IoT World Today

Published in collaboration with Internet of Things World

NEXT ▶

Overcoming the Smart Home Market's Top Challenges

While smart home adoption grows, the landscape remains fragmented and unsecure. Here's how the market can move forward.

By Brian Buntz

TABLE OF CONTENTS

AUTHOR'S PAGE

Brian Buntz

IoT World Today

Brian Buntz has served as content director for IoT World Today since 2016. He is a veteran journalist with more than 10 years of experience covering an array of technologies, including the Internet of Things, 3D-printing and cybersecurity. Prior to his current role, he served as the editor in chief of UBM's Qmed, where he overhauled the brand's news coverage and helped to grow the site's traffic volume dramatically. He previously held managing editor roles on the company's medical device technology publications including European Medical Device Technology (EMDT) and Medical Device & Diagnostics Industry (MD+DI), and served as editor-in-chief of Medical Product Manufacturing News (MPMN).

At UBM, Brian also worked closely with the company's events group on speaker selection and direction and played an important role in cementing famed futurist Ray Kurzweil as a keynote speaker at the 2016 Medical Design & Manufacturing West event in Anaheim, California.

In 2017, the B2B social media firm Leadtail selected Brian as one of the most influential people (No. 14) for IoT leaders.

EXECUTIVE SUMMARY

Understanding the smart home market entails pondering seeming contradictions and tough realities. One of the largest segments of the smart home market includes security devices such as video doorbells and connected surveillance cameras, and yet, many consumers find smart home devices intrinsically creepy. On the one hand, the smart home market includes digital interfaces, including smart speakers, which are among the quickest-growing products since the iPhone catalyzed the modern smartphone market. But on the other hand, the notion of the smart home itself is a sort of question mark or at least has failed to achieve universal support. Google Nest Vice President of Product and General Manager Rishi Chandra for one prefers the phrase "helpful home." IoT author Stacey Higginbotham declared the smart home to be dead in November, pointing to Chandra's rebranding of the smart home as part of the defense of that argument. The other crux of her argument is the observation that the capabilities of intelligent assistants have evolved more slowly than expected in the past several years.

While "dead" is much too strong of a word to describe a market that is maturing gradually, it is true that many smart home devices are buggy and tend to offer fragmented functionality. The 1950s and 1960s sci-fi visions of a future with domestic automation remain a dream.

Vendors have come a long way in the past several years in communicating the benefits of connected devices with consumers. As a result, consumer appetite for the technology is significant. This year, IDC estimated that the global smart home market will expand by 27% while projecting it will grow at a 17% rate annually from 2019 to 2023. Strategy Analytics is less bullish, anticipating the market will grow at 11% between now and 2023, reaching a $157 billion valuation in 2023.

Leading smart home vendors don't seem to be profiting handsomely from their success in the near term. Despite selling millions of Alexa products, Amazon doesn't disclose the revenue the product line generates, and the retail giant remains the most dominant company in the smart home market.

Part of the problem is that it remains unclear what a smart home is, or should be. Given the variable habits of consumers, it is likely the answer to that question depends largely on who is asking. For the broader smart home industry to mature, however, vendors need to collaborate to develop a more comprehensive and transformative vision.

By contrast, the first smartphones represented a dramatic upgrade over previous cellphones. And thus, the use of the descriptor "smart" to describe the capabilities of smartphones made sense in circa 2007. Such devices would ultimately go on to transform consumer expectations and habits, causing the market for traditional cellphones to quickly collapse. By 2009, nearly all cellular phones were becoming "smart," as Forrester noted.

Similarly, we are approaching a reality in which many appliances and devices, from televisions to speakers, are "smart" by default. But as we enter a new decade, it is still not clear how transformative such products are, either individually or in concert.

4 Steps to Unleash the Smart Home Market

The Smart Home Market has yet to see explosive growth. To set the product niche free requires a concerted effort in addressing its biggest stumbling blocks.

In the middle of the last century, companies ranging from General Motors (which then owned Frigidaire) to the radio company Philco released promotional films showcasing visions of the futuristic home, often centered around the kitchen. Home automation was a central theme. Some of the elements of such films have become a reality, or nearly so. The idea of pervasive computing seems within reach. The 1967 film titled "Year 1999 AD" predicted a refrigerator that can suggest menus based on the needs of family members. One theme common in such films that hasn't become a reality is the notion of discrete computing systems working in concert. Though today's vision of the smart home may bear a significant resemblance to the mid-century predictions about the future of domestic living, they couldn't predict how fragmented it would become half a century later. Or have foreseen the privacy-eroding consequences that tend to accompany a tech-laden domicile.

As we transition to a new decade, vendors

active in the smart home market need to carefully study their consumers' pain points — both the ones their products inadvertently cause, and the ones their products could potentially address.

1. Address the Smart Home's Often Unclear Value Proposition

The capabilities of smart home devices are so varied, there is no clear selling point for such products. They promise to offer home automation, enhanced physical security and entertainment. While all of those are noble goals, the benefits of the current crop of smart home devices in each of those domains are mixed.

Part of what drove the success of the smartphone was the presence of compelling use cases — killer apps. While there isn't a consensus on what exactly a killer app is, it is clear that everything from a smartphone's camera functionality and flashlight feature to navigation to ride-sharing apps to review apps like Yelp has had a transformative impact on consumers.

In the smart realm, there isn't a clear "killer app," according to Bill Ablondi, who directs the Strategy Analytics Smart Home Strategies advisory service.

There is also more room for differentiation and tighter integration. While the industry has come far in the past five to 10 years in terms of the breadth and depth of offerings, many products in the smart home landscape are broadly similar. Leading companies should design next-generation products with clear market differentiation centered around core user needs. It is ironic that many vendors selling products for use in the home have incorporated connected sensors with the aim of distinguishing their products in the marketplace, but have often failed to provide a fundamental level of usability of security in doing so.

In terms of better integration, the industry should strive to do a better job of finding synergistic opportunities to combine the functionality of smart home devices. For instance, if a connected surveillance camera or security system collects data indicating a potential break-in, they could sound an alarm while turning on smart lights as a potential deterrent.

> "While the industry has come far in the past five to 10 years in terms of the breadth and depth of offerings, many products in the smart home landscape are broadly similar."

2. Make Usability a Central Priority

While smart home devices should be useful, they also shouldn't fail when it comes to usability. The basic idea behind home automation is that it frees up time doing chores. But frequently, the devices that enable such a vision require hand-holding themselves. One example of that is a smart light bulb that is surprisingly difficult to restore to factory settings. An instructional video demonstrating how to do just that went viral. The first portion of the video demonstrated the necessity of turning off the bulb for at least five seconds and then turning it on for eight seconds, and then turning it off for two seconds for five times in a sequence, before finally turning it on one last time. Complicating matters is the

fact that the bulbs with an older firmware variant require a different instruction sequence. Trying to figure out the difference either requires knowing the firmware version, or remembering the type of packaging the bulbs arrived in. A YouTube video with the instructions attracted streams of snarky remarks.

While that is one extreme example, the usability of many smart home technologies is questionable. The servers that power the functionality of virtual assistants occasionally go down, while glitches cause alarms not to sound.

While design thinking and design-focused ethnography have achieved mainstream status for many consumer products and apps, such concepts are less common in the world of the smart home.

After reviewing a small army of smart home devices, Paul Boag, founding partner of user experience at consultancy Boagworks Ltd, concluded bluntly in a March 2019 podcast: "In the majority of situations, the user experience sucked. The number of issues I have encountered [included] fitting, setting up and using smart home devices is frankly staggering."

Part of the problem is the preponderance of walled gardens. While many new smart home devices offer support for Google Home, Apple HomeKit and Amazon Alexa environments, users with hybrid environments must configure smart home devices to work with each environment they offer.

And then there are the apps. A decade ago, Apple gleefully boasted in a commercial that there was an app for pretty much everything. When it comes to the smart home though, that isn't necessarily a good thing. While there are apps for smart home platforms like Alexa as well as smart air purifiers, ceiling fans, outlets, irrigation systems and more, a typical user wants to interact with software apps for the smart home as little as possible. If voice control is destined to emerge as a potentially default way of controlling many smart home devices, opening an app on a smartphone or tablet shouldn't be a prerequisite to enable such voice control of, say, a connected thermostat via a smart speaker.

Part of the promise of virtual assistants is that they give users new options for interacting with consumer devices. But despite considerable advances in such systems in understanding speech commands, these systems continue to

fail when it comes to understanding non-routine commands.

To improve the situation requires a concerted effort on the part of the industry to think less about selling consumers products and subscription services and using their personal data for marketing purposes, and more about how to improve their lives.

Smart home device makers need to provide products that are not only easier to use and configure but offer comprehensive customer support as well. Smart home devices should also be resilient, capable of recovering from power and connectivity disruptions and perhaps able to operate, to an extent, without the latter. For instance, a smart fan that fails to function upon resetting a router isn't so intelligent. Such a product should fall back to operating like a traditional fan upon losing connectivity.

Smart home products that require an app for full functionality should ensure such products are rigorously tested. Consider a user's frustration in purchasing a so-called smart plug to preheat an espresso machine daily at 5 a.m., only to find that the app it uses has a bug that prevents the timer from working.

One challenge is that many of the companies active in the smart home market come from a consumer electronics or home appliance background. Consequently, they tend to lack

> "Smart home device makers need to provide products that are not only easier to use and configure but offer comprehensive customer support as well."

experience relating to connected devices, app development and the like. The genesis of many smart home products consists of taking an existing product and adding IT technology to it to give it new functionality. Such was the case with the Amazon Echo. Its designers conceived it as a smart speaker rather than a hub to unify the functionality of various smart home gadgets. But the capabilities of the technology steadily evolved, thanks in part to internal development efforts and a robust third-party developer ecosystem along with Amazon's decision to make its Alexa platform open. As a result, the device provided a more convenient way for consumers to control smart home devices than opening up a smartphone app for individual connected gadgets.

While the emergence of smart speakers and hubs helping unify consumer interactions within the home solve an inherent problem for early smart home adopters, companies active in this market will need to take a more proactive approach to spur further growth. Striving to develop flawlessly functioning products is a vital ingredient, but, ultimately, companies active in the smart home market should work to solve unmet consumer needs as efficiently as possible. As designer Golden Krishna wrote in a book of the same name: "The Best Interface Is No Interface."

3. Strive to Make Smart Home Products More Universal

Roughly one-third of smart home households are millennials, according to Strategy Analytics, which also found that a clear majority of users are male. Smart home users also tend to be wealthier than average. And, perhaps not surprisingly, they tend to be homeowners rather than renters.

The situation may be improving. While cost

is “somewhat of an inhibitor” on sales of smart home devices, according to Ablondi, prices have fallen considerably in recent years.

As mentioned earlier, usability is an element here, as well. In the early days of the smart home, many devices such as smart lights required a separate hub using a wireless protocol such as Z-Wave or Zigbee to operate. Now, such functionality is included in a growing number of smart speakers

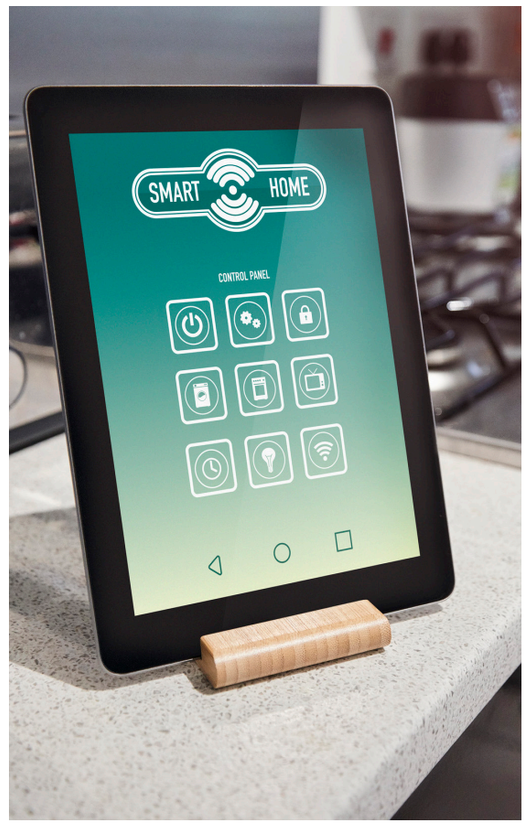
Additionally, device makers need to look to help connect the dots — among multiple family members and the growing variety of smart devices in a typical household.

4. Aim to Create Trustworthy Devices, Rather Than ‘Creepy’ Ones

A survey of roughly 6,000 consumers in six countries revealed 63% of respondents believed IoT devices generally were “creepy.” Nearly three-fourths believed users of smart home devices should worry about the potential for unauthorized data collection. In addition, 55% reported not trusting such connected devices, according to the survey from IPSOS Mori, which was conducted on behalf of the Internet Society and Consumers International. The consumers involved in the study were based in the United States, Canada, Japan, Australia, France and the United Kingdom.

A significant number of consumers, 77%, would factor information on security and privacy features into their buying decision, according to the research. “It’s behind cost and features, brand and some of the other things you would expect, but it is pretty high up there,” said Jeff Wilbur, technical director of the Online Trust Alliance.

While there is significant data to suggest



many consumers are uneasy about the privacy ramifications of smart home gadgets and other connected consumer products, that concern doesn’t prevent many consumers from buying them. Roughly 30% of consumers state they wouldn’t buy such devices out of concerns for security and privacy, Wilbur said, reflecting on the aforementioned survey and other similar research. “Then when you get to the actual purchases, only 5% or 10%, don’t buy because of lack of security and privacy,” he said. Wilbur theorizes most consumers don’t focus on security and privacy features more when purchasing a product because there is little to no information available on the subject. “So they just buy [connected devices], and hope for the best.” (For more on this subject, see “Expect Better-Informed Smart Home Consumers.”)

The situation could be changing thanks to the passage of legislation such as the California Consumer Privacy Act and California Senate Bill 327 and Oregon’s House Bill 2395, which hold manufacturers of connected devices accountable for including “reasonable security features” in their products. Those laws go into effect on January 1, 2020.

Already, a handful of vendors, such as Apple, are positioning themselves as privacy protectors. The company’s Chief Executive Officer Tim Cook has called for comprehensive U.S. data-privacy

protections. Apple, as well as Google and Amazon, has also announced plans to retool how it handles the data gathered by their smart speakers.

But it remains difficult for consumers to evaluate the security protections included in popular smart home products. In the future, however, it may become more manageable. The global safety assurance firm UL is unveiling an IoT Security Rating intended for retailers and device manufacturers. The rating system consists of five tiers, starting with bronze at the lowest level and extending to platinum and diamond at the upper end. The organization states that the security framework behind the initiative is the first of its kind. The IoT Security Rating weighs the potential of connected product security features to defend against frequent attacks and known exploits.

Already, there are a significant number of examples of organizations that have woven security features into their products or services as well as providers that helped another smart home firm layer security on top of a partner's service. "There are good examples of this [trend], whether it's Plume's partnership with Comcast or what Minim is doing in home security," said Marc Sorel, associate partner at McKinsey. In the first example, the startup Plume is working with the cable provider to enhance customers' connectivity while also deploying software-based security protections. For instance, Plume can filter out suspicious content while quarantining compromised IoT devices. Minim offers similar Wi-Fi management and IoT security service to internet service providers. Both companies are "examples of players that have identified ways to provide a layer of security and privacy on top of the products that are already in the home," Sorel said. They show the power of deploying security and privacy features as a source of differentiation in the marketplace.

"Ultimately, companies interested in the smart home marketplace should incorporate security and privacy features into their product development life cycle, while ensuring they are following best practices and standards such as ISO/IEC 27001."

Ultimately, companies interested in the smart home marketplace should incorporate security and privacy features into their product development life cycle, while ensuring they are following best practices and standards such as ISO/IEC 27001. Such organizations should also be more forthright about how they plan on using user data, and in winning the trust of users with their varying privacy thresholds, rather than seeing privacy as a chore for the legal team to handle when drafting an end-user license agreement. Finally, companies active in this market "should incorporate [what they are doing in terms of security] in discussions with customers — not necessarily customers in the home but potentially channel partners — to help drive differentiation from their peers," Sorel concluded.

Expect Better-Informed Smart Home Consumers

Traditionally, potential buyers of smart home decives lacked an objective means to compare those products' security features. That's beginning to change.

In game theory and economics, there is the concept of perfect information. In a game, the notion refers to a player's ability to observe a rival's moves, such as in chess. In economics, buyers and sellers with perfect information are informed about the utility and price of a given product. There is a related notion of complete information in which participants have full knowledge of their opponents' objectives.

The smart home market, in a sense, provides imperfect and incomplete information to consumers. The buyers of smart home devices don't know how the data such devices collect will be used or who, ultimately, will have access to it. In addition, information on the security and privacy protections included in such products is scarcely available.

The situation leaves many consumers feeling that smart home devices are "creepy," as reported in the accompanying article. The trend of traditionally analog devices — ranging from televisions to ovens and refrigerators — going digital underscores the importance of establishing a security baseline. "If you look at the exploits and problems we see with IoT systems, they're often not cutting-edge zero-day attacks," said Andrew Jamieson, director of security and technology at UL. "They're not somebody exploiting, say, a row hammer attack on a section of memory." More significant worries include the common use of universal default passwords or

bad implementations of cryptography and key management.

While smart home vendors had an incentive to skimp on security protections given the frequently thin margins of their wares, pressure is beginning to mount to provide "reasonable security features." California Senate Bill 327 and Oregon House Bill 2395 both go into effect on January 1, 2020. Both demand reasonable security controls in IoT devices, and allow for sanctioning of manufacturers that don't comply.

Organizations ranging from Arm to UL have been working to establish objective criteria that could ultimately lead to a sort of rating system for consumers for a device's cybersecurity features. It is likely that through legislation, voluntary marking systems will pop up around the world, according to Jamieson. And as a result, a segment of the consumer base is likely to seek out and pay more for products that meet a given threshold, as they do in the case of organic produce. In the end, "customers can say: 'Yes, I'm going to purchase that product [with enhanced security features]. Maybe I'll spend a little bit more money because I understand that they are looking out for me in terms of security,'" he said.

While it is relatively simple to conclude that a smart device that uses a default username and password presents a cybersecurity risk, it is a different proposition to find a secure product. For one thing, smart home devices are so variable, that the level of concern for, say, a smart lightbulb owner will likely be dramatically different than those of a person purchasing a smart door lock or IP camera for use indoors.

There are presently a variety of efforts underway to evaluate the security features of consumer IoT devices. Another prominent effort is the result of a collaboration between researchers from the University of North Carolina at Chapel Hill and Georgia Institute of Technology. Known as the YourThings Scorecard, it currently presents rankings for 45 devices and assigns them a letter grade from A to F along with a corresponding numeric ranking on a base-100 scale. The website gives separate scores for the cybersecurity features of the device itself in addition to its mobile, cloud and network security safeguards. Few of the products on the list score a good score across all four categories.

Omar Alrawi, a graduate research assistant at Georgia Institute of Technology acknowledged it is difficult to predict how cybersecurity ratings systems will affect consumers' buying habits. "Our approach is to inform consumers, vendors, researchers and legislators of the risks associated with smart devices," Alrawi said. "Security is hard to quantify, even for experts. One of the primary objectives of the YourThings initiative is to set a minimum bar for the security of IoT devices through a grading system."

The researchers aim to fully automate the security evaluation process to help expand the number of devices included on the site. "[W]e have received a lot of attention and requests to review more IoT devices and rate them," Alrawi said. "The next steps we are undertaking include adding more devices, reevaluating devices — since their security will change over time — and expanding into other aspects of IoT devices such as analyzing the security of low-energy protocols (Bluetooth, ZigBee, ZWave, etc.)."

The research project is supported by several grants, including from the U.S. Department of Commerce, the National Science Foundation, the Air Force Research Laboratory and the Defense Advanced Research Projects Agency.

Ultimately, as a growing number of devices designed for use in the home — ranging from lawn mowers to security cameras — gain software-defined and networking features, there is an increased risk of software- and cybersecurity-related risk to health and safety. "In the next decade, it's going to be very difficult to look at a product only from an analog point of view without really looking at the software that's in there as well," Jamieson said.

Internet of Things World

April 6 - 9, 2020
San Jose Convention Center
CA, USA

#IOTWORLD

THE INTERSECTION OF INDUSTRIES AND IOT TECHNOLOGIES

North America's largest IoT event, where strategists, technologists and implementers connect, putting IoT, AI, 5G and Edge into action across industry verticals.

GET THE INTERACTIVE BROCHURE