May 2018

Trust by Design: The Internet of Things

Security and privacy of smart-home devices and services

Internet Society

Sebastian Bellagamba - LAC Regional Director

bellagamba@isoc.org

The number of IoT devices and systems connected to the Internet will be more than

2.5x the global population

by 2020 (Gartner).

As more and more devices are connected, privacy and security risks increase.

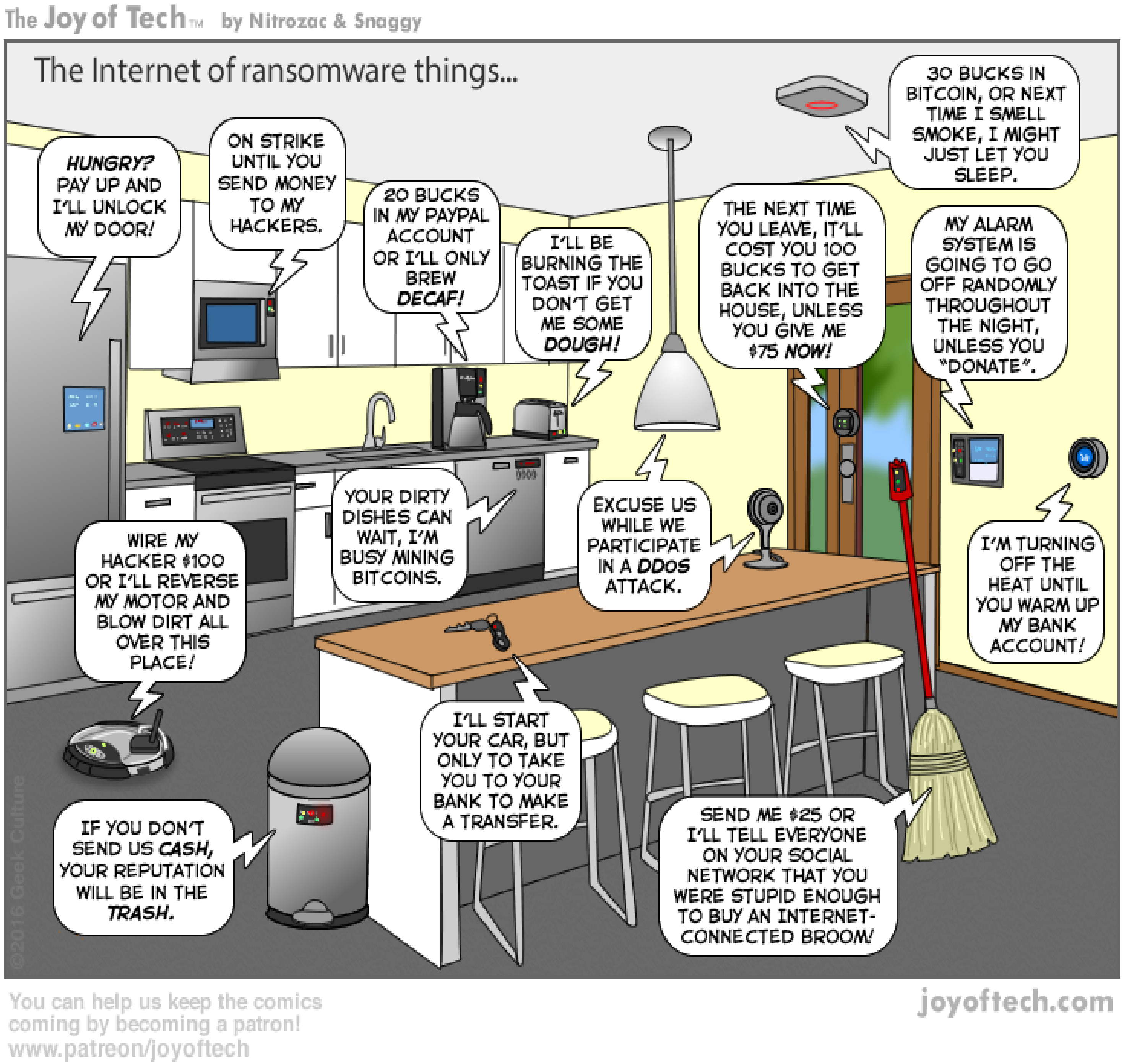
And most consumers don’t even know it.

What type of risks?

Unlocking doors, turning on cameras, shutting down critical systems and theft of personal property.

People’s safety or the safety of their family might even be at risk.

Large IoT-based attacks, such as the Mirai botnet in 2016, have crippled global access to high-profile Internet services for several hours.


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I’LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I’LL ONLY BREW DECAF!
I’LL BE BURNING THE TOAST IF YOU DON’T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT’LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU “DONATE”.
WIRE MY HACKER $100 OR I’LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I’M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I’M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I’LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON’T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I’LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

The challenges we face

A connected world offers the promise of convenience, efficiency and insight, but creates a platform for shared risk.

Many of today’s IoT devices are rushed to market with little consideration for basic security and privacy protections.

New devices, new vulnerabilities

The attributes of many IoT devices present new and unique security challenges compared to traditional computing systems.

- Device Cost/Size/Functionality
- Volume of identical devices (homogeneity)
- Long service life (often extending far beyond supported lifetime)
- No or limited upgradability or patching
- Physical security vulnerabilities
- Access
- Limited user interfaces (UI)
- Limited visibility into, or control over, internal workings
- Embedded devices
- Unintended uses
- BYOIoT

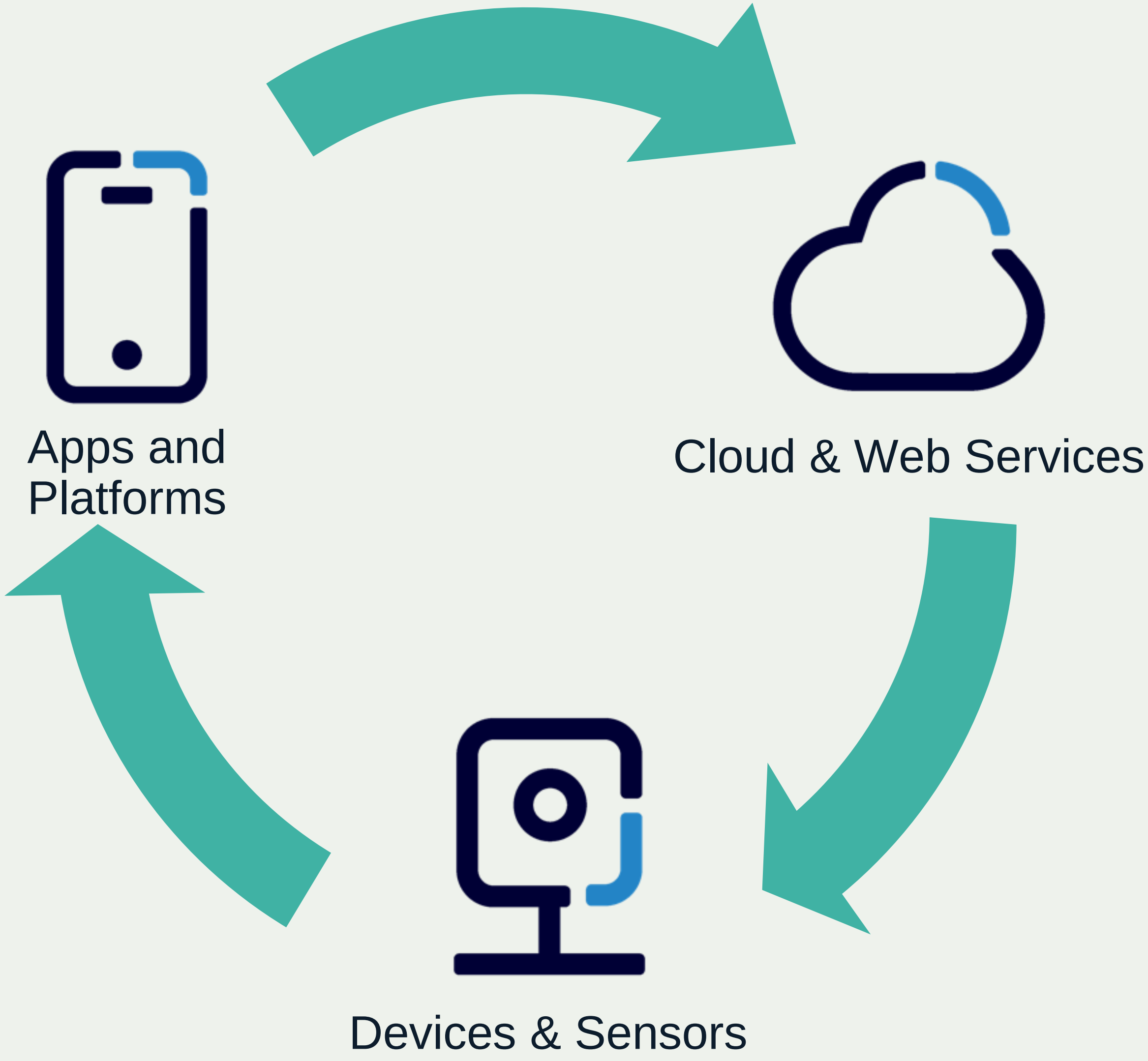
Key Challenge: IoT Ecosystem

Three Dimensions:

- Combination of devices, apps, platforms & services
- Data flows, touch points & disclosures
- Lack of defined standards

Impacts on Sustainability Issues:

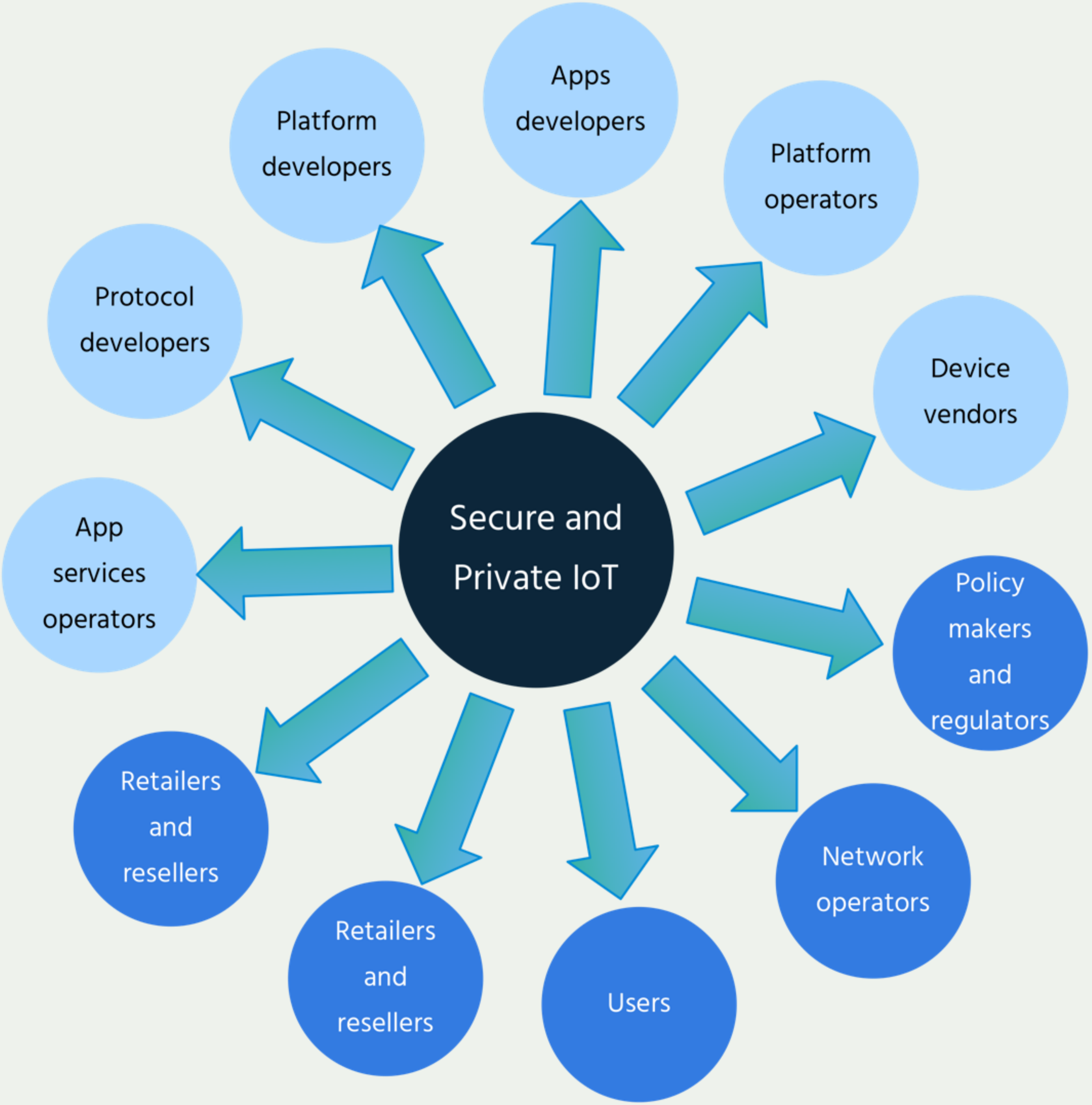
- Lifecycle supportability
- Data retention / ownership



Who is responsible?

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm.

We need a collective approach, addressing security challenges on all fronts.



Two views of IoT Security

Inward Security

Focus on potential harms to the health, safety, and privacy of device users and their property stemming from compromised IoT devices and systems.

Outward Security

Focus on potential harms that compromised devices and systems can inflict on the Internet and other users.

What we’re doing about it

The Internet Society is working for a better Internet.

We care about protecting people’s online privacy and security.

We want manufacturers and suppliers of consumer IoT devices and services to adopt security and privacy guidelines to protect the Internet and consumers from cyber threats.

IoT Trust by Design

1

Work with manufacturers and suppliers to adopt and implement the OTA IoT Trust Framework

2

Mobilize consumers to drive demand for security and privacy capabilities as a market differentiator

3

Encourage policy and regulations to push for better security and privacy features in IoT

Online Trust Alliance (OTA) IoT Trust Framework

- Provides a set of actions to raise the level of security for IoT devices and related services to protect consumers and the privacy of their data

- More than 100+ stakeholders from industry, government and consumer advocates contributed to the Framework

- Stands apart from other IoT-related Frameworks with its comprehensive focus on security, privacy and lifecycle issues, as well as a holistic view of the entire system

https://otalliance.org/iot/

Actionable principles in eight categories for manufacturers, developers and service providers

Authentication	Encryption	Security	Updates
Privacy	Disclosures	Control	Communications

A collective responsibility

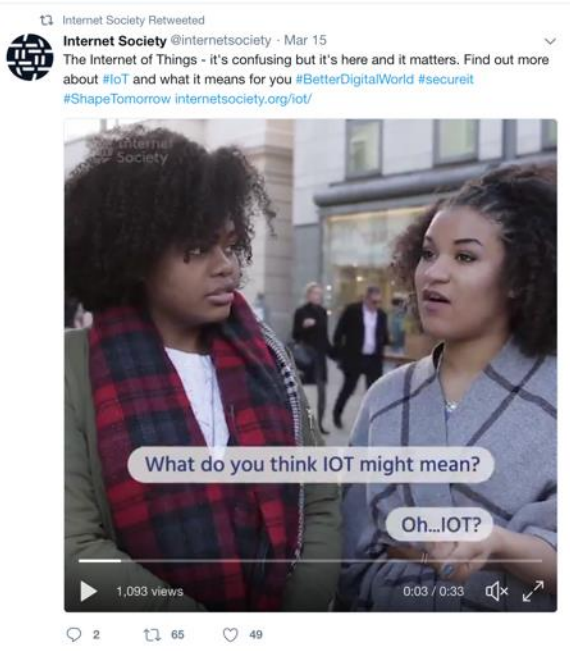
- IoT vendors and their supply chain
- Distribution channels
- Policymakers and governments
- Consumer testing and product review organizations
- Consumers and enterprises

Build consumer awareness and influence

We want consumers to know about the personal safety risks of IoT products and services.

We will provide opportunities for consumers to voice their concerns and drive demand for IoT offerings with security and privacy capabilities.

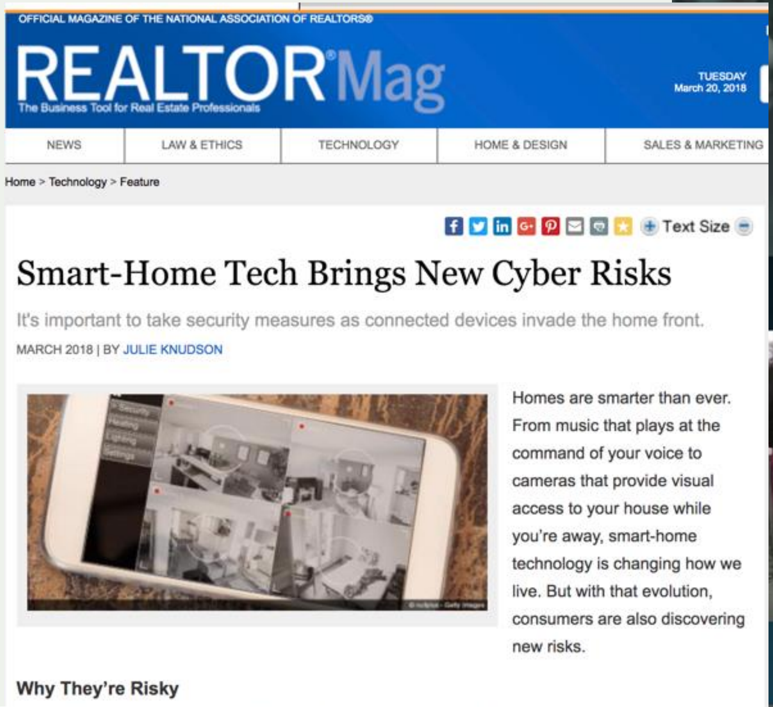
Igniting consumer interest



Internet Society Retweeted

Internet Society @internetsociety · Mar 15

The Internet of Things - it's confusing but it's here and it matters. Find out more about #IoT and what it means for you #BetterDigitalWorld #secureit #ShapeTomorrow internetsociety.org/iot/



OFFICIAL MAGAZINE OF THE NATIONAL ASSOCIATION OF REALTORS®

REALTOR® Mag

The Business Tool for Real Estate Professionals

TUESDAY
March 20, 2018

NEWS | LAW & ETHICS | TECHNOLOGY | HOME & DESIGN | SALES & MARKETING

Home > Technology > Feature

Text Size

Smart-Home Tech Brings New Cyber Risks

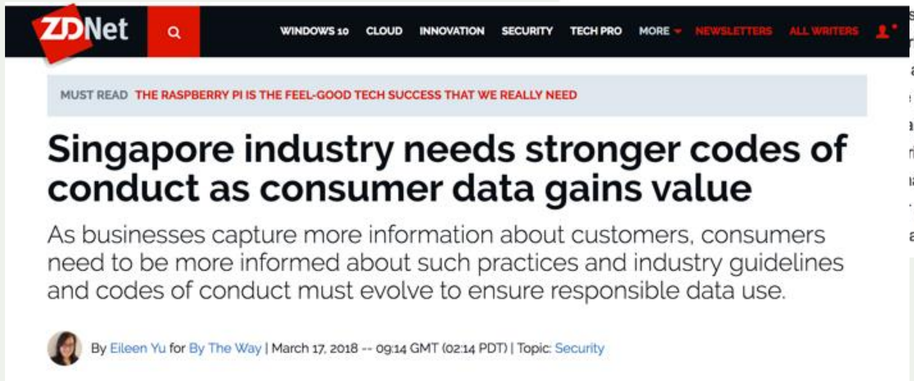
It's important to take security measures as connected devices invade the home front.

MARCH 2018 | BY JULIE KNUDSON

Homes are smarter than ever. From music that plays at the command of your voice to cameras that provide visual access to your house while you're away, smart-home technology is changing how we live. But with that evolution, consumers are also discovering new risks.

Why They're Risky

s internet of things technology—connect to the rk. Whether consumers add technology to their a home's sale, the vulnerability of this network is one essentially giving that device full access to your ains Patrick Tiquet, director of security and rity. While a smart fridge is probably not interested in at deep level of access still presents potential privacy world only block inbound traffic, any IoT device that ation out of your network."



ZDNet

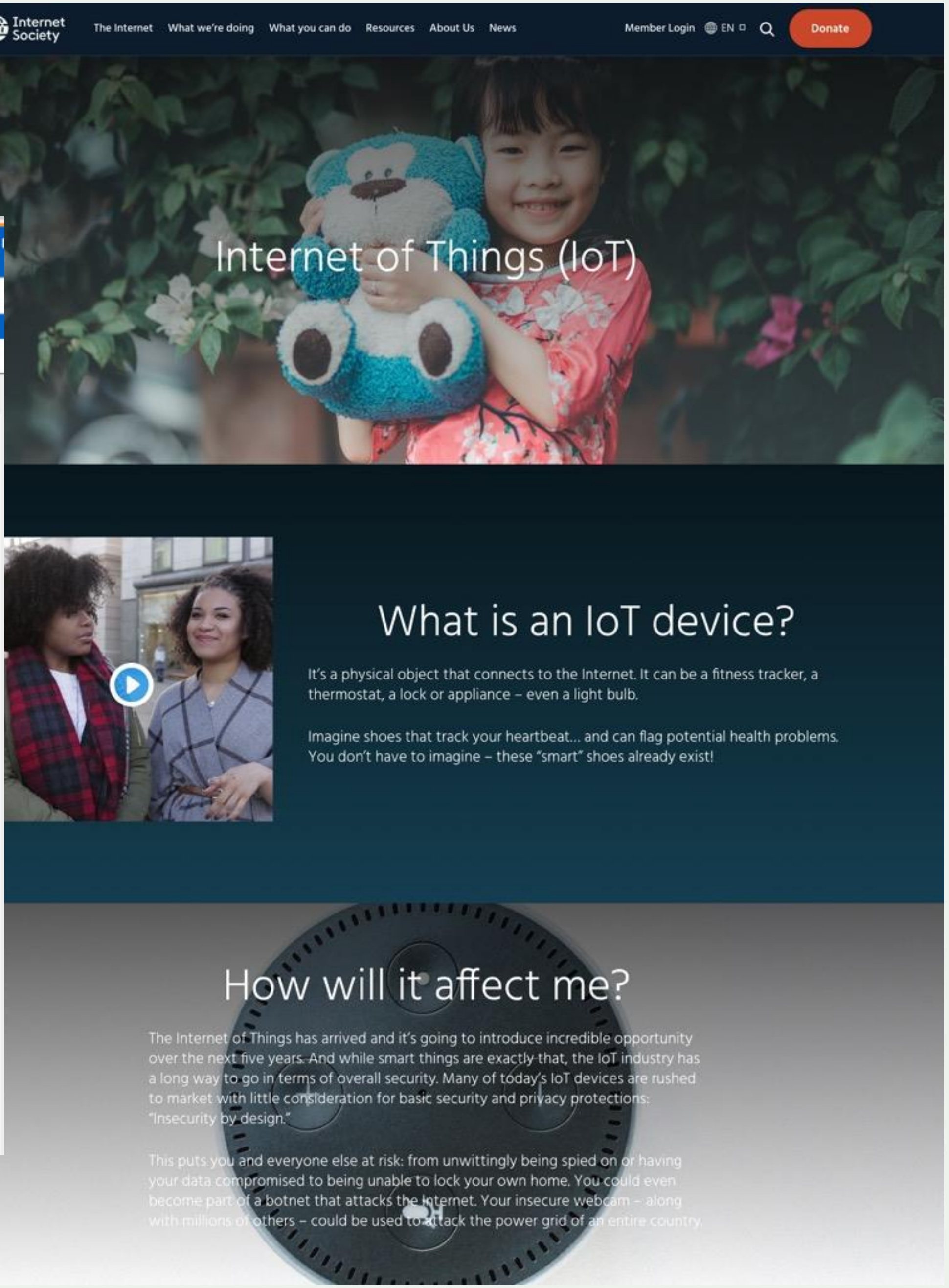
WINDOWS 10 | CLOUD | INNOVATION | SECURITY | TECH PRO | MORE | NEWSLETTERS | ALL WRITERS

MUST READ THE RASPBERRY PI IS THE FEEL-GOOD TECH SUCCESS THAT WE REALLY NEED

Singapore industry needs stronger codes of conduct as consumer data gains value

As businesses capture more information about customers, consumers need to be more informed about such practices and industry guidelines and codes of conduct must evolve to ensure responsible data use.

By Eileen Yu for By The Way | March 17, 2018 -- 09:14 GMT (02:14 PDT) | Topic: Security



Internet Society

The Internet | What we're doing | What you can do | Resources | About Us | News | Member Login | EN | Donate

Internet of Things (IoT)

What is an IoT device?

It's a physical object that connects to the Internet. It can be a fitness tracker, a thermostat, a lock or appliance – even a light bulb.

Imagine shoes that track your heartbeat... and can flag potential health problems. You don't have to imagine – these "smart" shoes already exist!

How will it affect me?

The Internet of Things has arrived and it's going to introduce incredible opportunity over the next five years. And while smart things are exactly that, the IoT industry has a long way to go in terms of overall security. Many of today's IoT devices are rushed to market with little consideration for basic security and privacy protections: "Insecurity by design."

This puts you and everyone else at risk: from unwittingly being spied on or having your data compromised to being unable to lock your own home. You could even become part of a botnet that attacks the Internet. Your insecure webcam – along with millions of others – could be used to attack the power grid of an entire country.

Work with Policymakers

We want policymakers to create a policy environment that favors strong security and privacy features in IoT products and services.

We need smart regulation that strengthens trust and enables innovation.

Actions for Policymakers

Governments have the opportunity to guide the IoT marketplace:

- Stimulate security and privacy best practice adoption
- Strengthen accountability through well-defined responsibilities and clear consequences
- Support industry adoption of the best practice principles from the IoT Trust framework

Activity highlights

OTA IoT Trust Framework implementation

- Best practices and toolkits
- Implementation guide
- Training for ISOC and community

Research

- Paper on IoT Security for Policymakers
- Policy research: mapping the IoT policy/regulatory landscape
- Economic study on IoT security externalities
- Study on “consumer grade” IoT markets, to better understand manufacturing trends and consumer behaviour

Global, regional and local partnerships

- Security-minded IoT alliances
- Certification organizations
- Civil society organizations
- Organizations that review consumer products
- Internet Society community

Outreach to policy makers

- Regional engagement in strategic countries
- Global and regional events
- Workshops and capacity building
- Thought pieces and articles

Get involved.

- Connect us with manufacturers and suppliers providing IoT products and services to adopt the OTA IoT Trust Framework
- Help us spread the word about the privacy and security risks of consumer IoT products and services
- Encourage policymakers to support better security and privacy features in IoT offerings
- Engage with policymakers, technical experts and consumer organizations around this issue in a collaborative and multistakeholder approach
- Promote our messages and recommendations to policymakers, as captured in the IoT Security for Policymakers paper
- Suggest key opportunities to broaden awareness of IoT security and privacy
- Recommend civil society and other partners to help us extend our reach

Thank you.

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120