Brought to you by Informa Tech

OMDIA

Connected Devices: Not as secure as consumers think

Publication date:
February, 2023

Author:
Hollie Hennessy, Senior Analyst, Cybersecurity

Introduction

When it comes to the Internet of Things (IoT), consumer devices make up a significant part of the market, almost a third of the total installed base. Omdia expects there to be more than twenty billion consumer IoT devices installed across the globe by 2028. This includes devices used daily, such as smart thermostats, or smart speakers, and extends to devices such as smart plugs, smart lightbulbs, and even connected household appliances and kitchen equipment. With this rate of growth, the expanded device landscape is an ideal target for increasing cyberattacks. Unfortunately, there are many gaps in device security, including a lack of consistent standards.

Currently, there is no consistent labeling or reference for device manufacturers to demonstrate that their devices meet objective security requirements. Despite this, in a survey of four hundred consumers Omdia found a consistent perception on the part of respondents that their devices are secure. Sixty-seven percent said they believe they know how secure their devices are. Only 22% said they were not sure. Most consumers cited the manufacturer as the source of this belief, as well as social media and friends and family, highlighting a lack of independent validation of security best practices and information about it.

Standards groups to the rescue

The reality is that these devices are not always as secure as consumers think. Connected home products are often relatively cheap and have quick production lifecycles. This means security and privacy principles may be ignored or not appropriately prioritized in the development of these devices. As an example, this could be in order to keep costs down and to emphasize ease of use. However, there are a range of issues that can make them insecure. ETSI, the European Telecommunications Standards

Institute, one of many global organizations looking at this problem has developed a globally applicable standard for securing these devices, which looks to protect against common areas of vulnerability. The standard (EN 303 645) highlights the following thirteen elements that may help to reduce vulnerabilities:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

Ultimately, the responsibility to secure devices should not lie with consumers, just as it is not the consumer's responsibility to ensure product safety in devices such as cars or kitchen appliances. Consumers should be able to purchase connected devices and expect them to have adequate cybersecurity and privacy protection. In fact, consumers also are beginning to expect this protection. A large majority (83%) of survey respondents rate device security as important or very important with the remainder listing it as somewhat important.

In order to protect consumers from harm arising from insecure devices, country regulators and government bodies are taking up the responsibility to specify security requirements on consumers' behalf. Below are some examples of countries where work has been done to progress and develop legislation, certification, or labeling in the area of consumer IoT security.

Table 1: Summary of IoT device security specifications by geographic region

Region	IoT device security specification	Mandatory/ voluntary	Certification	Labeling	Key standard referenced
Asia					
Australia	Under development	Voluntary	Yes	Yes	ETSI EN 303 645
China	Yes	Mandatory	No	No	None
India	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Japan	Yes	Voluntary	No	No	NIST, ETSI EN 303 645
Singapore	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
South Korea	Yes	Voluntary	Yes	Yes	ITU X.1352
Thailand	Under development	Voluntary	No	No	None
Vietnam	Yes	Voluntary	No	No	ETSI EN 303 645
Europe					
France	Yes	Voluntary	No	No	ETSI EN 303 645
Germany	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Spain	No	Voluntary	No	No	None
UK	Yes	Mandatory	Yes	Yes	ETSI EN 303 645
Americas					
Brazil	Yes	Mandatory	Yes	Yes	ETSI EN 303 645, ISO/IEC 27402
US	Yes	Voluntary	Yes	Yes	NIST

Source: Omdia

Call to action

At present though, this is all relatively new. The ETSI standard mentioned above was only published in 2020. The PSTI Act in the UK only received royal assent at the end of last year, in December 2022, and much consumer IoT-specific legislation is yet to be finalized or made mandatory. So the question is: What do we do in the meantime?

Regulation is coming, that is clear; cybersecurity requirements will be mandated, and devices will hopefully become more secure. This gives industry players a significant opportunity. Getting ahead of regulation and legislation, those in the IoT industry can work together to create products in line with security best practices and begin to make it clear to consumers.

Three of the main standard bodies relevant to IoT cybersecurity include ETSI, NIST (the National Institute of Standards and Technology, part of the US government) and ISO (the International Organization for Standardization), with varying levels of commonality. Despite regulatory and governmental efforts, the overall picture is still highly fragmented. There's little harmonization and a clear need for a global approach in order to guide manufacturers with as little confusion as possible.

When regulation is in place and enforced, the difference in global standards and the sheer number of them make it overly burdensome for manufacturers to meet the requirements and gain certification. The Connectivity Standards Alliance (Alliance) is leading a campaign to create a harmonized standard, building on those that are already most widely adopted, and a certification model in order to help solve the issue. Collaborating with companies, governments, and consumer advocates, the Alliance has created a Product Security Working Group and, more recently, a Data Privacy Working Group with the goal of tackling disconnects in consumer IoT security and privacy.

Overall, there have been a lot of developments in IoT cybersecurity, but there is more work to be done, whether that's further harmonization of standards as discussed above or tackling the issue of security and privacy labeling. Governments and standards bodies globally have begun to work on labeling schemes, but it remains something to be widely adopted and needs careful consideration. Labels need to be accurate but simple enough for consumers to understand. Omdia has recently developed a research report, *Consumer IoT Devices Cybersecurity Standards, Policies, and Certification Schemes*, looking at the global landscape, commonality, and full results of our consumer survey with labeling recommendations.

Author

Hollie Hennessy, Senior Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy: Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

About Connectivity Standards Alliance

To become a member of the Connectivity Standards Alliance and get involved with all our initiatives, including product security and privacy visit: www.csa-iot.org

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

customersuccess@omdia.com