

CaribNOG 17
12 April 2019
Bridgetown, Barbados

IoT Security & MANRS campaigns



Shernon Osepa,
Manager Regional Affairs Latin America & the Caribbean
osepa@isoc.org [@ShernonOsepa](https://twitter.com/ShernonOsepa)

Why does Internet Society care?

“An Open, Globally-Connected, Trustworthy, and Secure Internet for Everyone”



Why an IoT Security Campaign?

The number of IoT devices and systems
connected to the Internet will be more than
2.5x the global population
by 2020 (Gartner).



New devices, new vulnerabilities

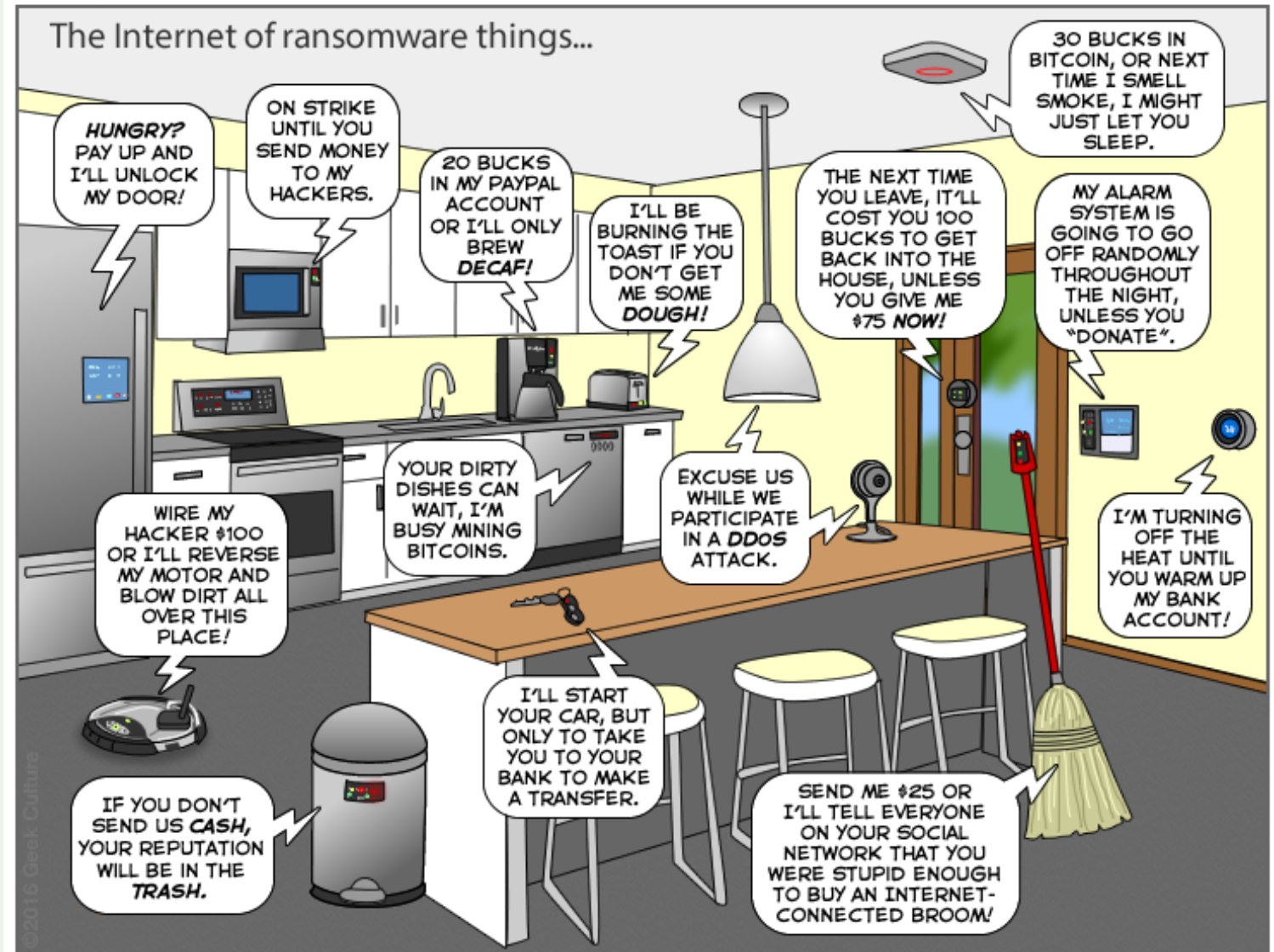
The attributes of many IoT devices present new and unique security challenges compared to traditional computing systems.

- **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**



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

The Joy of Tech™ by Nitrozac & Snaggy



Used with permission. <http://www.geekculture.com/joyoftech/joyarchives/2340.html>

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



There are two ways to view 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

Who is responsible?

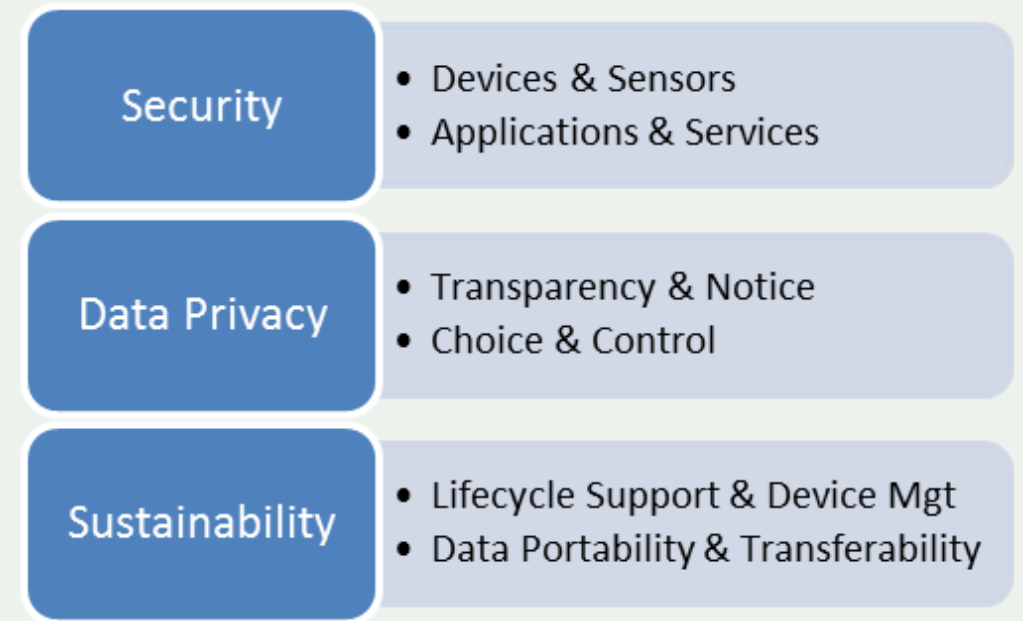
Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm

To scale up we need a collective approach, addressing security challenges on all fronts.



Online Trust Alliance IoT Security & Privacy Trust Framework

- Measureable principles vs. standards development
- Consumer grade devices (home, office and wearables)
- Address known vulnerabilities and IoT threats
- Actionable and vendor neutral



<https://otalliance.org/iot/>

Online Trust Alliance IoT Security Resources

Internet of Things A Vision for the Future



The rapid rise in the Internet of Things (IoT) has brought forth a new generation of devices and services representing the most significant era of innovation and growth since the launch of the Internet. IoT solutions are game-changers offering consumers, businesses and governments across the globe countless benefits. From fitness trackers to "smart" thermostats and connected toys to connected cities and healthcare services, society is on the cusp of a new technological era. By 2020, it is estimated that there will be in use worldwide in 2016 and will continue to grow every day.¹

"An ecosystem built on trust and innovation, where benefits to society and commerce are realized by prioritizing security and privacy"

In many cases, these fears may be justified. An insecure IoT device can drive collective action, becoming proxies for abuse with a capacity for disruption.

In order to realize the economic and social benefits of IoT, we must address these security, privacy, and trust issues. This will require innovation, leadership, and action. Stakeholders can come together and achieve what no one can do alone. We will also keep regulation at bay, increase the resilience of infrastructure and help bring IoT to scale.

The Online Trust Alliance (OTA) believes that a secure, private, and trustworthy world is possible. We are working with stakeholders to create a more trustworthy connected world. OTA is a policy-driven organization that proactively addresses these challenges.

Working with all stakeholders, OTA is committed to enhancing online trust and empowering standards and deep technology expertise, helping make security and privacy core to IoT.

Internet Of Things: A Vision For The Future



Securing the Internet of Things A Collaborative & Shared Responsibility

Society and the global economy are witnessing an unparalleled level of innovation being brought forth from the introduction of thousands of new Internet of Things (IoT) connected devices. They are providing significant benefits to the home and office, while wearable devices offer the promise of enhancing one's personal lifestyle and health. Yet to date, the level of commitment to device security, privacy and sustainability is unclear. Many within the security community believe industry is not adequately addressing fundamental security, privacy and life-safety issues. All too many IoT devices appear to be designed primarily for convenience and functionality while long-term security is conspicuously absent. Many of these "smart" devices are often not as smart as suggested.

In the absence of adoption of security norms and responsible privacy practices we are reaching a crossroads where regulation may be required. Yet in reality legislation by itself will not be effective. Passing regulation will take too long and will never keep pace with the evolving threat landscape. One promising alternative is an inclusive, multi-stakeholder effort that recognizes the need for change and expresses a willingness to adopt self-regulatory frameworks. Self-regulation is not without its own challenges. While well intended, it is often the case that decision makers are not committed and the consensus-driven process results in little if any impactful results.

Much like global warming or industrial pollution, there will be long-term consequences resulting from inaction with IoT threats. The impact of these threats have jumped to the physical world, ranging from unlocking doors, turning on cameras, shutting down critical systems and theft of personal property. The door has been opened. The lack of action has created a treasure chest ripe for abuse by white collar criminals, terrorists and state sponsored actors as IoT devices become weaponized. Left unchecked we may realize a "digital environmental disaster".



CHALLENGES OF THE CONNECTED AUTO, GYM, HOME & OFFICE

Risks to one's personal and physical safety have become reality. All too many connected devices ranging from automobiles and thermostats to children's toys and fitness devices, have insecure remote access and controls. By default many collect vast amounts of personal and sensitive information which may be shared and traded on the open market. The majority of these devices do not have the functionality (or an easily discoverable method) to easily remove one's personal data. Ideally, they would have a single reset button to delete all data on the device when the device is sold, transferred or rented to others. Such a function should preserve security patches and updates, while deleting user data and disabling any access by the previous owner, remove supporting applications and permanently deleting data related applications on backend services.



Enhancing the Security, Privacy & Safety of Connected Devices



Addressing cyber threats: identify the threat, assess the risk, and mitigate the damage

- ☐ Inventory all devices connected to your network and network.
- ☐ Contact your Internet Service Provider (ISP) to ensure that your network is secure and that your devices are not identified.
- ☐ Check that contact information is regularly updated.
- ☐ Confirm devices and services are secure and maximize protection.
- ☐ Review all passwords, accounts and avoid using codes no longer used. Reduce the risk of you being trying to access your device.
- ☐ Review the privacy policy and sharing with third parties. Reset as appropriate.
- ☐ Review devices' warranty, patches and updates, device.
- ☐ Before discarding, reset it to factory settings.
- ☐ Review privacy settings, contact sharing, bluetooth applications to promote security.
- ☐ Back up your files including contact information that are not permanent.

https://otalliance.org/SmartHome

8 104



SMART DEVICE PURCHASE & SETUP CHECKLIST Maximizing Security & Privacy with Your Smart TV & Connected Devices



SECURITY	
<input type="checkbox"/>	Prior to purchase confirm your ability to return the device for a refund if on set up you find the security and/or privacy practices do not comply with industry best practices or your personal requirements. If you cannot opt out of sharing data with third parties or are not provided the option of opting in, consider alternative products.
<input type="checkbox"/>	Prior to purchase review device's warranty and support policies and verify the security and software patches are provided for the life of the product, beyond that of the device warranty period offered by the manufacturer.
<input type="checkbox"/>	Register your device providing your contact information and primary email address with the manufacturer to help ensure you receive security updates and related notifications to help maximize your security and privacy.
<input type="checkbox"/>	Verify your device is updated and patched directly from the manufacturer. Install updates as soon as they become available. If possible enable automatic updates on the device setup options.
<input type="checkbox"/>	Use a unique user name and password which does not identify your family or the brand/model of the device and change them frequently. This can reduce the threat of your device being maliciously targeted by hackers.
<input type="checkbox"/>	When downloading apps to your device, install them directly from the manufacturer's official site where possible and carefully review any requested permissions such as location tracking, use of the camera and microphone.
<input type="checkbox"/>	When browsing sites with your connected device, exercise the same caution as you would with your personal computer.
<input type="checkbox"/>	Turn off and unplug your device(s) if you are gone for extended periods of time to reduce the risk of your device being hacked, being susceptible to power surges and save on energy use.
<input type="checkbox"/>	If possible, connect your device directly through a wired connection. If your home router has a guest network use it to isolate your device(s) from other networks.
<input type="checkbox"/>	Disable or protect remote access to your connected device(s) when not needed to reduce the risk of hacking.
<input type="checkbox"/>	Any device that connects to the Internet should be guarded by a firewall to help prevent unauthorized access. Use a router-based firewall and turn on any built-in firewall settings your device might have.
<input type="checkbox"/>	Document all of the smart devices and applications you use. List the company URL, passwords, contact email and phone numbers. Password protect the document or use a password "vault" mobile application.
PRIVACY	
<input type="checkbox"/>	If you are selling your connected device, reset the device to factory settings and/or clear any saved data. If you are purchasing or using a previously owned or opened device, be sure the device has been reset to factory settings (including advertising identifiers, parental controls and all privacy settings) before using it.
<input type="checkbox"/>	Review the privacy practices of connected devices you own or are considering buying including data collection and sharing policies with third parties. Reset permissions to reflect your preferences (for example - data collection and sharing, camera and microphone settings and other functions). If your settings cannot be modified, consider the "reset to factory settings" option to start a clean setup.
<input type="checkbox"/>	To maximize your privacy, disable use of the camera and microphone. Consider removing the camera, flipping it to face the wall or covering the camera lens to prevent accidental or unauthorized use. Doing so means the camera will only capture a black image or the wall.
<input type="checkbox"/>	Create user profiles with unique settings for children's use of the device.

ISOC “IoT Trust by Design” Campaign

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

Why a MANRS Campaign?

The challenges we face

Routing Incidents are Increasing!

Routing Incidents Cause Real World Problems!

MANRS improves the **security** and **reliability** of the global Internet routing system, based on **collaboration among participants** and **shared responsibility** for the Internet infrastructure.



Everyone Benefits

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.



Why join MANRS?

Improve your security posture and reduce the number and impact of routing incidents

Join a community of security-minded operators working together to make the Internet better

Use MANRS as a competitive differentiator



Join Us

Visit <https://www.manrs.org>

Fill out the sign up form with as much detail as possible.
We may ask questions and run tests

Get Involved in the Community

Members support the initiative and implement the actions in their own networks
Members maintain and improve the document and promote MANRS objectives



Thank you.

Shernon Osepa

Manager Regional Affairs Latin America & the Caribbean

osepa@isoc.org

Visit us at
www.internetsociety.org
Follow us
[@internetsociety](https://twitter.com/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

