RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: AST3-W02

THE PROMISE OF IOT BEST PRACTICES, TESTING & THE HAZARDS OF INACTION

MODERATOR: **Craig Spiezle**
Managing Director, Agelight Risk Advisory Group
Founder & Chairman, Online Trust Alliance
@craigspi

PANELISTS: **Patricia Adair**
Director of Risk Management Group
Consumer Product Safety Commission
@USCPSC

Justin Brookman
Director, Privacy & Technology Policy
Consumers Union
@JustinBrookman

Terrell McSweeny
Commissioner
Federal Trade Commission
@TMcSweenyFTC

Danger Will Robinson IoT Devices Ahead!

Challenge of The IoT Ecosystem

Devices

Cloud

Apps

Shift from Online to Risks to Hazardization

- Amplified Impact to Critical Infrastructure & Communities

IoT Incident of the Week

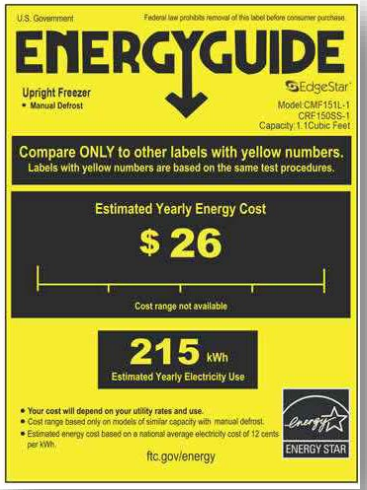
Hackers exploit casino's smart thermometer to steal database info

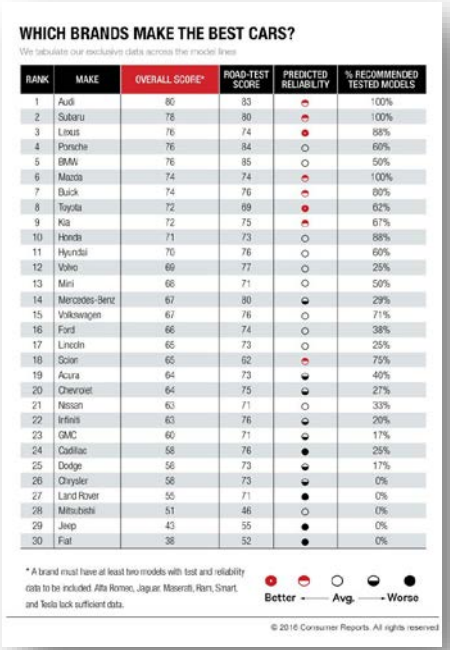
Share on Facebook | Share on Twitter | +

WHAT'S THIS?

A casino in Las Vegas.

Testing Models – Can They Apply To IoT?





WHICH BRANDS MAKE THE BEST CARS?

We tabulate our exclusive data across the model lines

RANK	MAKE	OVERALL SCORE*	ROAD-TEST SCORE	PREDICTED RELIABILITY	% RECOMMENDED TESTED MODELS
1	Audi	80	83	◓	100%
2	Subaru	78	80	◓	100%
3	Lexus	76	74	●	88%
4	Porsche	76	84	○	60%
5	BMW	76	85	○	50%
6	Mazda	74	74	◓	100%
7	Buick	74	76	◓	80%
8	Toyota	72	69	●	62%
9	Kia	72	75	◓	67%
10	Honda	71	73	○	88%
11	Hyundai	70	76	○	60%
12	Volvo	69	77	○	25%
13	Mini	68	71	○	50%
14	Mercedes-Benz	67	80	◒	29%
15	Volkswagen	67	76	○	71%
16	Ford	66	74	○	38%
17	Lincoln	65	73	○	25%
18	Scion	65	62	◓	75%
19	Acura	64	73	◒	40%
20	Chevrolet	64	75	◒	27%
21	Nissan	63	71	○	33%
22	Infiniti	63	76	◒	20%
23	GMC	60	71	◒	17%
24	Cadillac	58	76	●	25%
25	Dodge	56	73	◒	17%
26	Chrysler	56	73	◒	0%
27	Land Rover	55	71	●	0%
28	Mitsubishi	51	46	○	0%
29	Jeep	43	55	●	0%
30	Fiat	38	52	●	0%

* A brand must have at least two models with test and reliability data to be included. Alfa Romeo, Jaguar, Maserati, Ram, Smart, and Tesla lack sufficient data.

Better ◓ ○ ◒ ● Worse

How Do We Protect Consumers?

Kidde Recalls Dual Sensor Smoke Alarms Due to Risk of Failure to Alert Consumers to a Fire

A yellow cap left on during the manufacturing process can cover one of the two smoke sensors and compromise the smoke alarm's ability to detect smoke.

Fitbit Recalls Force Activity-Tracking Wristband Due to Risk of Skin Irritation

En Español

Note: On February 20, 2014, Fitbit Inc. announced a refund program for the Fitbit Force. This news release serves as the official recall announcement. C
effective 1/11/16.

Name of product:
Wireless activity-tracking wristband

Hazard:
Users can develop allergic reactions to the stainless
strap, or adhesives used to assemble the product, r
where the skin has been in contact with the tracker.

Remedy:
Refund

Recall date:
March 12, 2014

Units:
About 1,000,000 in the U.S. and about 28,000 in Ca

CONSUMER PRODUCT SAFETY COMMISSION
UNITED STATES

Security & Privacy Concerns

Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds

Security and privacy testing of several brands also reveals broad-based data collection. How to limit your exposure.

Harmonizing Risk Assessment Models

Guiding Directives

- Address the root causes of risks at-scale
- Promote security and privacy practices which are feasible to adopt
- Reduce consumer risk & support burdens
- Drive supply chain continuous improvement
- Incentivize adoption & differentiation
- Ability to evaluate & select secure products
- Be applicable globally

Scoring Criteria

- User benefit & completion
- Impact to ecosystem (internal and externally)
- Financial and performance impact
- Physical safety risks if not addressed
- Effort to support over a product's life
- Regulatory and product liability risks

IoT Safety & Trust Design Architecture & Risk Guide

	GDPR / Article 29 WG	U.S. FTC	NIST Framework	ENISA	UK Secure by Design
	Referenced or Required				
	✓ Yes				
Disclose if device security updates and patches are provided and the duration of support Notes – All devices should receive security updates and patches throughout their expected life. In some cases companies may offer extended support for a fee as a managed service. In addition existing protocols and standards may have to be updated due to newly discovered vulnerabilities such as KRACK compromising devices which support WPA2. See #22 for related requirements and context.		✓		✓	✓
Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where an update must overwrite device settings, the user must be prompted to review and select settings prior to install. Notes – User device configurations ranging from security, privacy to battery power settings have been inadvertently "written over" from updates which have placed devices back to their default or "factory shipped" status. If overwriting preferences and settings cannot be prevented, prior to updates being installed users should be prompted to review and record their settings to facilitate the ability to reset them. On "first use" the user should be prompted and walked through re-setting such settings.	✓	✓			

IoT Safety & Trust Design Architecture & Risk Guide

	GDPR / Article 29 WG	U.S. FTC	NIST Framework	ENISA	UK Secure by Design	User Benefit	Ecosystem Impact	Financial	Hazardization	Dev & Time to Market	Reg. or Legal Risk	Total
	Referenced or Required					Company Risk - A total 50 points						
	✓ Yes					8.3	8.3	8.3	8.3	8.3	8.3	50
						Principle Scoring Up to 10 points @						
Disclose if device security updates and patches are provided and the duration of support Notes – All devices should receive security updates and patches throughout their expected life. In some cases companies may offer extended support for a fee as a managed service. In addition existing protocols and standards may have to be updated due to newly discovered vulnerabilities such as KRACK compromising devices which support WPA2. See #22 for related requirements and context.		✓		✓	✓	10	5	9	10	10	10	**450**
Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where an update must overwrite device settings, the user must be prompted to review and select settings prior to install. Notes – User device configurations ranging from security, privacy to battery power settings have been inadvertently "written over" from updates which have placed devices back to their default or "factory shipped" status. If overwriting preferences and settings cannot be prevented, prior to updates being installed users should be prompted to review and record their settings to facilitate the ability to reset them. On "first use" the user should be prompted and walked through re-setting such settings.	✓	✓				10	2	10	2	10	10	**367**

Optional ← Organization's "Risk-Appetite" → Must-implement

Apply What You Have Learned Today

Within 30 days:

- Organizations / Users
  - Inventory devices and review privacy and security settings
  - Be thoughtful of the benefits / risks before you buy
- Device Vendors
  - Embrace established IoT trust principles and standards
  - Review FTC guidance and EU General Data Protection Regulations (GDPR)
  - Review your marketing claims and privacy policies

Within 180 days

- Organizations / Users
  - Establish and implement device configurations based on your “risk appetite”
  - Move all devices to an isolated network / Disable insecure products/functions
- Device Vendors
  - Develop a life-cycle / sustainability support plan
  - Tune your practices and policies - Shift from compliance to stewardship

Looking Ahead- Q & A

Resources https://agelight.com/IoTResources.html

- Consumer Products Safety Commission https://www.cpsc.gov/
- European Union Agency for Network & Information Security (ENISA) https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/
- Internet Society https://internetsociety.org/IoT
- UK Government Secure by Design https://www.gov.uk/government/publications/secure-by-design
- Department of Commerce, NTIA – IoT Upgradability & Patching Initiative https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security
- Department of Commerce, NTIA – Coordinated Vulnerability Disclosures https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
- FTC & The NIST Cybersecurity Framework https://go.usa.gov/xQqgA
- FTC Building Security into IoT https://ftc.gov/carefulconnections
- AgeLight https://agelight.com/iot.html
- Consumer Reports / Digital Standard https://www.thedigitalstandard.org/
- Underwriters Laboratory (UL) https://ul.com/consumer-technology/en/industries/internet-of-things