PARKS
ASSOCIATES

Cybersecurity Impact on Smart Home Market Growth

A Parks Associates Whitepaper

Cybersecurity Impact on Smart Home Market Growth

This whitepaper reports on the market impact of cybersecurity features in home systems and devices.

Smart home applications are delivered by components interconnected via a home communications network that may be wired or wireless. Such components are often called "Internet of Things" (IoT) or smart home devices.

Many of these devices also exchange messages with external servers via the internet for applications such as a:

- **Smart thermostat** that communicates with the manufacturer's server as part of a learning program to improve comfort.
- **Smart TV** that communicates with the manufacturer for app functions including voice commands and streaming video.

> Consumers will purchase more than 485 million connected consumer devices in 2021, including smart home, connected health, mobile, and connected entertainment products. By 2022, sales will exceed 520 million units.
>
> © Parks Associates

Parks Associates conducts in-depth quarterly surveys of 10,000 broadband households to learn about their purchases, purchase intentions, and interest in new features and applications. **Nearly one-third of broadband households own a smart device that includes remote monitoring.** Consumers are becoming aware of cybersecurity risks to their personal data from unauthorized access of these devices. This is influencing purchase decisions.

This whitepaper examines the reality, benefits, challenges, and possible technical solutions for cybersecurity. It also addresses methods to deal with consumer concerns about excessive collection of private data. Technology is emerging based on standards for communication gateways that guard and limit access to private data.

Smart home device ownership tripled between 2014 and 2018 with broadband households owning an average of six smart devices. Here are some key findings about the impact of cybersecurity on such products, which could influence market growth:

- **63%** of the general public are concerned about cybersecurity.
- **71%** of those with smart devices are concerned about cybersecurity.
- More than **40%** do not trust companies to keep their data safe.
- **54%** do not feel they get much in return for sharing data.
- 25% of those who do not own smart devices reported having concerns about privacy and security.

© Parks Associates

PARKS ASSOCIATES

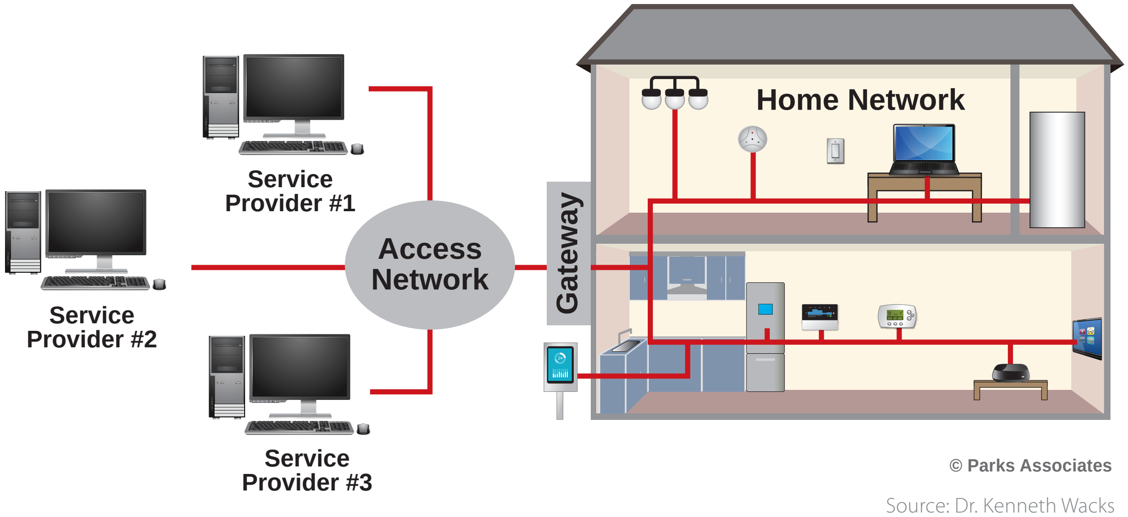
Home Devices Become Cyber Devices

Home devices are increasingly vulnerable to cybersecurity attacks that affect operation.

The press regularly reports incidents where consumer data have been lost or stolen. Consumers are concerned about data breaches; manufacturers have been focusing on protecting data when sent between consumer devices and service provider computers. The term cybersecurity has been the common label for protecting the transmission of consumer data. This is becoming a narrow view of cybersecurity because home devices are increasingly vulnerable to cybersecurity attacks that affect operation and data accumulated within these devices.

The devices and systems in our homes have been changing from electrical and mechanical to electronics and computers. This change started with TVs and other entertainment devices that were originally built with tuners and audio/video features wired into circuit boards. TVs are now designed with programmable controllers. Traditional devices such as light bulbs, doorbells, and thermostats have fixed functions. Now some versions of these devices, relabeled as IoT, include embedded firmware that can be updated remotely. These devices are interconnected via a home network, which is often linked to external servers through a gateway between the home network and an access network such as the internet.

Smart Home Devices Linked to Service Providers



Source: Dr. Kenneth Wacks

According to the National Institute of Standards and Technology (NIST, US Department of Commerce), cybersecurity "is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein …."[1]

Broadly speaking, the devices in a connected home consist of the following:

- **Sensors** for detecting physical phenomena such as temperature, occupancy, and light levels.
- **Actuators** for operating physical devices such as relays and motors.
- **User interfaces** for gathering user preferences and informing users. User interfaces range from wall switches to keypads to touch panels to voice-recognition systems including "smart speakers."
- **Controllers** for processing sensor, actuator, and user interface data.

The protections used for personal computers, such as anti-malware programs, need to be adapted for home system components since many include computer functions making them vulnerable to cyber attacks.

[1] https://csrc.nist.gov/glossary/term/cybersecurity

Customer Data Security

For efficiency reasons, the principal of a shared bus (wires and radio channels carrying digital data packets) has been adopted for internet communications and local area networks, which form the pathways for home networks. Every device on the shared bus can see the packets traveling to the other devices on the bus. Devices are programmed to read the digital data contained in packets addressed to them and to ignore the other packets.

> Some devices might be inadvertently or deliberately programmed to read data intended for other devices.

Until home systems proliferated, there was little concern about protecting data. Now that more important control and personal data may be contained in these packets, these data have become targets for thieves. This is why cybersecurity techniques were developed.

Achieving data security on a shared-medium network is challenging. There are well-established techniques for data security that depend on a set of rules, protocols, and secrets known only to the sender and recipients. Messages are protected by limiting access to the bus and by making the data unintelligible except to the recipient.

Security can be inadvertently compromised by a weak link – perhaps a device that is miscoded or a trusted entity with a database that was not properly updated. Data security could be threatened deliberately for malevolent purposes. Adding layers of security for appliances, home devices, and interfaces to public access networks via a gateway can enhance protection against these threats. A standard for the gateway is under development to incorporate cybersecurity features that complement security features embedded in some home IoT devices.

Cybersecurity is embodied in the principles of *security-by-design.*

The Cybersecurity Sentry

With the growth of the internet for home services, consumer product sales are being combined with subscriptions to these services. Subscriptions require data flows between home systems and external servers via a gateway. The gateway can provide a layer of cyber protection by screening and filtering data, thereby providing "data sentry services." Nevertheless, cybersecurity is ultimately the responsibility of product manufacturers and service providers.

> Manufacturers can use standards as a platform for developing innovative applications.

In 2018, the United States proposed a series of international standards for a communications gateway that could be extended with gateway sentry functions to monitor and manage data flows into and out of a house or building. These proposals were offered to an international committee (ISO/IEC[2]) that develops standards for the interconnection of electronic equipment and products for homes and buildings. The project to develop gateway cybersecurity standards was approved by the voting nations in 2019 without objection. International standards organizations were established in the twentieth century to foster commerce as a productive alternative to commercial and military conflicts among nations. These standards are all voluntary and are intended to promote trade.

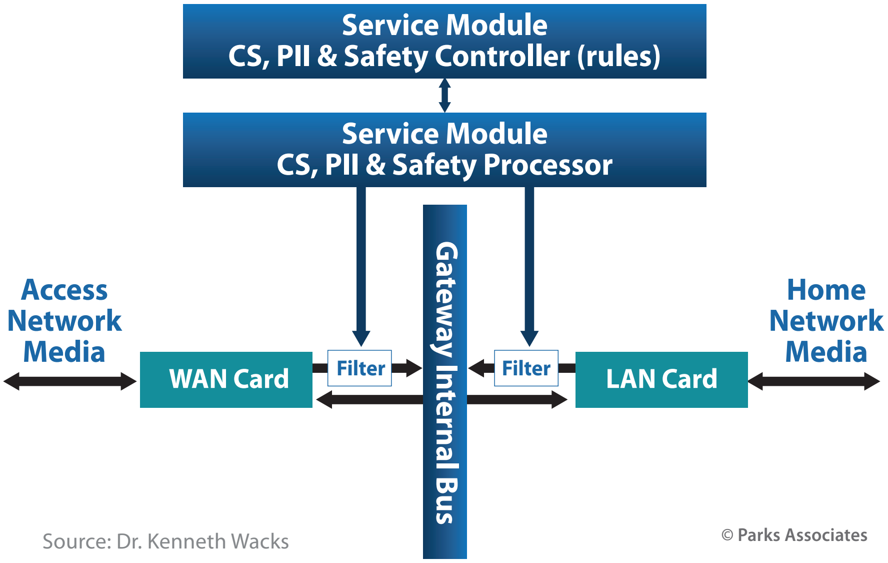
[2] ISO = International Organization for Standardization
IEC = International Electrotechnical Commission
ISO and IEC collaborate on the development of information technology standards such as Ethernet and standards for images (JPEG standards) and streaming video (MPEG standards).

The proliferation of non-wired networks, such as radio, infrared, and powerline carrier, makes it easy to connect rogue devices to a home network. Therefore, the gateway might be designed to contain a registry of legitimate devices. The gateway would validate digital certificates presented by attached devices to determine if the device belongs on this network. A certificate is a digital message verifying that a device was provided by a known company and operates according to agreed rules.

Another responsibility of the gateway sentry is to validate the connection to an external server in order to ensure that the home device is connecting to the intended service provider. The gateway sentry would maintain a list of authorized servers providing application services for the devices and systems installed in the house. This would prevent malware implanted in a home device from sending consumer data to an unintended external server that might misuse this data or issue bogus control signals.

Additional gateway sentry features screen data traffic for compliance with policies that protect consumer privacy. Also, appliance control messages impacting safety might be screened and blocked by the same mechanism. For example, using a smartphone app when away from home to start a burner on a cook-top could be dangerous unless someone is at home to check that the appropriate pot with food is in place and nothing flammable is nearby.

Gateway Filtering for PII and Safety



Source: Dr. Kenneth Wacks

© Parks Associates

CS = Cybersecurity
LAN = Local Area Network
PII = Personally Identifiable Information
WAN = Wide Area Network

The elements in the gateway for protecting Personally Identifiable Information (PII) and safety include the PII & Safety Controller containing the rules about which data flows are allowed and which are blocked, and the PII & Safety Processor to enforce these rules by filtering the data to allow or block transmission.

Data Privacy

Product developers may offer features that depend on consumers providing personal data. Privacy policies for smart home manufacturers should list the data requested, the use of these data, with whom these data may be shared, how long these data will be retained, and how the data will be protected to minimize loss in a cyber breach.

Many service providers state their privacy policies, but offer no customer options other than to demand click-through approval for accessing any services. As cybersecurity tools evolve, customers may be offered multiple service-level options, each with a corresponding list of requested personal data. The gateway sentry could be programmed to pass only data corresponding to the agreed service level, while blocking other private data from transmission outside the house.

> Privacy is no longer an abstract concept but can be enabled with appropriate policies, technologies, and products.

We may be at a confluence of social, political, and technical events that make standards and technology specifications for privacy timely. Consumers are becoming increasingly aware that personal data can be misused.

- In May 2018, the European Union (EU) General Data Protection Regulation (GDPR) became law. It protects the personal data such as names, addresses, photos, and voice recordings of all EU residents regardless of where the data are processed. Explicit consent is required before processing personal data for one or more specific purposes.
- Currently, the only mandated privacy protection at the federal level in the United States applies to health data. Consumers want products with technology that can protect privacy. To guide consumers in making informed decisions involving privacy, manufacturers should address privacy issues. Otherwise, privacy will be legislated, as was recently done in the California Consumer Privacy Act of 2018. This law grants California residents the right to know what personal information a business is collecting and how it is being used, plus the right to opt out and have their information deleted.

It is now up to designers and manufacturers to incorporate privacy technology into products and for service providers to offer privacy choices with opt-in provisions. Privacy is built around policy issues described in the table below. As NIST explains, "… cybersecurity risk and privacy risk are related but distinct concepts. For cybersecurity, risk is about threats to devices or data. For privacy, risk is about problematic data actions—operations that process PII."[3]

Effective privacy policies must be executed in a cyber-secure environment including secure storage within each device. The first line of a cyber defense is within connected devices. However, some legacy devices may not be adequately protecting internal data. Maintaining customer data privacy requires cybersecurity tools appropriate for the capabilities of the connected devices. Building in privacy protection during product design is less costly for manufacturers than fixing problems later and compensating consumers for breaches.

Privacy Policy Issues

Privacy Topic	Customer Options
Data collected	What data are collected?
	When and how often are data collected?
	Can the customer update the data?
Services provided	What services will be delivered in exchange for providing these data?
	Are there options for reduced services requiring less personal data?
	Will these data be used for purposes other than providing specific services?
Data access and accuracy	Who has access to these data?
	How can the customer review the data for accuracy?
	How can the customer correct or revise the data?
	Will these data be transmitted or sold to third parties?
	Will these data be correlated with other databases for "data mining"?
	Will these data be aggregated? If so, will personal details be removed?
Data deletion	How long will collected data be retained?
	Will data be archived or erased after the retention date?
	When will backup files containing data after the retention date be purged?
	Will the customer be notified when the data and backup files have been erased?
Privacy policy changes	Is the consumer notified of any changes in the privacy policy?
	What options are available to the consumer if the privacy policy is changed?

Source: Dr. Kenneth Wacks

© Parks Associates

[3] Excerpted from NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, June 2019, p. 5

Security-by-design

Integrated home systems are assembled from carefully designed applications (such as entertainment, lighting, etc.) created by experts in each field. The equipment should be optimized for the application and should conform to interoperability standards to facilitate coordinated actions where appropriate among application controllers.

Manufacturers' decisions about the following critical issues affect cybersecurity:

Application organization and optimization

Which control functions, sensors, actuators, and user interfaces are needed?

Application interactions

Which parameters of an application are controllable and observable from other applications?

Data security

Where is data security needed?

What level of security is warranted based on the consequences of possible breaches?

Which security algorithms are appropriate?

Who are the trusted entities for administering security certificates and encryption keys?

Layers of control and security

What control and data are allowed to flow between consumers and service providers, between consumers and associates (colleagues, family, etc.), between consumers and the public, and between consumers and the government?

How should these messages be protected?

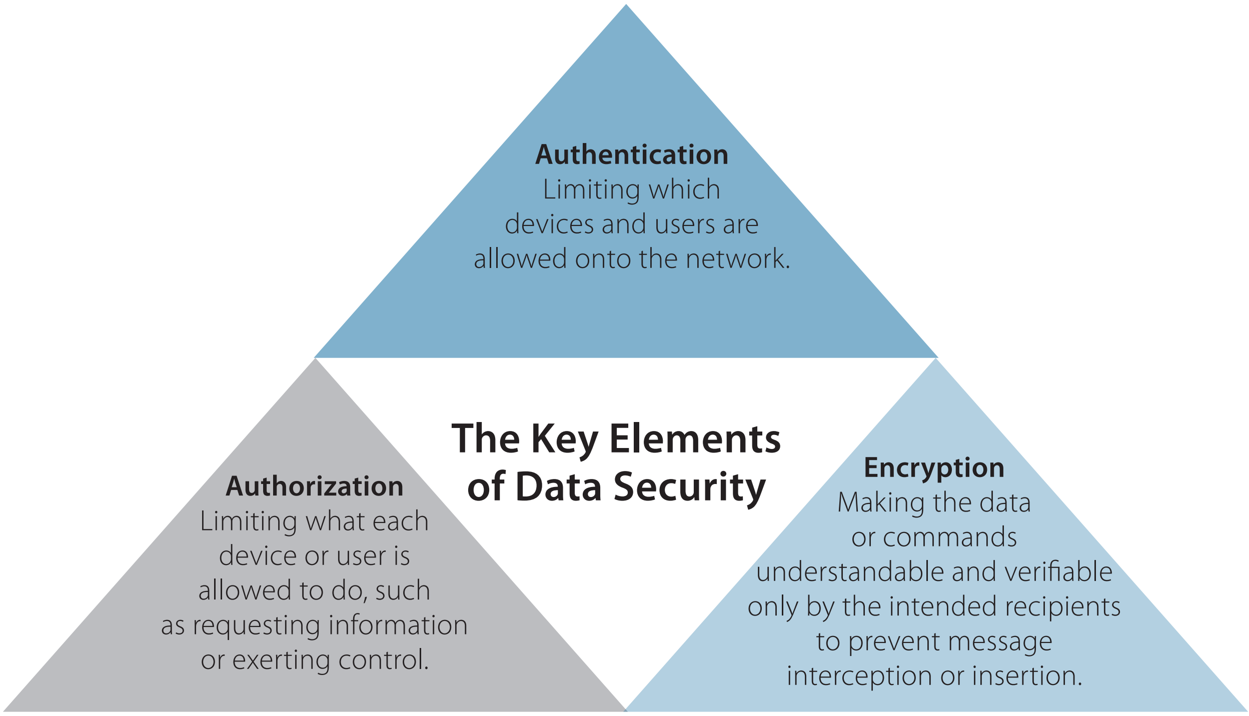
Consumer privacy

What consumer data can and should be kept private?

Whom might the consumer allow to view and change private data?

How are privacy violations detected and remedied?

Cybersecurity starts with an organized, structured, and disciplined system design. For effective cybersecurity, home system manufacturers should complement this organized system design with a security-by-design approach. Security-by-design involves engineering choices of integrated circuits, modules, software, data processing, and the interfaces to a communications network. Practical measures include closing unused data ports, implementing appropriate encryption techniques, and updating software for the operating system and applications. Updates are important because cybersecurity protections need to improve as the cost of penetration and time to penetrate decrease with technological advances.



The Key Elements of Data Security

Authentication
Limiting which devices and users are allowed onto the network.

Authorization
Limiting what each device or user is allowed to do, such as requesting information or exerting control.

Encryption
Making the data or commands understandable and verifiable only by the intended recipients to prevent message interception or insertion.

For proper network security, every participating device must be programmed with the correct security algorithm. Security depends on trusted entities (software and/or hardware from trusted suppliers) that are responsible for the following:

- **Authenticating** devices—often by using certificates
- **Authenticating** users—often with passwords; sometimes with physical tokens
- **Authorizing** actions—and limiting access to critical functions
- **Maintaining** secret codes for encryption—using complex alphanumeric keys

Effective security requires agreements not only on the algorithms but also on the interactions among the devices and the trusted entities.

A process for validating security programs and for vetting trusted entities is essential.

Effective cybersecurity requires that security-by-design be extended to real-time analysis of data flows and operating parameters to detect anomalies in data or sequences of operation. A comprehensive system should perform like a computer operating system running data validation algorithms, virus and malware checks, and maintaining an audit trail for forensic analysis of failures, whether caused by design bugs or deliberate attempts at penetration and data theft.

Parks Associates published a whitepaper *IoT Data: Securing the Connected Home* explaining some of the prominent practices for security-by-design such as specialized hardware to protect data. Hardware-based operating-system boot procedures limit the ability to hijack the operating system in the controller. Likewise, encryption, authentication, key management, and certificate management based in hardware improve execution speed and prevent malware from reprogramming a device to compromise operation and data transfers.

Engineering practices for security-by-design are well documented. NIST has published extensively on cybersecurity.[4]

[4] https://www.nist.gov/topics/cybersecurity

Cybersecurity Practices from Traditional to Leading Edge

1. Security through air gaps (no connections to the internet)

In this base-level design, data are not protected, but the operating environment inside the home is supposedly protected through isolation from the outside world. Staying off the internet sounds like a simple solution for cybersecurity, but it is becoming more difficult. Software and firmware-based devices occasionally need to be updated. Consumers might want to upgrade a product with new services. Even if the device is not connected for real-time modifications, the consumer might plug in a memory device (USB or flash memory) that could contain malware.

2. Security through obscurity

Many local networks for factories, buildings, and homes were based on proprietary designs and message sets Of course, a determined thief could reverse engineer such a system if the ultimate theft or remote access were worth the time and effort, but this was rare. Manufacturers are gradually switching to standardized networks to cut costs and to provide remote access for monitoring and controlling operations. They can buy infrastructure components from multiple vendors and integrate the management of device networks with information networks to consolidate training and equipment maintenance. The downside is the emergence of a larger community of experts who understand the network; a few miscreants might attempt to use this knowledge to penetrate the network.

3. Security through real-time vulnerability monitoring

More advanced cybersecurity is required as thieves adapt to new home technologies. An organization needs a dynamic process to identify and respond to new vulnerabilities and threats.

> "Organizations need to have 'situational awareness' over their information systems and to understand their security posture in a constantly evolving IT environment."—David Waltermire, a NIST computer scientist [5]

4. Security through data traffic monitoring and device operation monitoring

The proliferation of home products that communicate with external service providers elevates cybersecurity threats. The gateway sentry functions described above are intended to monitor data traffic.

5. Security through AI (artificial intelligence) to detect unusual patterns of operation

AI introduces sophisticated algorithms to detect anomalous behavior of device operations (e.g., types and frequency of inputs and outputs). Cybersecurity based on AI is not without risk since thieves might learn how to defeat the algorithm.

6. Security through honeypots

A honeypot is a deliberate weakness built into a system of networked computers and devices in order to attract hackers to attempt penetration. A clever honeypot will collect data about such a penetration that engineers can study to strengthen the cybersecurity defenses. Also, the hacker might be tracked and located.

> "A secure system relies on a variety of defense methods to guard your system. However, as goes for virtually any piece of technology, a honeypot is not foolproof. No defense mechanism is 100% reliable. But if used correctly and sparingly, honeypots can be the perfect strategy for protecting your system from hackers."
> —Caleb Townsend, *United States Cybersecurity Magazine* [6]

7. Defense-in-depth for Cybersecurity

Comprehensive cybersecurity monitoring requires advanced proactive real-time measures. In an ideal system employing security-by-design principles, these measures would be built into every device on the home network including the gateway. Furthermore, the telecommunications company, internet service provider (ISP), and application service provider would all comply with appropriate standards and practices for cybersecurity. In reality there is a cost to manufacturers, mistakes are made, and the latest technology is not employed.

8. Dynamic Cybersecurity Protection

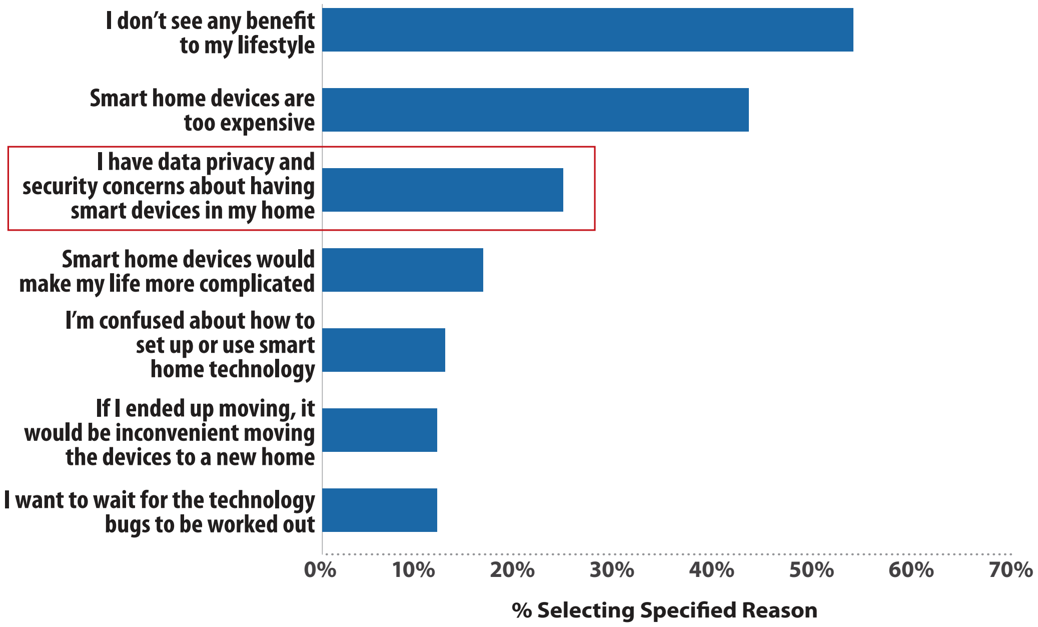
It is unrealistic to expect that every vendor in the smart-home value chain will apply necessary levels of cybersecurity. Vendors need protection from the risk of inadvertent design flaws in their products, as well as in other vendors' devices with which they share networks. A realistic remedy is to adopt a proactive security tool that can dynamically address all possible threats. For example, a real-time prevention, detection, and response platform could protect devices with a real-time, AI-driven response to both known and unknown (zero day) threats complemented by continuous support from a 24/7 security operations team.

[5] https://www.nist.gov/news-events/news/2012/01/nist-publishes-draft-implementation-guidance-continuously-monitoring

[6] https://www.uscybersecurity.net/honeypot

Smart Home Devices: Purchase Inhibitors

Among the 52% of US Broadband Households Not Owning and Not Intending to Buy Any Smart Home Device



© Parks Associates

The Cybersecurity Imperative

Consumers need products with technology that can protect security and privacy. There are emerging specifications for technologies that allow consumers and service providers to choose and enforce cybersecurity and privacy options. It is now up to designers and manufacturers to incorporate these technologies into products and for service providers to offer privacy choices with opt-in provisions.

Building in cybersecurity during product design and monitoring system operations for cybersecurity breaches are less costly for manufacturers than fixing problems later and compensating consumers for breaches. Cybersecurity and privacy are no longer abstract concepts but can be enabled with appropriate policies, technologies, and products.

Cybersecurity vulnerabilities influence purchase decisions. Manufacturers who embrace new and advanced cybersecurity measures will be differentiated from competitors and gain a key advantage in reaching out to consumers in this crowded market.

About Parks Associates

Founded in 1986, Parks Associates creates research capital for companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, workshops, executive conferences, and annual service subscriptions.

The company's expertise includes the Internet of Things (IoT), digital media and platforms, entertainment and gaming, home networks, Internet and television services, digital health, mobile applications and services, support services, consumer apps, advanced advertising, consumer electronics, energy management, and home control systems and security.

For more information, visit **parksassociates.com** or contact us at **972.490.1113** / **info@parksassociates.com**

About The Author

Kenneth Wacks, Ph.D., *Home, Building & Utility Systems (www.kenwacks.com); Contributing Analyst,* **Parks Associates**

Dr. Wacks has been a pioneer in establishing the home systems industry and a management advisor to more than 150 clients worldwide. His business spans IoT for home and building systems, energy management for smart grids, and digital media networks. He also provides due-diligence for investors and expert witness services for litigants including patent cases. Please visit **kenwacks.com** for information about his industry services, projects, and publications.

Dr. Wacks was appointed by the United States Department of Energy to serve four terms on the GridWise Architecture Council. He is a founding member of the Smart Grid Interoperability Panel, now part of the Smart Electric Power Alliance, where he chairs the Customer Grid Edge committee.

For seven terms, Dr. Wacks has chaired the ISO/IEC committee developing international home and building system standards, and in September 2018, Ken received the IEC 1906 Award. Ken has written American National Standards in home automation and networked appliances for the Consumer Technology Association, where he chairs the energy management standards committee. Dr. Wacks received his Ph.D. in electrical engineering from MIT as a Hertz Fellow and studied at the MIT Sloan School of Management.

ATTRIBUTION—**Authored by Dr. Kenneth Wacks.** Published by Parks Associates. © Parks Associates, Addison, Texas 75001. All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher. Printed in the United States of America.

DISCLAIMER—*Parks Associates has made every reasonable effort to ensure that all information in this report is correct. We assume no responsibility for any inadvertent errors.*