

Industry, hackers, and consumers for a global baseline for consumer IoT security

Network-connected devices have become a dominant trend in the evolution of consumer products. Today, everything from TV's, to watches, to refrigerators are increasingly part of the internet of things (IoT). While these "smart" devices offer myriad benefits to consumers, they also expose individuals and organizations to added cyber risk when they are not developed and maintained with security in mind and often lack the security capabilities of traditional computer products. With billions of connected consumer devices now on the market, and billions more soon to follow, there is need for a strong global baseline for IoT security in the next generation of consumer products.

A multistakeholder consensus

Gathered together initially through the World Economic Forum's platform for multistakeholder cooperation, we are a community reflecting the interests of security researchers, technology providers, and consumers, alarmed by rising threats stemming from insecure consumer IoT devices. Building the next generation of connected consumer products to be more secure will require a cohesive, multistakeholder approach to security.

While all stakeholders – manufacturers, distributors, vendors, regulators, even consumers themselves – have respective roles to play in the safe development, deployment and use of IoT products, device security requires manufacturers and vendors who place devices on the market to adhere to best practices to ensure products are designed with security in mind. With connected devices today having supply chains that reach around the world, establishing a recognized global baseline for consumer IoT security is a critical step toward a more resilient and trusted digital future.

A global consensus for consumer IoT security

We welcome the global consensus forming around three key capabilities that can begin setting a clear baseline for consumer IoT security – (1) *No universal default passwords*; (2) *Implement a vulnerability disclosure policy*; and (3) *Keep software updated*– and support these as an immediate priority for respective manufacturers and vendors to implement in order to improve consumer IoT device security. In addition, our community recognizes the importance of two other capabilities related to securing data – (4) *Secure communications*; and (5) *Ensuring that personal data is secure*. Taken together, these five device capabilities are [found in over 100 standards, specifications and guidelines across the world](#) and establish a minimum level of security which should form the basis of all consumer IoT cyber security standards, specifications and guidelines.

One standard that champions these capabilities is [EN 303 645](#), developed by the European Telecommunications Standards Institute (ETSI) as the first globally applicable industry specification that establishes a baseline for consumer IoT security. We support the collaborative and rigorous multistakeholder process that went into the creation of this standard, which was first developed by ETSI in 2019, before being published in its current form in 2020. Since then, increasing numbers of governments have been developing guidance, regulations, and labelling schemes that reflect the 13 provisions in this standard, showing an important consensus emerging.

Widespread development and implementation of baseline IoT security standards will enable a future where every consumer can expect basic security features in every connected IoT device. This is a key step in advancing IoT security generally, which also must focus on security at the network level. **As a global community representing a diversity of interests and expertise, we collectively endorse these five capabilities in particular – (1) *No universal default passwords*; (2) *Implementing a vulnerability disclosure policy*; (3) *Keeping software updated*; (4) *Securely communicating*; and (5) *Ensuring that personal data is secure* – as a global baseline**

for consumer IoT device security. We encourage governments to promote these capabilities in particular to further harmonize standards around the needs of consumers, and call on IoT device manufacturers and vendors to:

- 1) Take immediate action to ensure the implementation of these five baseline capabilities and develop a comprehensive plan to adopt the mandatory elements of all 13 ETSI EN 303 645 provisions or equivalent IoT baseline standards, guidelines, or best practices.
- 2) Take steps to ensure consumers are aware of security information, either through product labelling or other forms of communications and/or documentation.

This document is intended to serve as a jumping off point to continue building consensus and promoting robust device security. Those of us endorsing this statement come from across stakeholder groups, including members of industry at various stages of adopting these best practices. We recognize that implementing these capabilities poses different challenges to manufacturers and vendors around the world. We also recognize the broad range of stakeholder activity relevant to this work. Therefore, we plan to continue working together through the World Economic Forum's [Council on the Connected World](#) and [Centre for Cybersecurity](#) on technology governance and other spaces to share resources and provide guidance for doing so. This includes working to track and highlight which businesses are implementing these provisions, to show progress and showcase different practices and approaches for the benefit of others.

To have your organization endorse this statement or for more information on how to get involved, please contact: info@cybertechaccord.org

Endorsers (alphabetical):

- 1) ABINC - Associação Brasileira de Internet das Coisas
- 2) ABO2O - Associação Brasileira Online to Offline
- 3) Accenture
- 4) AIMS360
- 5) AIQuatro
- 6) Arcelik
- 7) Archive360
- 8) Arm
- 9) AstraZeneca Brazil
- 10) Australian Communications Consumer Action Network
- 11) BigCloud Consultants
- 12) Binare.io
- 13) BlocPower
- 14) BrainBox AI Inc
- 15) Bsquare Corporation
- 16) BugCrowd
- 17) C4IR Brazil
- 18) C4IR Turkey
- 19) Carnegie Mellon University
- 20) Census Labs

- 21) Center for Internet Security
- 22) Check Point Software Technologies
- 23) Confederation For Consumer Organisations (TÖK)
- 24) Consumer Reports
- 25) Copper Horse Ltd
- 26) CUTS International
- 27) Cyber Threat Alliance
- 28) Cyber Threat Intelligence League
- 29) Cybereason
- 30) CyberPeace Institute
- 31) Cybersecurity Coalition
- 32) Cybersecurity Policy Working Group
- 33) Deloitte
- 34) Device Authority
- 35) Disclose.io
- 36) Euroconsumers
- 37) Ezrest e BiomarkerAi
- 38) Fluxus
- 39) Foundation for Consumer Rights (FUNDECOM)
- 40) F-Secure
- 41) Global Cyber Alliance
- 42) Google
- 43) Graymatics
- 44) Greenlight Information Services
- 45) GRIMM
- 46) HackerOne
- 47) HCL Technologies
- 48) Helpful Places, Inc
- 49) Hong Kong Consumer Council
- 50) Horizon Next Technology Co. Ltd.
- 51) HumanFirst
- 52) IAR Systems
- 53) iconectiv
- 54) ICS Village
- 55) Immersive Labs
- 56) Independent Security Evaluators
- 57) InfoCons Association
- 58) Institute for Security and Technology
- 59) IoT Security Foundation
- 60) IoT Security Trust Mark
- 61) IoT Village
- 62) Karsu
- 63) Kigen
- 64) Kudelski Group
- 65) LastWall
- 66) LEEDARSON IoT
- 67) Lexi Inc.

- 68) Libelium
- 69) Loudmouth Security
- 70) Luta Security
- 71) Madison Computer Works
- 72) Meddriven
- 73) MEXT Technology Center
- 74) Microsoft
- 75) Myanmar Consumers Union
- 76) NEC
- 77) Northwave
- 78) NTT
- 79) Pax8
- 80) Pentest Partners
- 81) Qualcomm Technologies, Inc.
- 82) Quantela
- 83) Queue Associates
- 84) QuintessenceLabs
- 85) Rapid7
- 86) Research Institute for Sociotechnical Cyber Security
- 87) Resecurity
- 88) SCYTHE
- 89) Secure Thingz
- 90) Sensoro
- 91) Signify
- 92) Silent Breach
- 93) Stratigos Security
- 94) Supply Chain Sandbox
- 95) Talion
- 96) The @ Company
- 97) The Cyber Security Agency of Singapore
- 98) The Department for Digital, Culture, Media and Sport (DCMS), UK Government
- 99) The PETRAS National Centre of Excellence for IoT Systems Cybersecurity
- 100) The Scientific and Technological Research Council of Turkey (TÜBİTAK) Informatics and Information Security Research Center (BİLGEM)
- 101) The Victor Pineda Foundation / World Enabled
- 102) Thirdwayv
- 103) Transatel
- 104) Trinity Mobility Private Limited
- 105) TRTEST Test and Evaluation Inc.
- 106) Unitel S.A.
- 107) US Licensing Group
- 108) Validy Net
- 109) VDI - Associação de Engenheiros Brasil – Alemanha
- 110) Weevil Netherlands/Weevil Sverige
- 111) Which?
- 112) WISeKey
- 113) ZARIOT