

# APSI DAY

## INTERNET OF THINGS

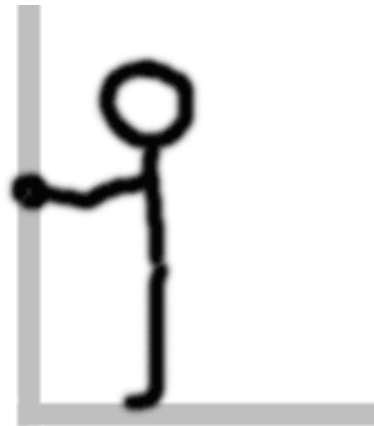
“Risks linked to this new Universe – And if it is an opportunity?”

Christophe Bianco  
2 November 19th 2014

# Internet of Things

---

**Threat or Opportunity?**



# Google Is Buying Connected Device Company Nest For \$3.2B In Cash

Posted Jan 13, 2014 by [Matthew Panzarino \(@panzer\)](#)

16.1k  
SHARES



Google is acquiring connected device company Nest for \$3.2 billion. Google sent out an email to employees noting the acquisition today and later issued a press [release](#).

ADVERTISEMENT

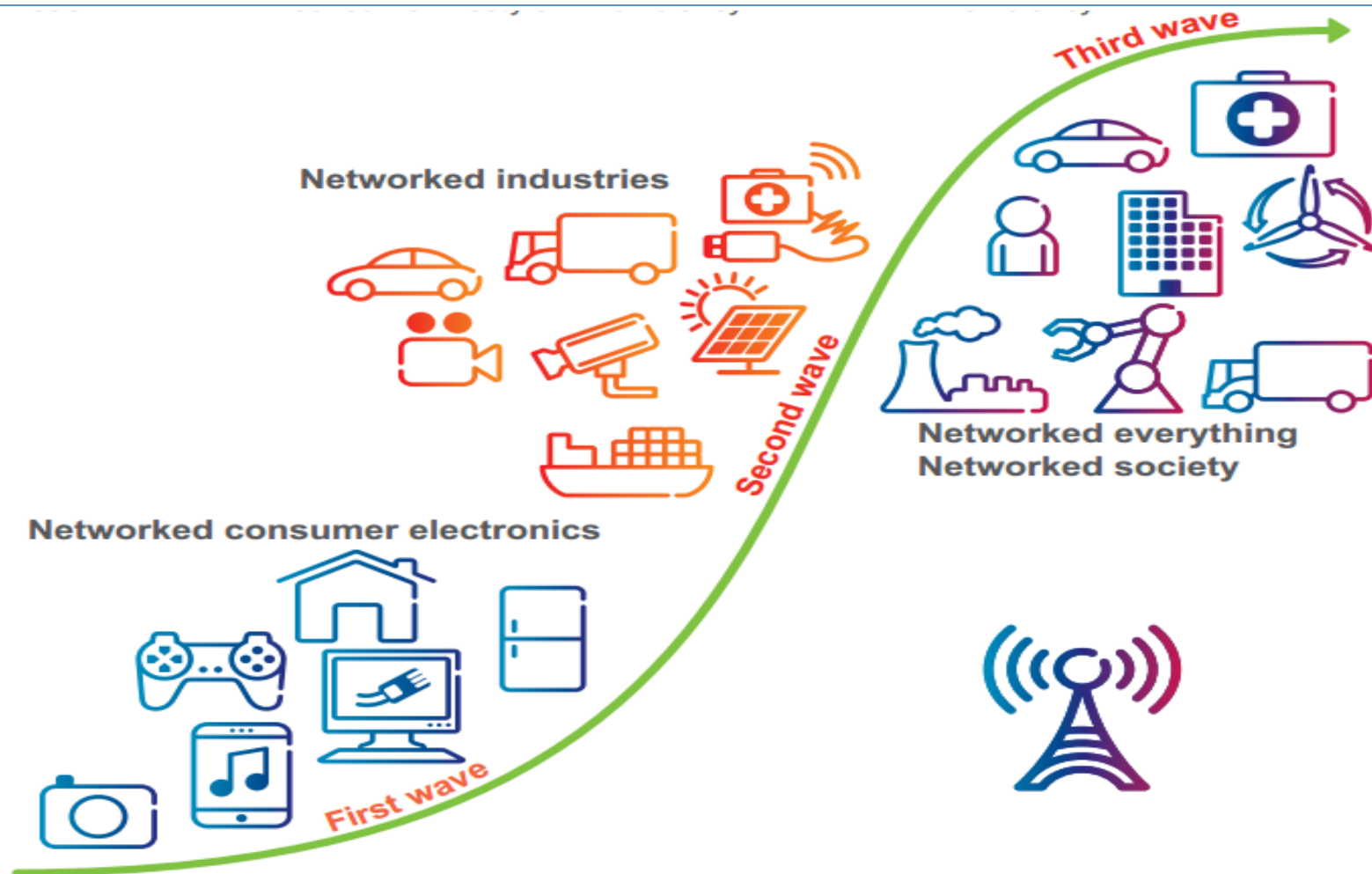


## CrunchBase

**Nest Labs**

FOUNDED

# A tremendous market



Business insider, *Here's Why 'The Internet Of Things' Will Be Huge, And Drive Tremendous Value For People And Businesses*, Dec. 2013  
CB Insights, *Internet of Things Companies Haul In More than \$1 Billion in Venture Capital in 2013*, March 2014

# A disruptive approach

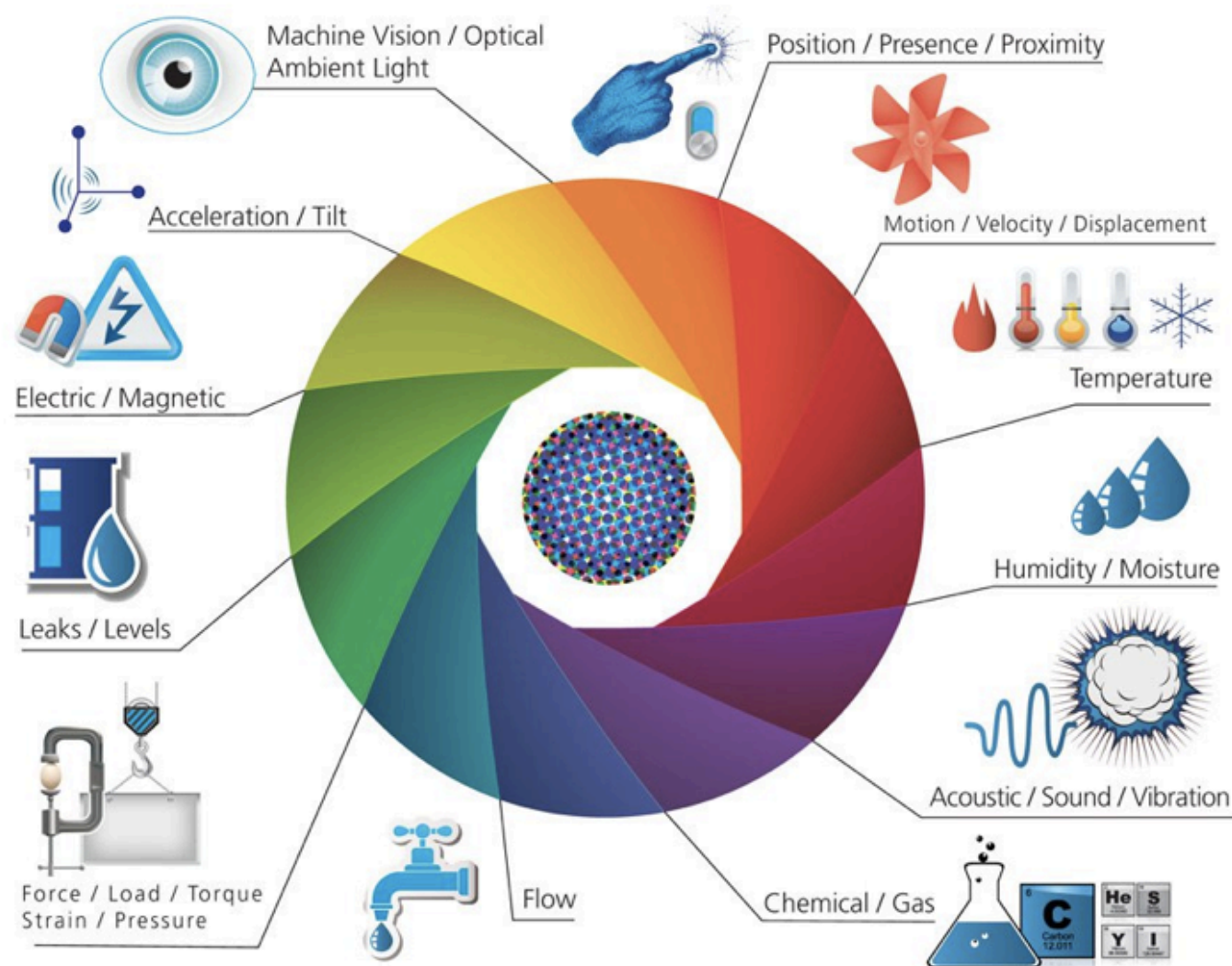
---

From computing devices to an everyday devices' connectivity

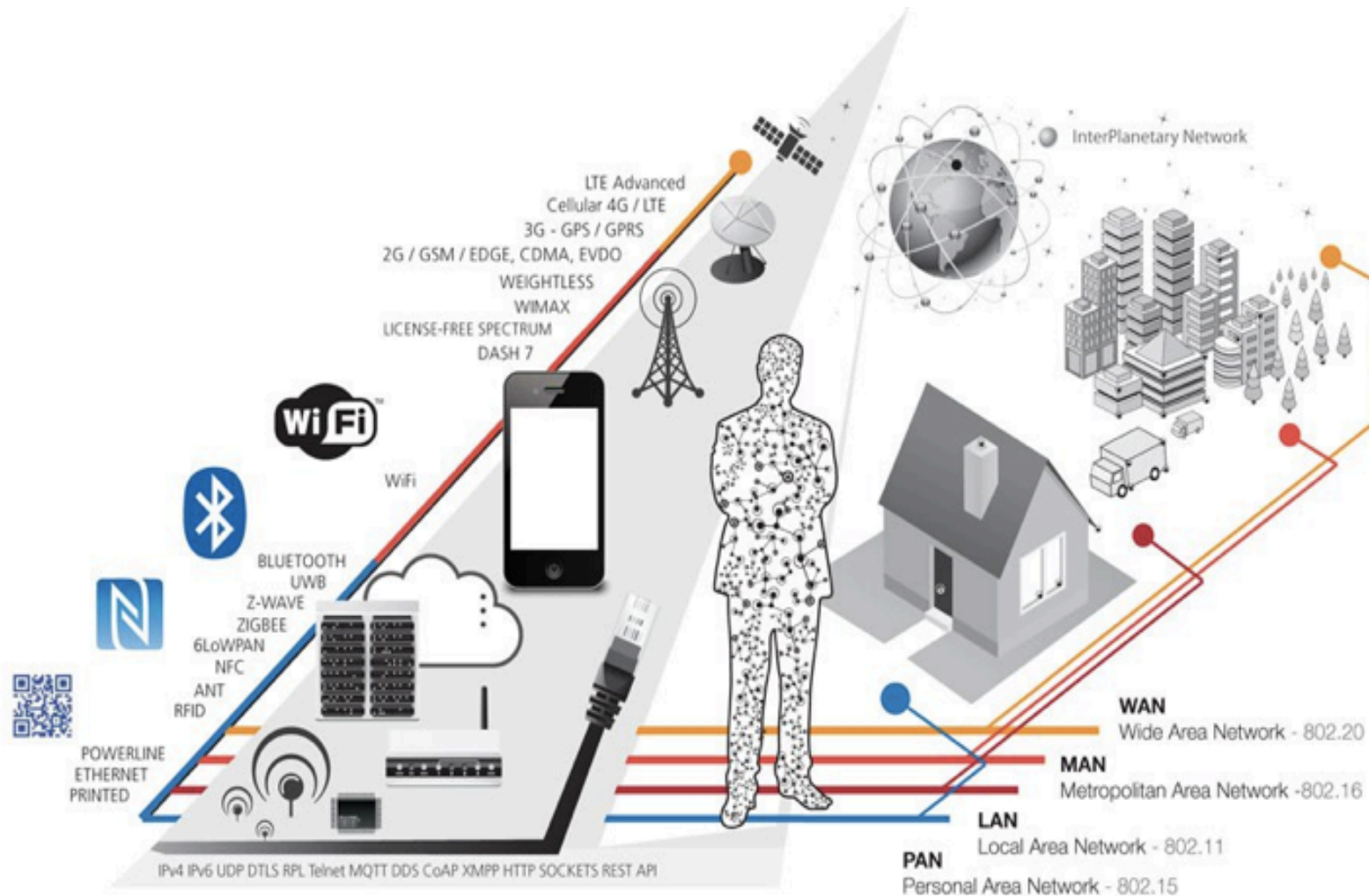
- Miniaturization & nanotechnologies partially enable the growth of the Internet of things
  - As sensors become a low-cost technology, it is cheaper and cheaper to add them to any device
- ➔ Machine-to-Machine communications begin to power billions of everyday devices, from parking meters to home thermostats
- Big data is high volume, velocity & variety information
  - Connected devices create, collect & communicate big data
- ➔ The future will see an Internet of Things where billions of devices are connected to each other, all sharing data via the Internet

# We are giving our world a nervous system!

---

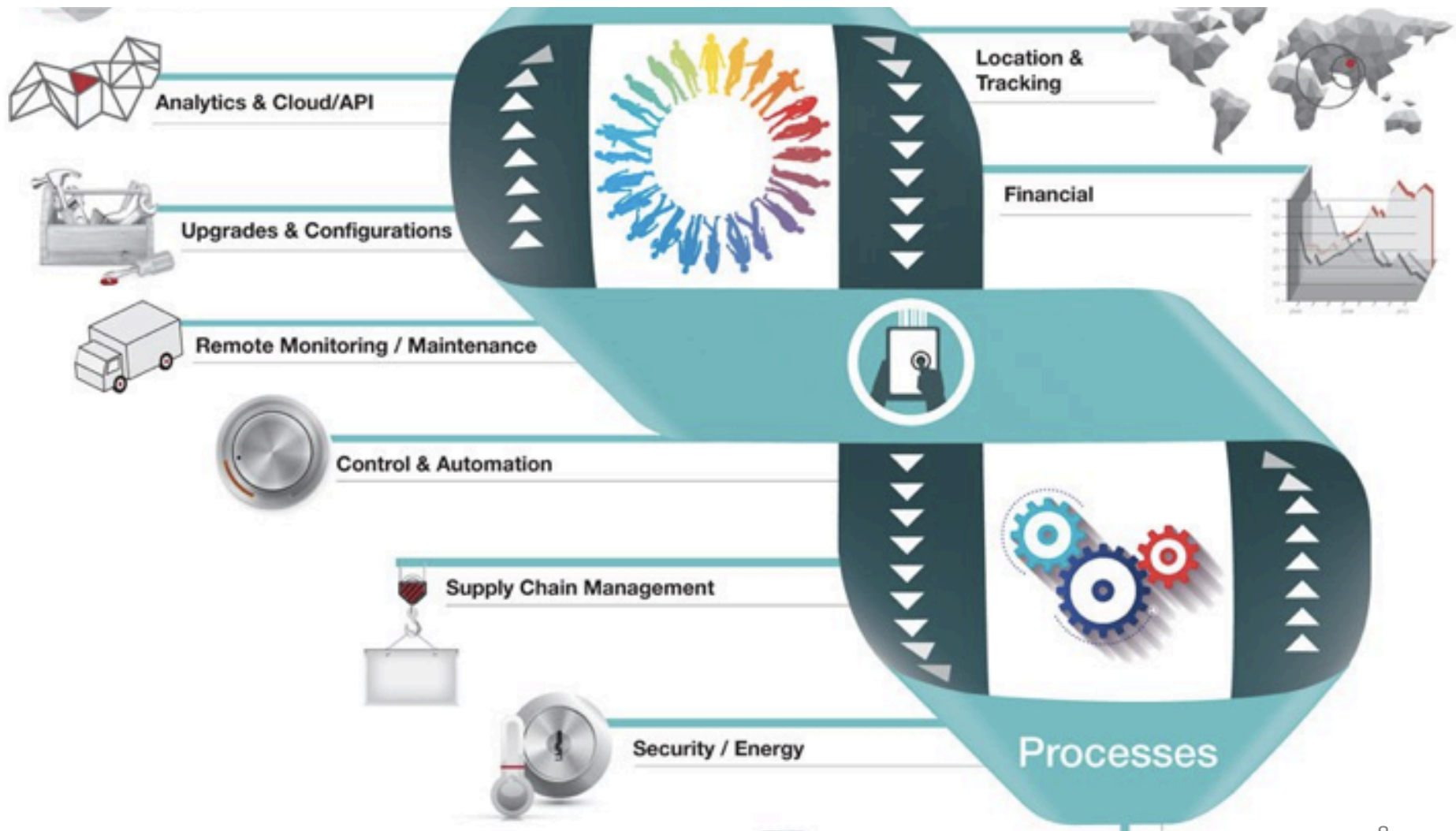


# Digitalized onto networks ...





# Integrating People & Processes





# Allowing to create new types of smart applications and services

---

## SMART THERMOSTATS



Save resources and money on your heating bills by adapting to your usage patterns and turning the temperature down when you're away from home.

## CONNECTED CARS



Tracked and rented using a smartphone. Car2Go also handles billing, parking and insurance automatically.

## ACTIVITY TRACKERS



Continuously capture heart rate patterns, activity levels, calorie expenditure and skin temperature on your wrist 24/7.

## SMART OUTLETS



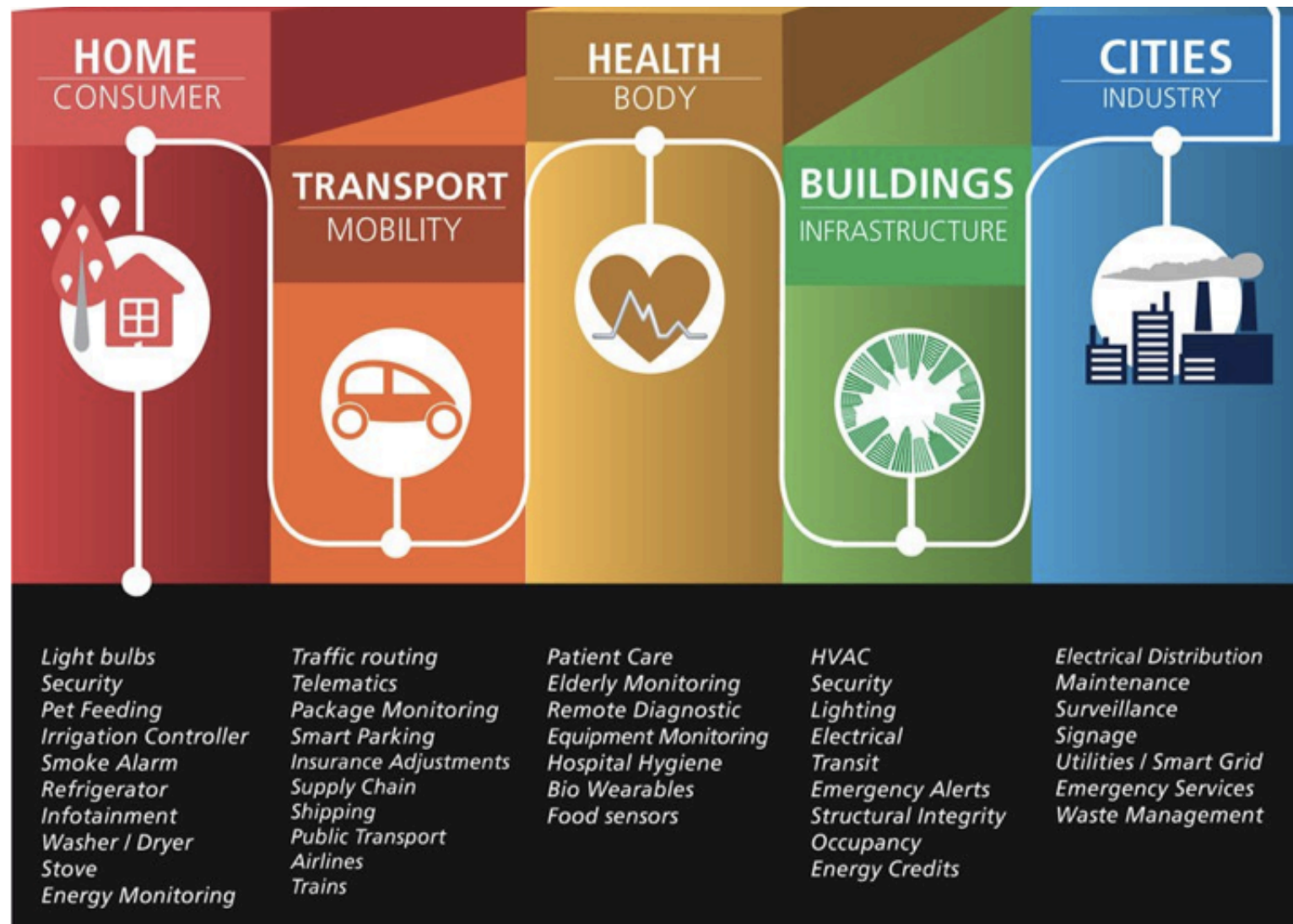
Remotely turn any device or appliance on or off. Track a device's energy usage and receive personalized notifications from your smartphone.

## PARKING SENSORS



Using embedded street sensors, users can identify real-time availability of parking spaces on their phone. City officials can manage and price their resources based on actual use.

# With Specific domains targeted!



# IoT – New opportunities

---

- ***New business models:*** The IoT will help companies create new value streams for customers, institute processes that speed time to market, triage market performance, and respond rapidly to customer needs.
- ***Real-time information on mission-critical systems:*** With IoT, organizations can capture more data about their processes and products in a more timely fashion to create new revenue streams, improve operational efficiency, and increase customer loyalty.
- ***Diversification of revenue streams:*** The IoT can help companies create new services and new revenue streams on top of traditional products, e.g., vending machine vendors offering inventory management to those who supply the goods in the machine.
- ***Global visibility:*** The IoT will make it easier for enterprises to see across the business regardless of location, including tracking effectiveness and efficacy from one end of the supply chain to the other.
- ***Efficient, intelligent operations:*** Access to information from autonomous end points, as today's smart grid already supplies to utility companies, will allow organizations to make on-the-fly decisions on pricing, logistics, sales, and support deployment, etc.



# Privacy?

---

## EBay asks 145 million users to change passwords after cyber attack

BY JIM FINKLE, SOHAM CHATTERJEE AND LEHAR MAAN

BOSTON/BANGALORE | Wed May 21, 2014 4:25pm EDT

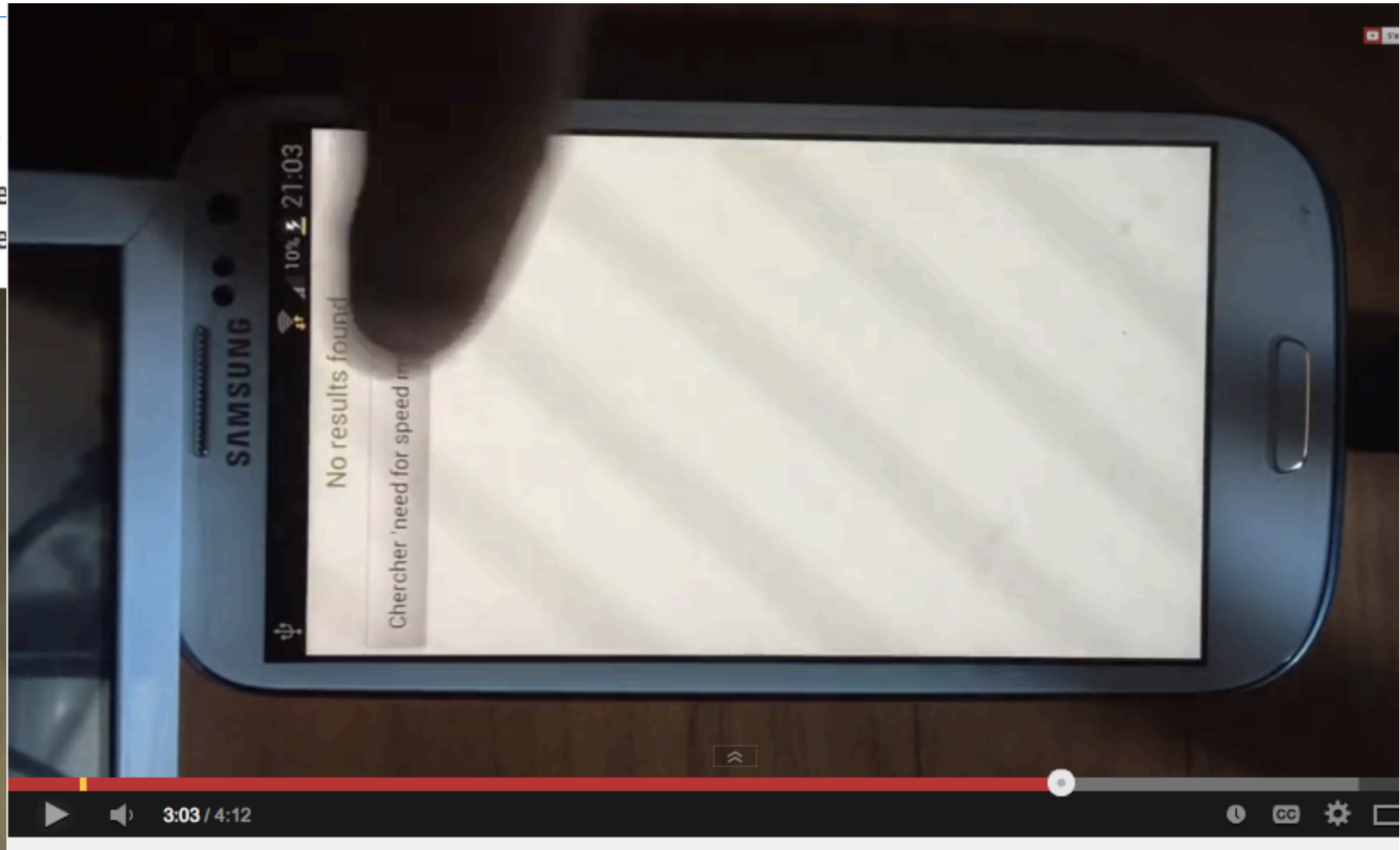
[Tweet](#) 1,076 [in Share](#) 248 [f Share this](#) [g+1](#) 91 [Email](#) [Print](#)



John Donahoe, chief executive of eBay, speaks at the Reuters Global Technology Summit in San Francisco, June 17, 2013.

# Security?

If  
ge  
de



[Crack]Jailbreaker son téléphone android en 2 minutes



# But is it new?

The image is a screenshot of the Shodan website's homepage. The background is dark with a green grid pattern on the left side, resembling a computer screen. At the top, the Shodan logo (three red dots) and the word "SHODAN" are visible. Below the logo, there is a search bar. The main heading "EXPOSE ONLINE DEVICES." is in large, white, bold letters. Underneath, a list of device types is shown: "WEBCAMS. ROUTERS. POWER PLANTS. IPHONES. WIND TURBINES. REFRIGERATORS. VOIP PHONES." To the right of this text is a red map of the Americas. At the bottom, there are two buttons: "TAKE A TOUR" (red) and "FREE SIGN UP" (green). Below the buttons, a line of text reads "Popular Search Queries: D-Link Internet Camera - D-Link Internet Camera DCS-5300 series, v".

**SHODAN**

## EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.  
POWER PLANTS. IPHONES. WIND TURBINES.  
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries: D-Link Internet Camera - D-Link Internet Camera DCS-5300 series, v



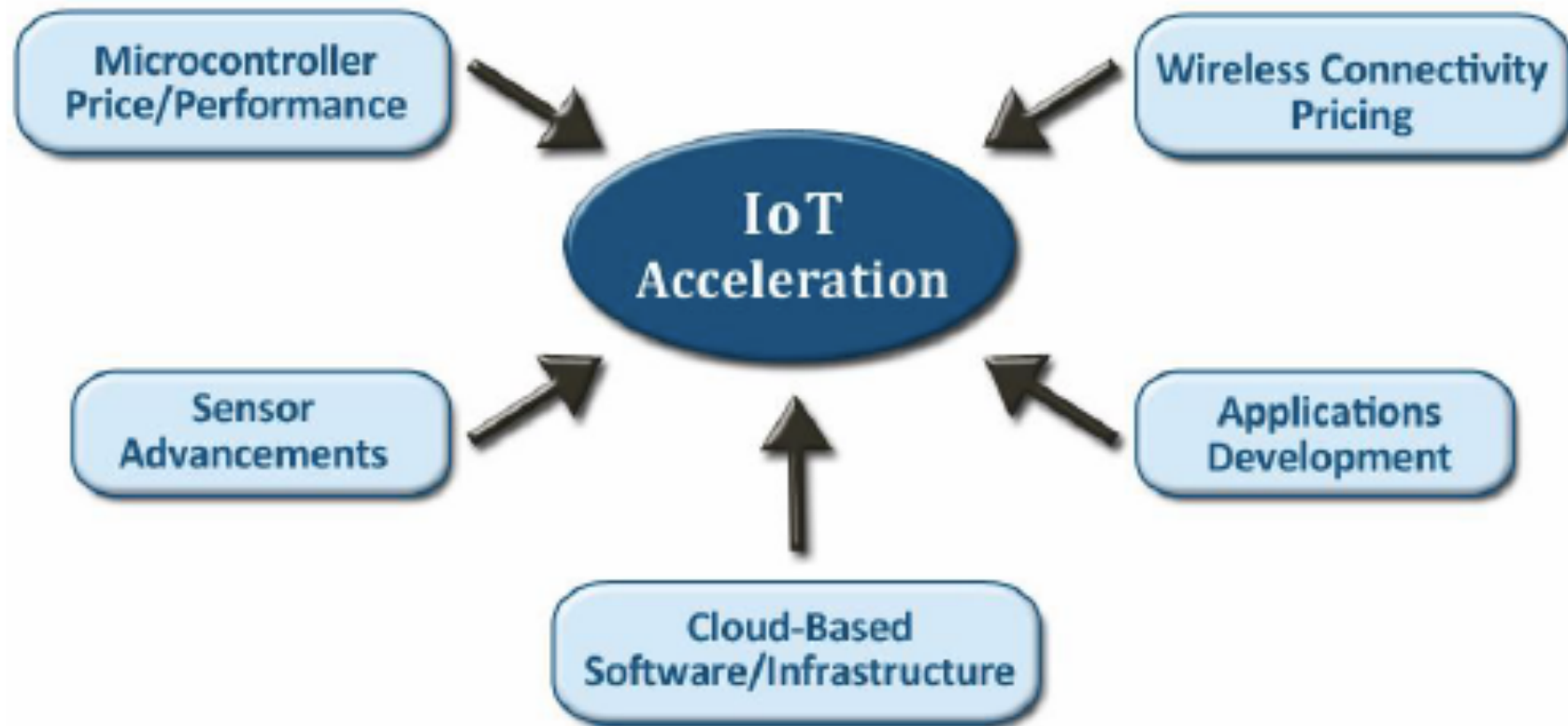
# Top 10 risks of IoT (based on OWASP)

---

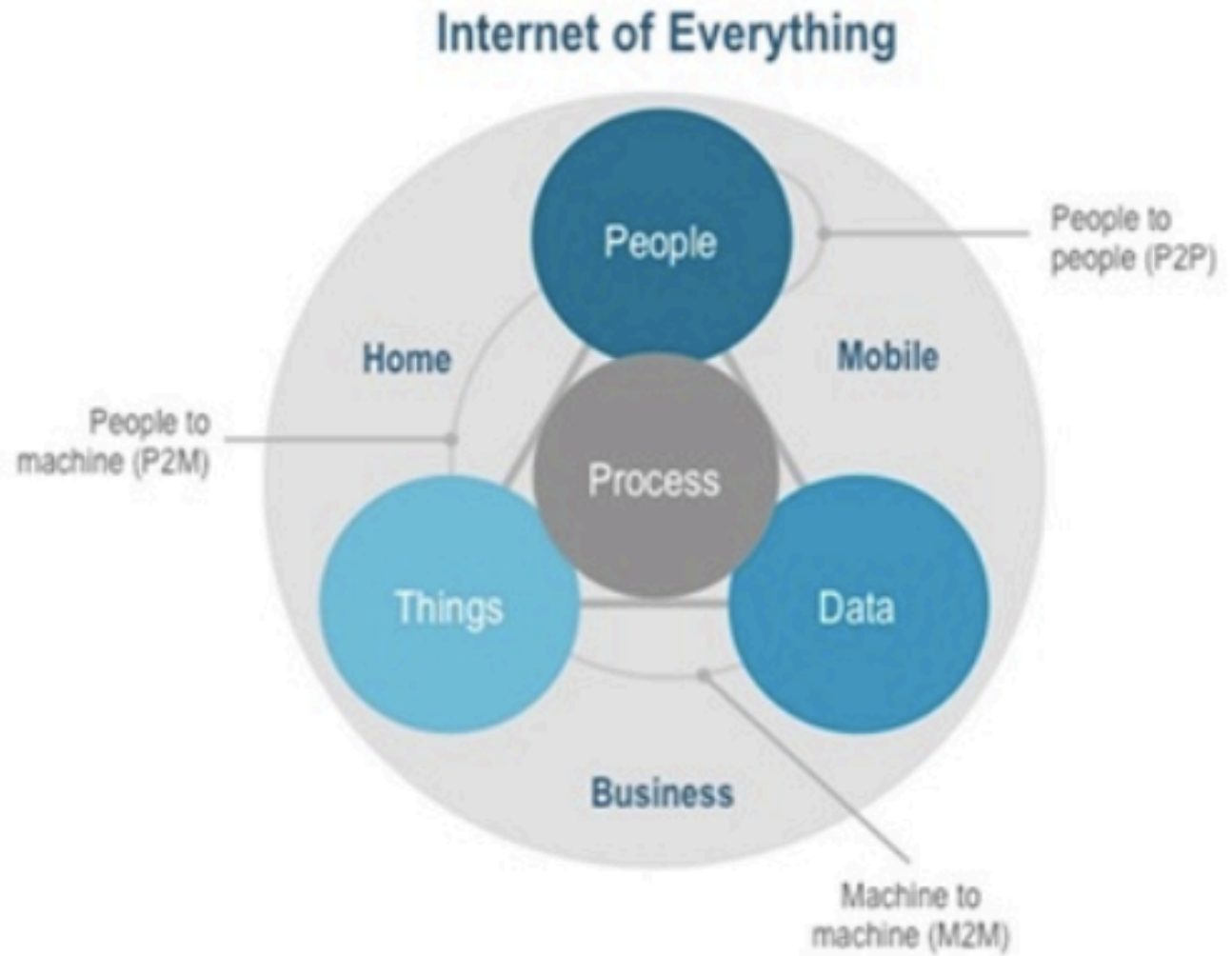
1. ***Insecure Web Interface*** >> Consider anyone who has access to the web interface including internal and external users.
2. ***Insufficient Authentication / Authorisation*** >> Consider anyone who has access to the web interface, mobile interface or cloud interface including internal and external users.
3. ***Insecure Network services*** >> Consider anyone who has access to the device via a network connection, including external and internal users.
4. ***Lack of transport encryption*** >> Consider anyone who has access to the network the device is connected to, including external and internal users.
5. ***Privacy concerns*** >> Consider anyone who has access to the device itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.
6. ***Insecure Cloud interface*** >> Consider anyone who has access to the internet.
7. ***Insecure Mobile interface*** >> Consider anyone who has access to the mobile application.
8. ***Insufficient security configurability*** >> Consider anyone who has access to the device.
9. ***Insecure Software / Firmware*** >> Consider anyone who has access to the device and/or the network the device resides on.
10. ***Poor physical security*** >> Consider anyone who has physical access to the device.

# Acceleration / combination

---

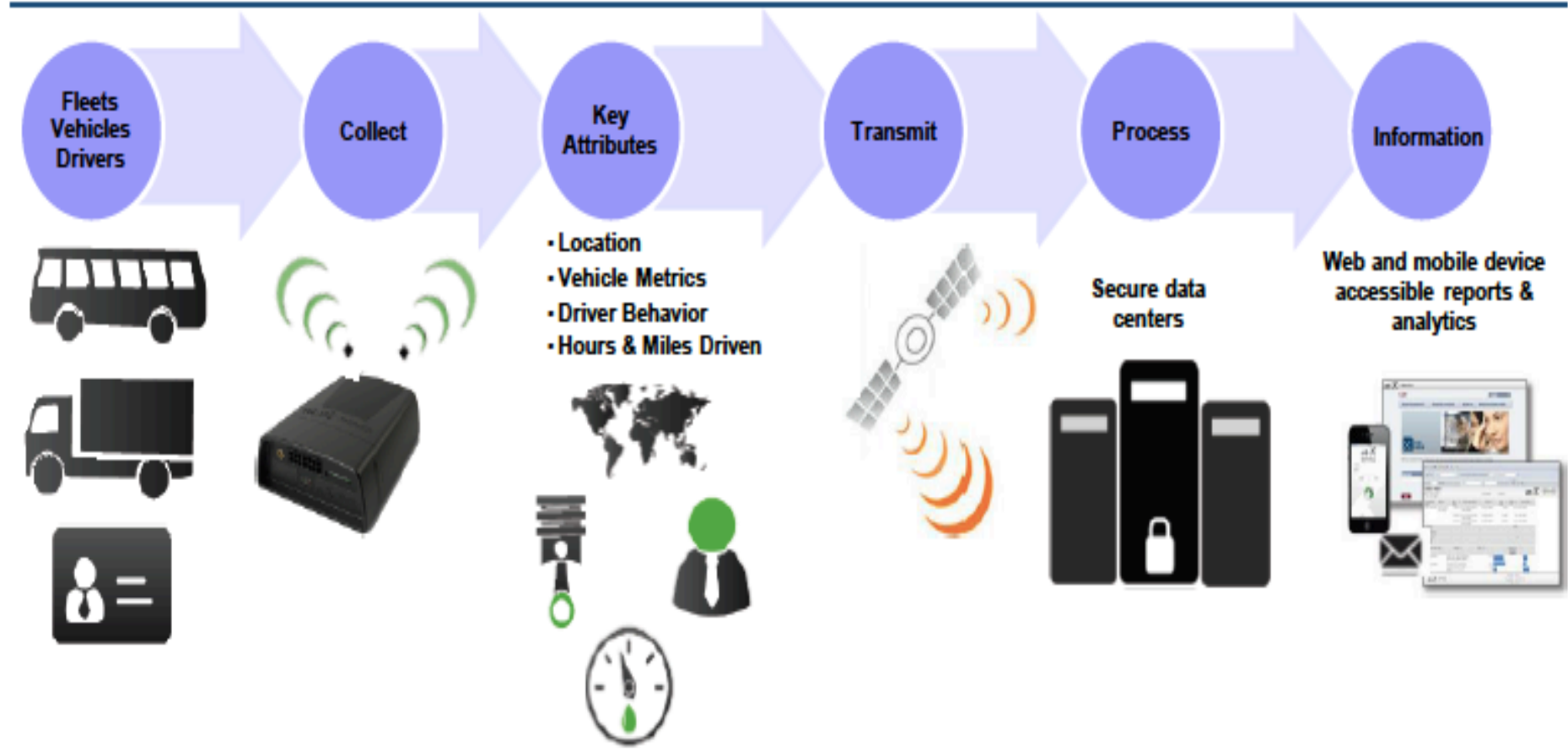


# Internet of .... Everything



# A fully integrated chain

---

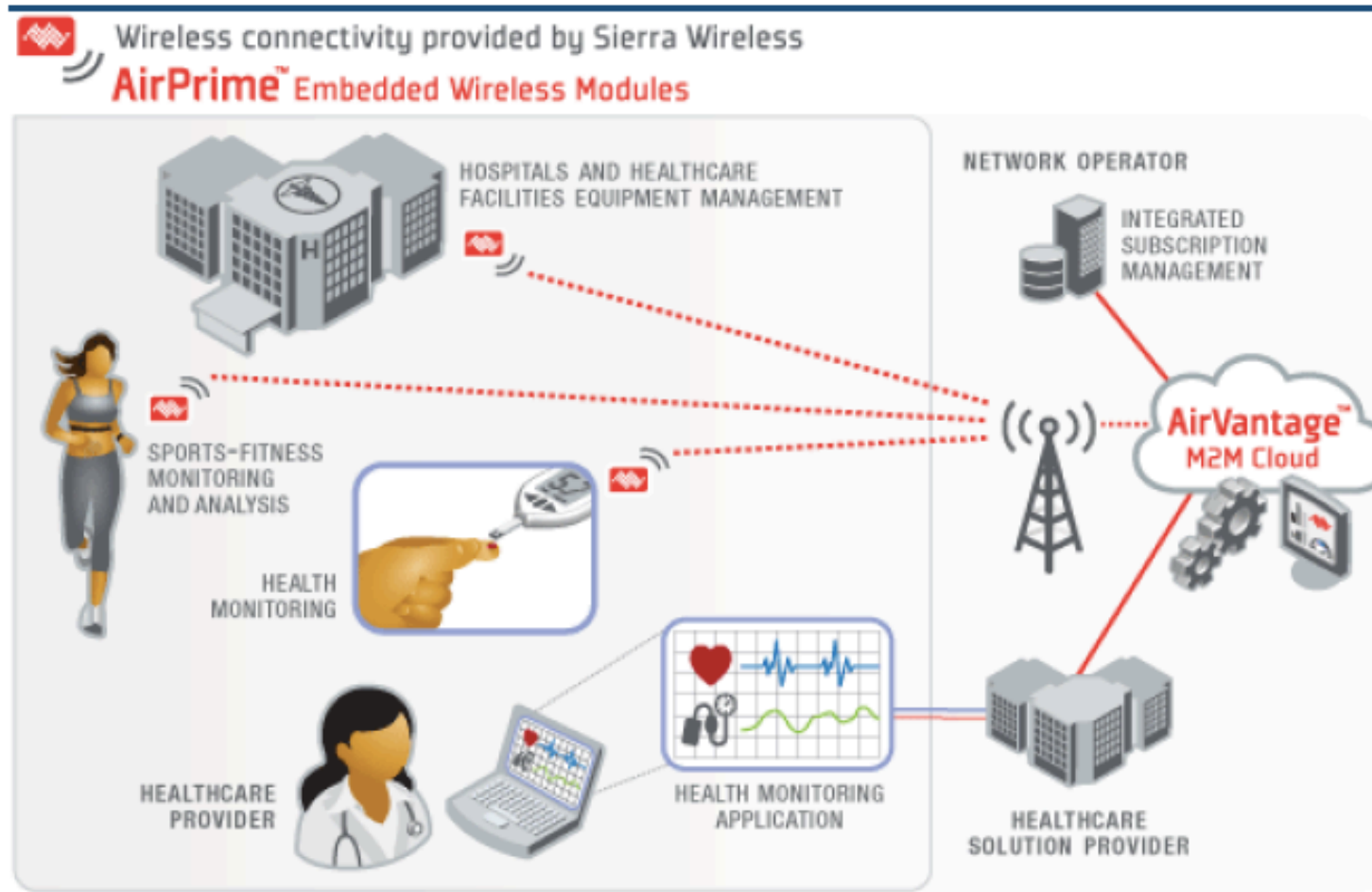


# Risk aversion or opportunity?

---



# But of course .... Cyber crime interest!









# Advices for users

---

- Use a screen lock or password to prevent unauthorized access to your device
- Do not reuse the same user name and password between different sites
- Use strong passwords
- Turn off Bluetooth when not required
- Be wary of sites and services asking for unnecessary or excessive information
- Be careful when using social sharing features
- Avoid sharing location details on social media
- Avoid apps and services that do not prominently display a privacy policy
- Read and understand the privacy policy
- Install app and OS updates when available
- Use a device based security solution
- Use full device encryption if available

*(The following steps could help users stay safe when using self-tracking apps)*

# Advices for app developers and service providers

---

- Build security in from the start, not as an afterthought
- Always use secure protocols when transmitting data
- Ensure that the device is not directly or indirectly traceable
- Only collect data that is necessary to provide a service and nothing more
- Require strong passwords for user accounts
- Implement secure session management
- Follow best practices for password handling (only store salted hashes and not the real password)
- Follow secure coding practices
- Provide an easy to understand privacy policy and act within the stated policy
- Pen test system infrastructure to ensure security
- Ensure that backend systems are well protected from intrusion
- Make security testing a part of the product development process
- Ensure that staff are properly trained on how to handle sensitive information
- As a data controller, be sure to comply with relevant data protection laws

# Thanks!

---



**Christophe Bianco**  
***[cbianco@excellium-services.com](mailto:cbianco@excellium-services.com)***