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) AIMS360
4) AIQuatro
5) Arcelik
6) Archive360
7) Arm
8) AstraZeneca Brazil
9) Australian Communications Consumer Action Network
10) BigCloud Consultants
11) Binare.io
12) BlocPower
13) BrainBox AI Inc
14) Bsquare Corporation
15) BugCrowd
16) C4IR Brazil
17) C4IR Turkey
18) Carnegie Mellon University
19) Center for Internet Security

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

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