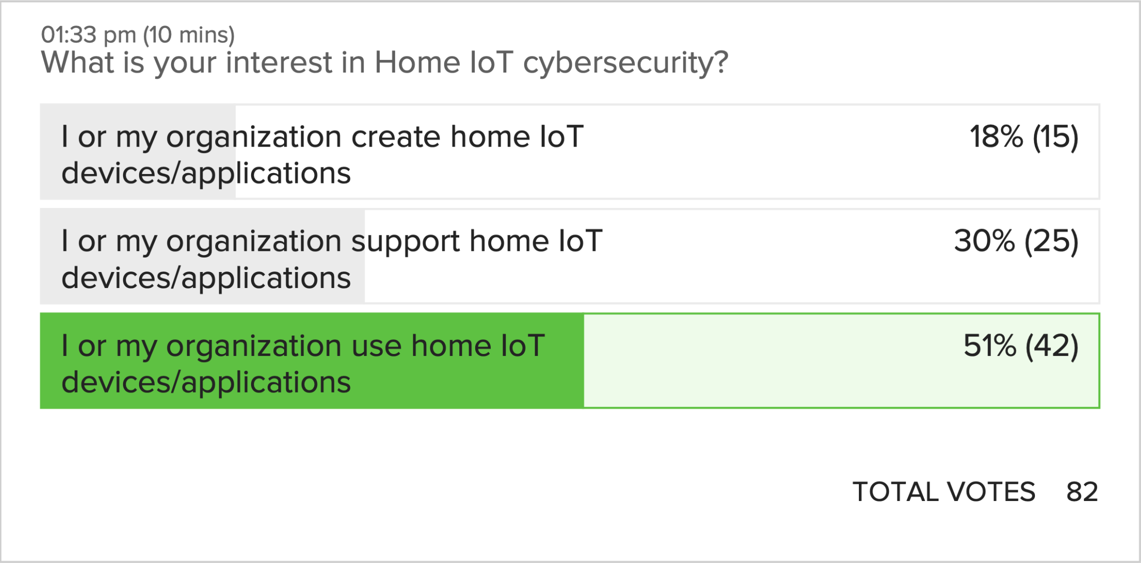
01:13 pm (8 mins)

Who has the primary responsibility for making sure that a home IoT device is secure?

Manufacturer	42% (51)
User	3% (4)
Combination of both	53% (64)

TOTAL VOTES 119

A.4 Reason for Interest in Home IoT Cybersecurity

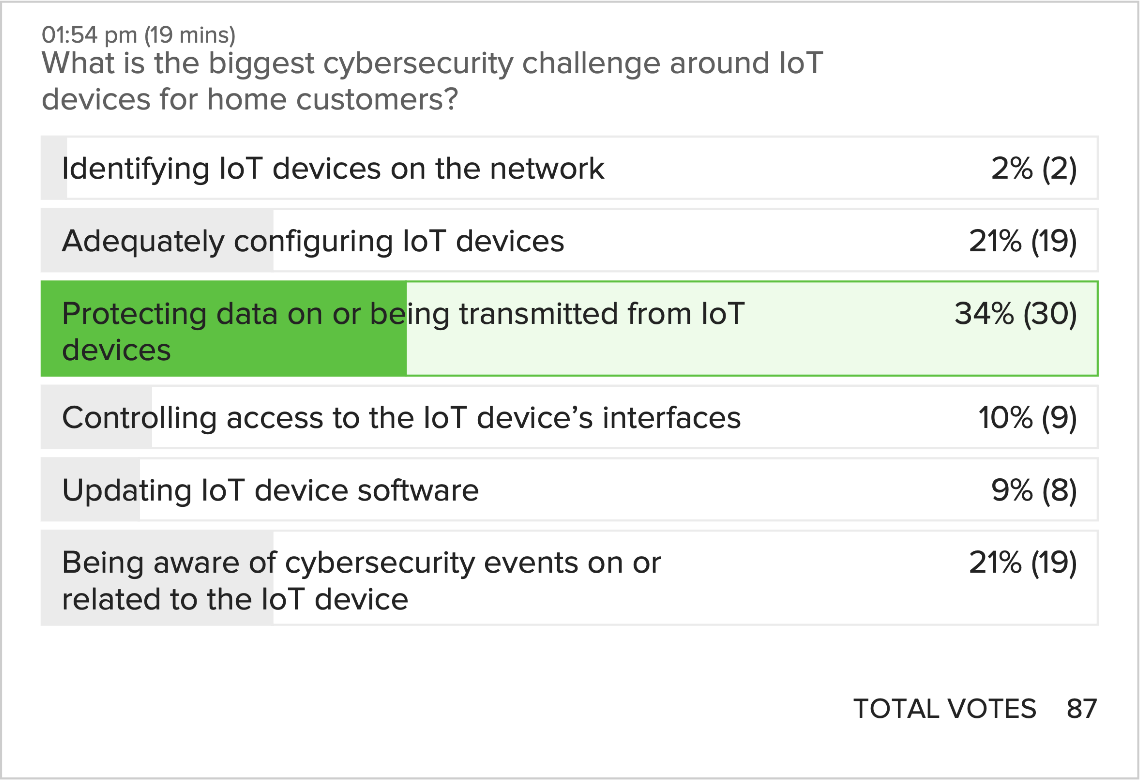


01:33 pm (10 mins)
What is your interest in Home IoT cybersecurity?

I or my organization create home IoT devices/applications	18% (15)
I or my organization support home IoT devices/applications	30% (25)
I or my organization use home IoT devices/applications	51% (42)

TOTAL VOTES 82

A.5 Biggest Cybersecurity Challenge for IoT Devices for Home Customers

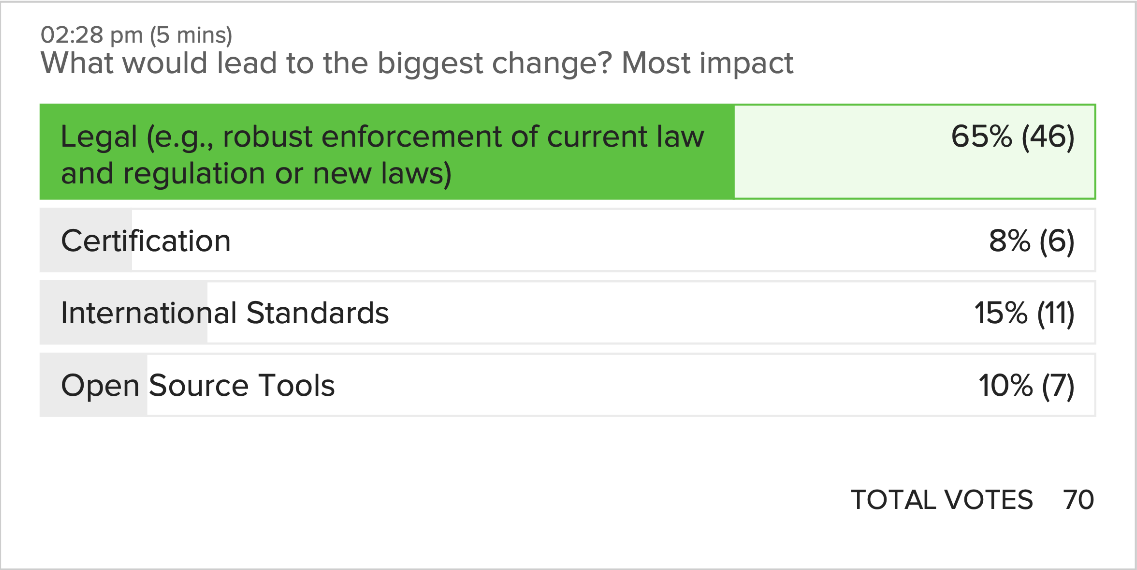


01:54 pm (19 mins)
What is the biggest cybersecurity challenge around IoT devices for home customers?

Identifying IoT devices on the network	2% (2)
Adequately configuring IoT devices	21% (19)
Protecting data on or being transmitted from IoT devices	34% (30)
Controlling access to the IoT device’s interfaces	10% (9)
Updating IoT device software	9% (8)
Being aware of cybersecurity events on or related to the IoT device	21% (19)

TOTAL VOTES 87

A.6 Biggest and Most Impactful Force for Change



02:28 pm (5 mins)
What would lead to the biggest change? Most impact

Legal (e.g., robust enforcement of current law and regulation or new laws)	65% (46)
Certification	8% (6)
International Standards	15% (11)
Open Source Tools	10% (7)

TOTAL VOTES 70

Appendix B—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CTA	Consumer Technology Association
FOIA	Freedom of Information Act
IoT	Internet of Things
IT	Information Technology
ITL	Information Technology Laboratory
MFA	Multi-Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
SP	Special Publication