



# The Insecurity of Things

## The adventures of IoT Security

- Be in a defensible position.
- Be cyber resilient.

June 8<sup>th</sup>, 2017



# Agenda

- Why Are We Here?
- Introduction to Internet of Things (IoT)
- IoT Risks
- Fun Facts
- IoT Hacking
- What can be done?
- Questions???

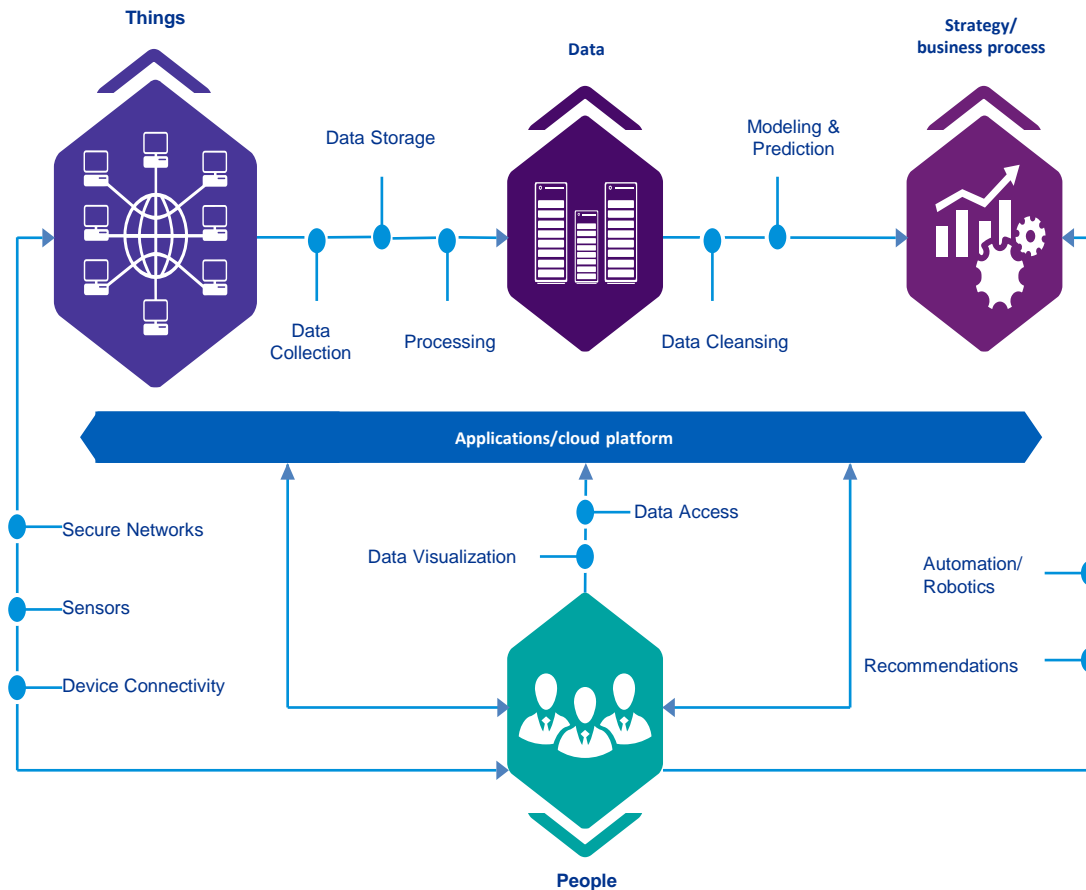




# Why Are We Here

- IoT is already an immense footprint with billions of points of presence on the Internet and it is only expected to grow at an ever increasing rate
- Organizations not always aware of what is on their own networks; people not always aware of use in daily life
- Leading to an equally immense potential attack surface as many of these devices are unsecured out-of-the-box
- Little to no regulation but awareness is growing
  - How can we address the security risks IoT devices represent
  - What can we do to drive towards a better IoT future

# What is the Internet of Things (IoT)?

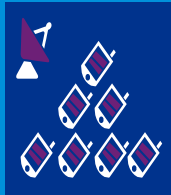


## Concepts

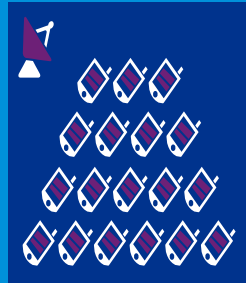
- Everyday devices and systems (i.e., things) are connected to the internet through low-cost sensors.
- Devices can autonomously take action based on real-time data, processes, and information.
- Interconnected devices collect environmental and behavioral data that can help generate timely business decisions and improve customer interactions.

# IoT (by the numbers)

## Mobile Devices



2015:  
**13B**



2020:  
**>34B\***

## Smart Homes



2015:  
**300M**

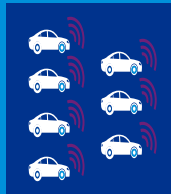


2020:  
**1B\***

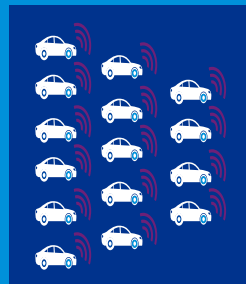
## 2025 IoT Usage Forecast:

- More company revenue from sales of services than products
- Over 10% of electricity will be micro-generated by consumers and contributed to the Smart Grid.
- At least 5 countries will target “zero road fatalities,” relying on connected cars and smart road infrastructure to prevent accidents.

## Connected Automobiles



2015:  
**370M**

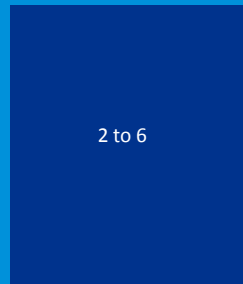


2020:  
**3.5B\***

## Connected Wearables



2020:  
**No. of wearable bands shipped\***



2020:  
**No. of IoT “devices” per person**

\*Analyst forecasts vary significantly in methodology and IoT definition

Source: [State of the Market: The Internet of Things 2015, Verizon \(2015\)](#)

# IoT (by the numbers)

- The IoT ecosystem has more stakeholders than traditional products
- Each stakeholder has a **specific perspective** paired with a **cost/benefit**
- Who is focused on the bigger picture? Who **is following the life of the data?**
- Is anyone focused on **building consumer trust** through security, safety, and privacy?



Creator



Enabler



Consumer

## Focus Areas

- Product functionality
- Design and consumer engagement
- Product adoption and platform promotion / preservation
- Telematics architecture
- Availability and connectivity
- Cost-focused service offerings and infrastructure management
- Product reliability and usability
- Dynamic user experience
- Privacy of personal information
- Brand loyalty and trust

# IoT Public Sector

- Why would the public sector want to invest in IoT?
  - Create cleaner cities
  - Deliver better healthcare
  - Make transportation systems safer
  - Conserve water
  - Boost productivity
  - Have IoT work for the everyday citizen

76%

76% of IoT adopters in public sector institutions say that an organizational structure that encourages flexibility and cross-functional work is important for improving performance around IoT<sup>3</sup>.

81%

81% of IoT early movers in the public sector believe their citizens increasingly expect them to offer enhanced services using data from IoT<sup>3</sup>.

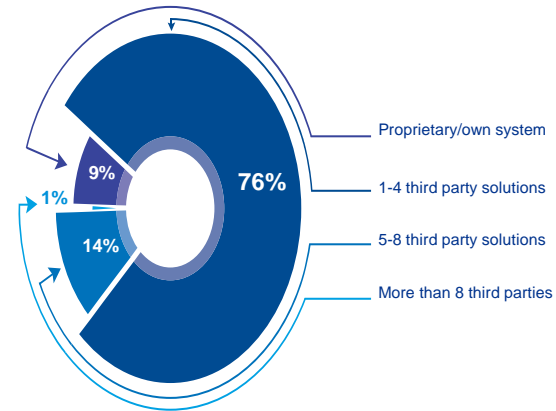
\*Analyst forecasts vary significantly in methodology and IoT definition

Source: State of the Market: The Internet of Things 2016, Verizon (2016)

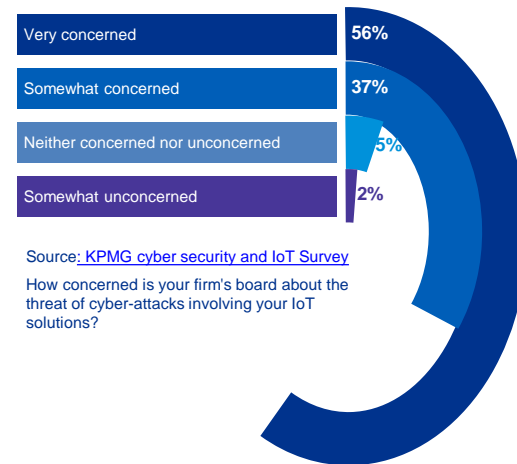
# Marketplace perspective

The IoT ecosystem is growing and users increasingly understand that they need to rely on third parties and providers to develop a strong market proposition

- KPMG's IoT Security survey demonstrated increased focus and concern from Boards of Directors
- Emphasis on foundational Security/Privacy by Design; layered throughout product lifecycle
- Third-party risk management viewed as largest threat to IoT ecosystem



IoT users and their boards are becoming increasingly concerned about the risk of cyber attack on their IoT solutions



Source: [KPMG cyber security and IoT Survey](#)

How concerned is your firm's board about the threat of cyber-attacks involving your IoT solutions?



# Stakeholder perspectives

- The IoT ecosystem has more stakeholders than traditional products
- Each stakeholder has a **specific perspective** paired with a **cost/benefit**
- Who is focused on the bigger picture? Who is **following the life of the data**?
- Is anyone focused on **building consumer trust** through security, safety, and privacy?

## Focus Areas



Creator

- Product functionality
- Design and consumer engagement
- Product adoption and platform promotion / preservation



Enabler

- Telematics architecture
- Availability and connectivity
- Cost-focused service offerings and infrastructure management



Consumer

- Product reliability and usability
- Dynamic user experience
- Privacy of personal information
- Brand loyalty and trust

# IoT introduces new risks

- The exponentially growing connected ecosystem is creating new challenges for organizations to manage
- Market innovation continues to invent new ways for devices, people, and the cloud to talk to one another, creating a moving target for developers, and security and risk professionals
- IoT has impacts on various risk domains, notably security, privacy and safety, which all impact trust

## Examples of IoT Impacts on Risk Domains



### Security

- Denial of service attack, causing disruption of communications
- Spoofing a device to take control or exfiltrate data.
- Theft of device to gain foothold into an IoT ecosystem



### Privacy

- Release of location history
- Release of personal data stored on a device or in the cloud, with the potential for blackmail
- Release of corporate data/trade secrets



### Safety

- GPS location tampering to facilitate robbery, ambush, etc.
- Medical device tampering, causing negative impact to health/life.
- Sensor tampering, causing vehicle crash, robot malfunction, nuclear accident, etc.



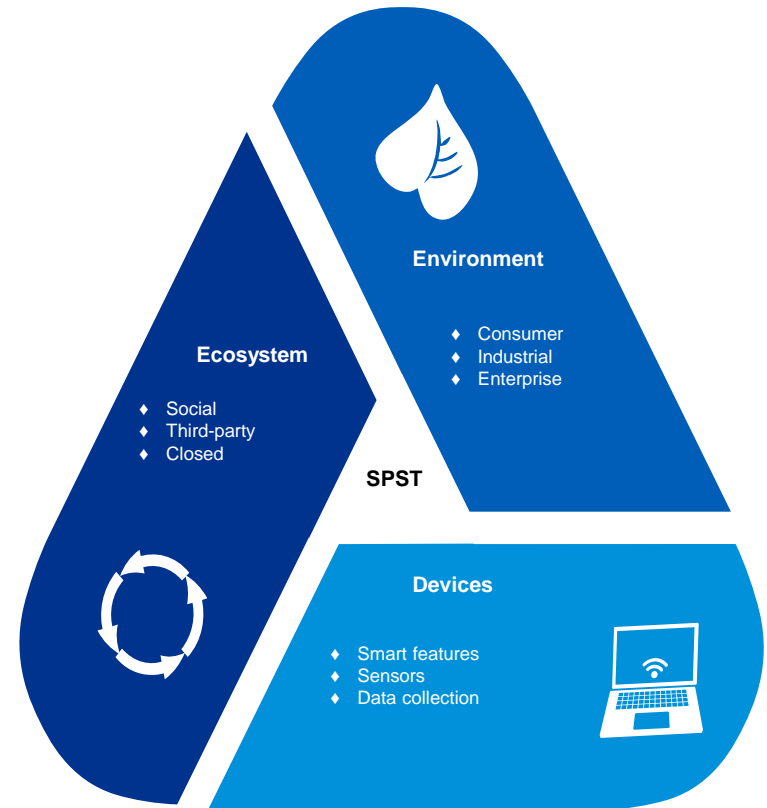
Trust

## Examples of IoT Incidents

- Vehicle remotely controlled
- Iran's nuclear program damaged by Stuxnet
- German steel mill boiler damaged
- DDoS caused by IoT botnet
- Credit cards breached via HVAC

# KPMG's understanding of IoT risks

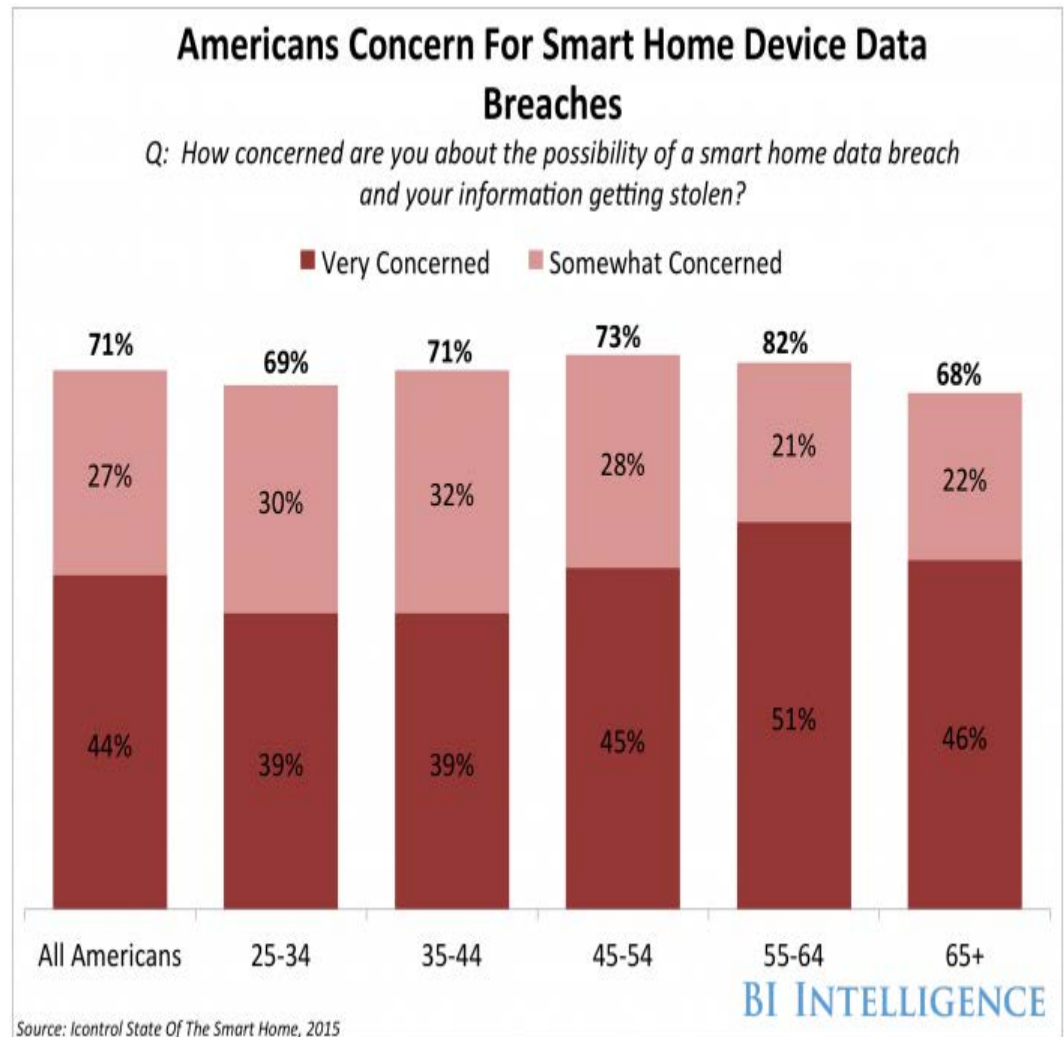
- Our approach to understanding IoT risk is to evaluate devices and their interconnections within, their ecosystem based on the risk domains of security, privacy, trust, and safety. When assessing an IoT device from these four domains, we identify risks from three perspectives:
  - Device: Is it a smart device? Or is it simple? Is the device able to perform complex tasks and provide data? Does the device perform automated tasks, based on sensor data?
  - Ecosystem: Is the device part of an open standard? Does it work with multiple types of systems? Does it need to interact with third parties? Is the network isolated?
  - Environment: Is the device used in a consumer, industrial, or enterprise context? Is the device mobile? Is it required to be in a public area to record data?
- By considering these perspectives, KPMG is able to form a threat landscape specific to an IoT product, enabling further evaluation of risks and controls within an organization's IoT program.



**SPST** = Security, Privacy, Safety and Trust

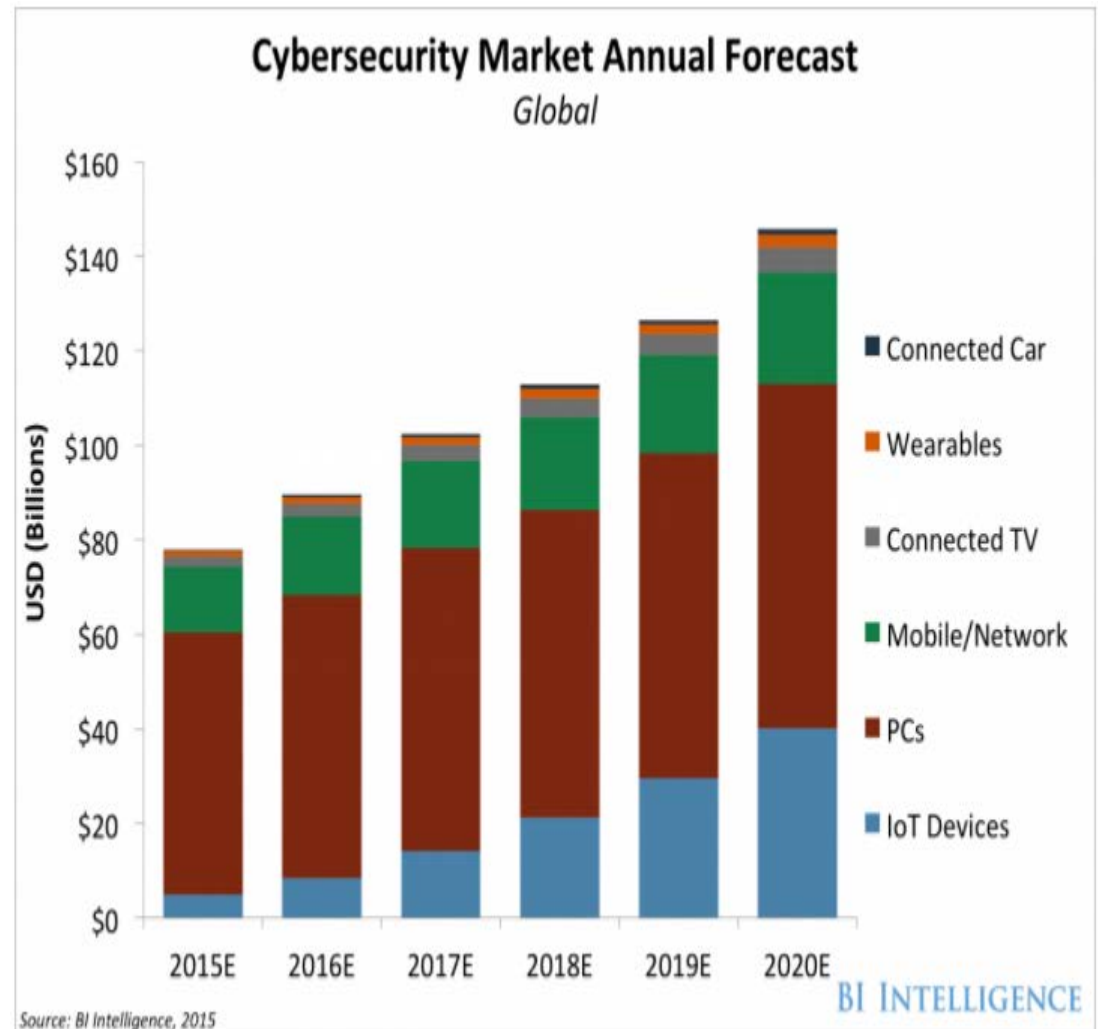
# Simply Put: People are worried about IoT

- ...and they should be – the security track record for IoT devices is horrendous
- Convenience leads to compromising the security of more critical systems
- The people building these devices – don't know how they're hacked.



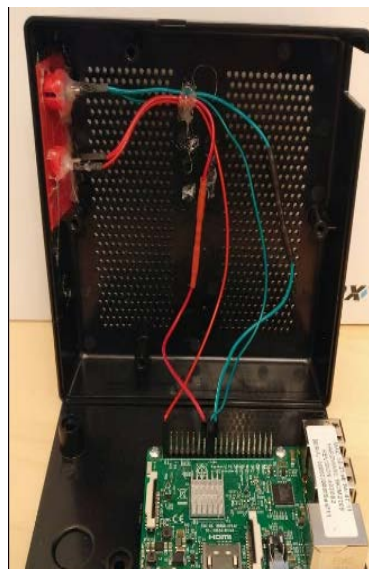
# Why attack systems that have security – if there's tons without?

- PC's have security software, does your thermostat or car?
- IoT: Small system – less ability to update
- No commitment to patching
- Do you know what data is leaking out



# If security vendors can't get it right, what makes IoT vendors think they can?

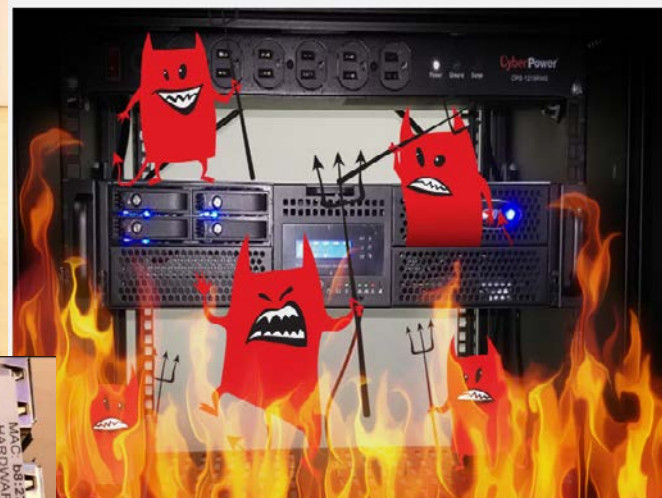
- IoT vendors shouldn't build things without first understanding how they can be broken into
- What risk are you bringing into your organization?



## Punching holes in nomx, the world's "most secure" communications protocol

Extraordinary claims require extraordinary proof, and nomx implodes under scrutiny.

SCOTT HELME 4/27/2017, 10:05 AM



Artist's impression of a nomx product under the scrutiny of security researchers.

<https://arstechnica.com/information-technology/2017/04/punching-holes-in-nomx-the-worlds-most-secure-communications-protocol/>

# If security vendors can't get it right, what makes IoT vendors think they can?

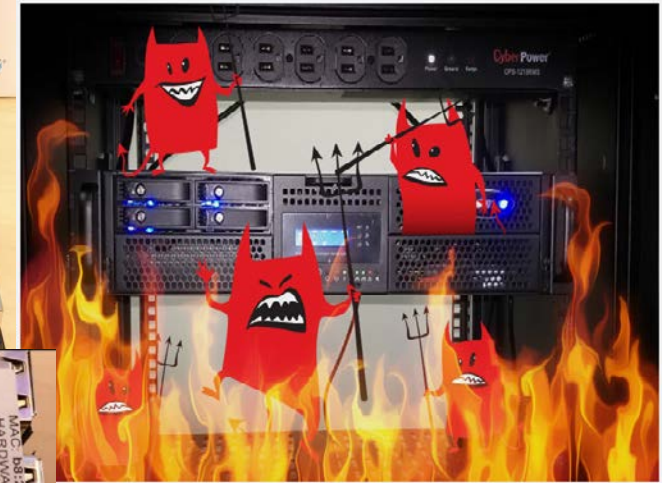
- BTW – that's a Raspberry Pi in there... (>\_>)



Punching holes in nomx, the world's "most secure" communications protocol

Extraordinary claims require extraordinary proof, and nomx implodes under scrutiny.

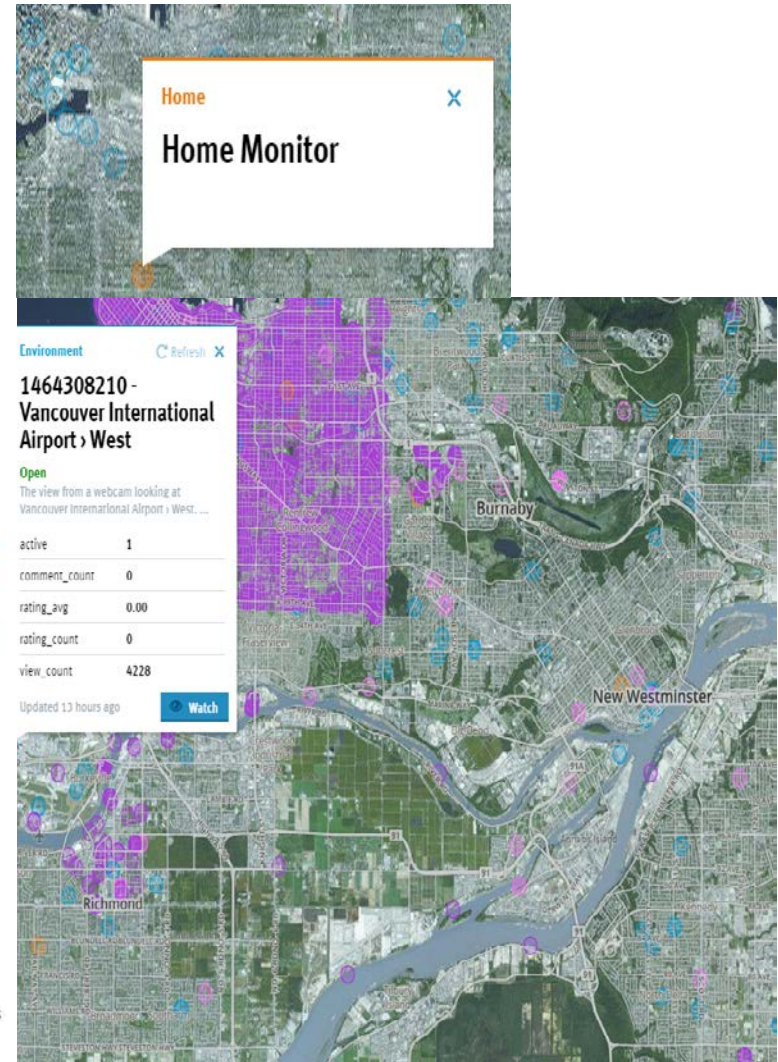
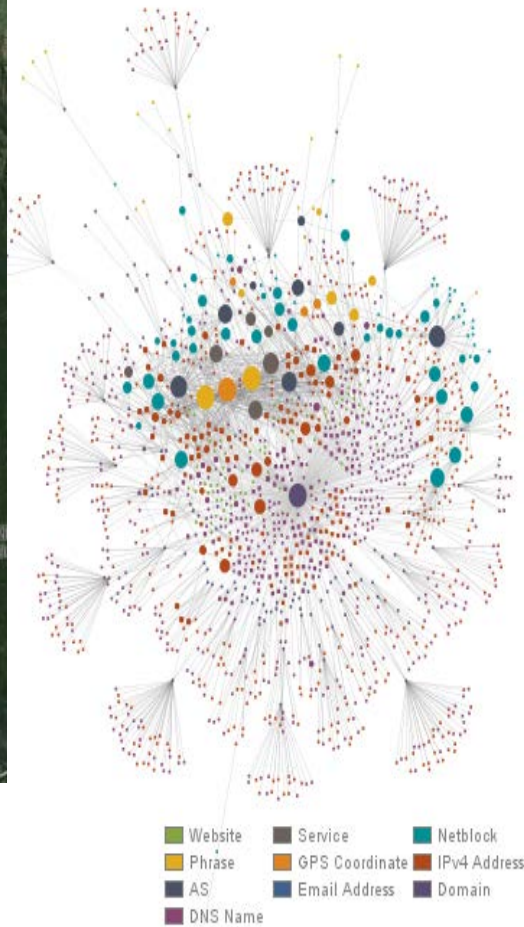
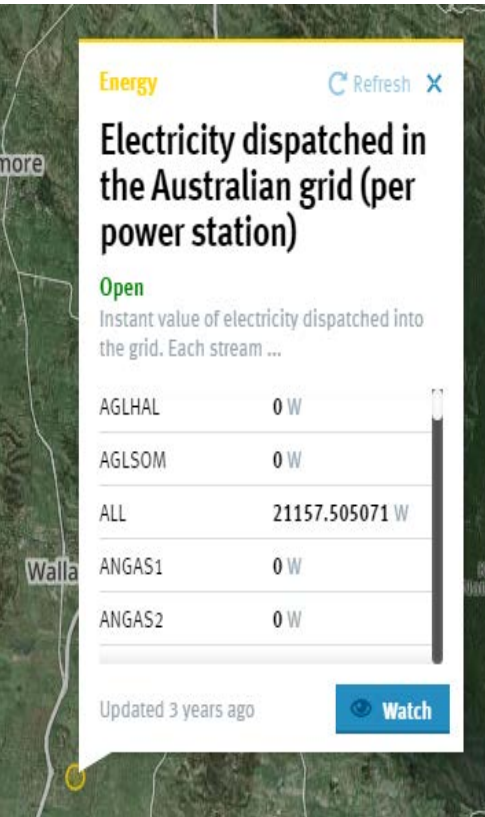
SCOTT HELME - 4/27/2017, 10:05 AM



/ Artist's impression of a nomx product under the scrutiny of security researchers.

<https://arstechnica.com/information-technology/2017/04/punching-holes-in-nomx-the-worlds-most-secure-communications-protocol/>





# Getting Intel – IoT Scanning Tools





# KPMG thought leadership

Additional IoT related resources available for download at KPMG Global

-  [KPMG Connected Devices Portal](#)
-  [Security and the IoT ecosystem](#)
- 
  - [Automotive](#)
  - [Your connected car is talking. Who's listening?](#)
  - [Test-driving vehicle cybersecurity](#)
- 
  - [Healthcare](#)
  - [The time to address medical device cybersecurity is now](#)



**KPMG**

## Your connected car is talking. Who's listening?

Moving the data-driven user experience forward with value, security and privacy

@YourCar: Feeling extra #chatty today.

The graphic features a dark background with a car's dashboard and speedometer visible in the bottom right corner.

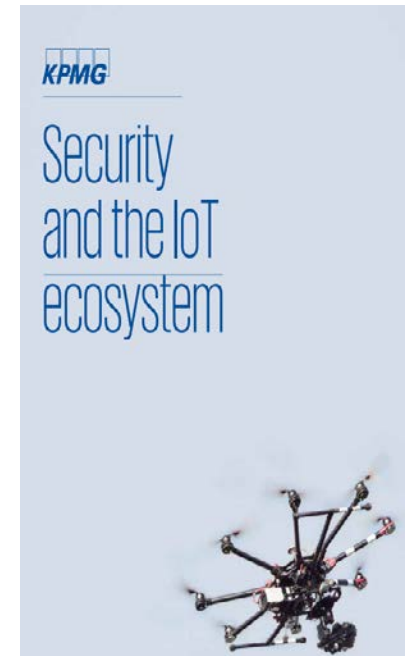


**KPMG**

## The time to address medical device cybersecurity is now

Corporate reputations, hospital operations, and patient safety are all at stake.

The graphic shows a blurred background of medical equipment with a digital display showing '98'.



**KPMG**

## Security and the IoT ecosystem

The graphic features a light blue background with a drone flying in the bottom right corner.



Questions?





# Thank you

KPMG's Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

- Contact us

Guy Grosario

Manager, Cyber Security

T: 250 589 2538

E: [grosario@kpmg.ca](mailto:grosario@kpmg.ca)



[kpmg.ca/cyber](https://kpmg.ca/cyber)



© 2017 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.