Internet Of Things (IoT)

William Favre Slater, III, M.S. MBA, PMP, CISSP, CISA

Sr. Cybersecurity Consultant and Adjunct Professor, IIT School of Applied Technology

ILLINOIS INSTITUTE OF TECHNOLOGY

Agenda

- Introduction
- WHY is this Presentation Important?
- Internet of Things – How Big Is It?
- Internet of Things Ecosystem
- Internet of Things at Work
- Hidden IoT at Work
- Developers and the Internet of Things
- Business and the Internet of Things
- Actual Internet of Things Devices – Raspberry Pi and eRIC
- The Security Economics of Internet of Things
- What is a Botnet?
- DDoS Attacks
- What Did the Mirai Botnet Do in October 2016?
- How Did Mirai Work?
- How Can an Organization Protect Against Mirai and Other DDoS Attacks?
- Conclusion
- Questions
- Bio

ILLINOIS INSTITUTE OF TECHNOLOGY

Introduction

- The term, "***Internet of Things***" was coined in 1999 by Kevin Ashton when he was working in the Media Center at the Massachusetts Institute of Technology.
- The Internet of Things (IoT) is an area of Information Technology that is exploding with promise and possibilities because of the rapid proliferation of inexpensive, yet powerful technologies both in hardware and in software. In fact, it has heralded a new paradigm shift in Internet-enabled computing, adding to and enhancing the present state of complex digital infrastructures.
- Still, IoT rapid adoption has also revealed its weaknesses in the areas of security, lack of privacy, and manageability.
- The Mirai Botnet Attack of October 2016 used known security weaknesses in tens of thousands of Internet of Things (IoT) Devices to launch massive Distributed Denial of Services Attacks against DYN, which is a major DNS Service provider. The result was a notable performance degrades in tens of thousands of businesses who rely heavily on the Internet
- This presentation will briefly examine the implications of IoT and the Mirai Botnet attacks of 2016.

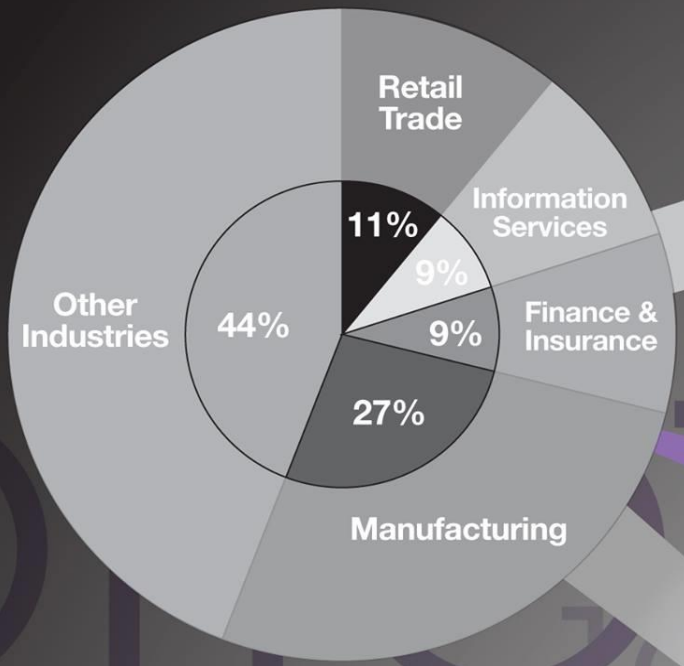
ILLINOIS INSTITUTE OF TECHNOLOGY

WHY Is This Presentation Important?

- The Internet has been business critical since 1997.
- The Internet and the World Wide Web, and the applications, data, resources they represent are considered by many to be ***critical infrastructure***.
- The ***Internet of Things*** that plays a major role in this saga, continues to grow exponentially in popularity and in capability.
- Outages (any) can cost ***money***, ***lost customers***, and even ***brand damage***.
- Everyone who uses the Internet in a business capacity should be aware of the DDoS Threat that the ***Mirai Botnet*** and similar programs represent.

Internet of Things

The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.[1]



50 BILLION

IP devices will be connected by 2022[2]

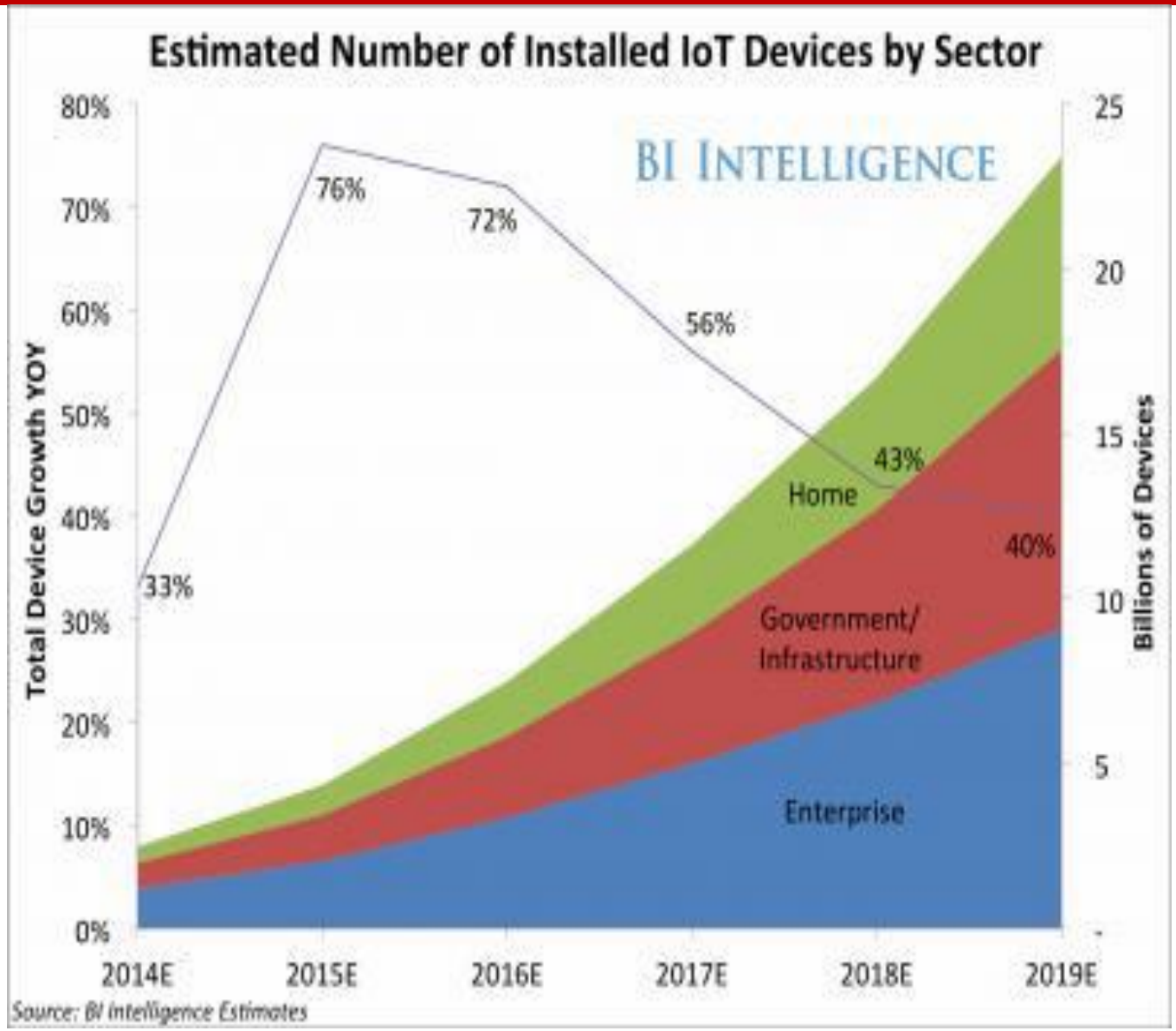
By 2016 annual global IP traffic will reach

1.3 ZETTABYTES

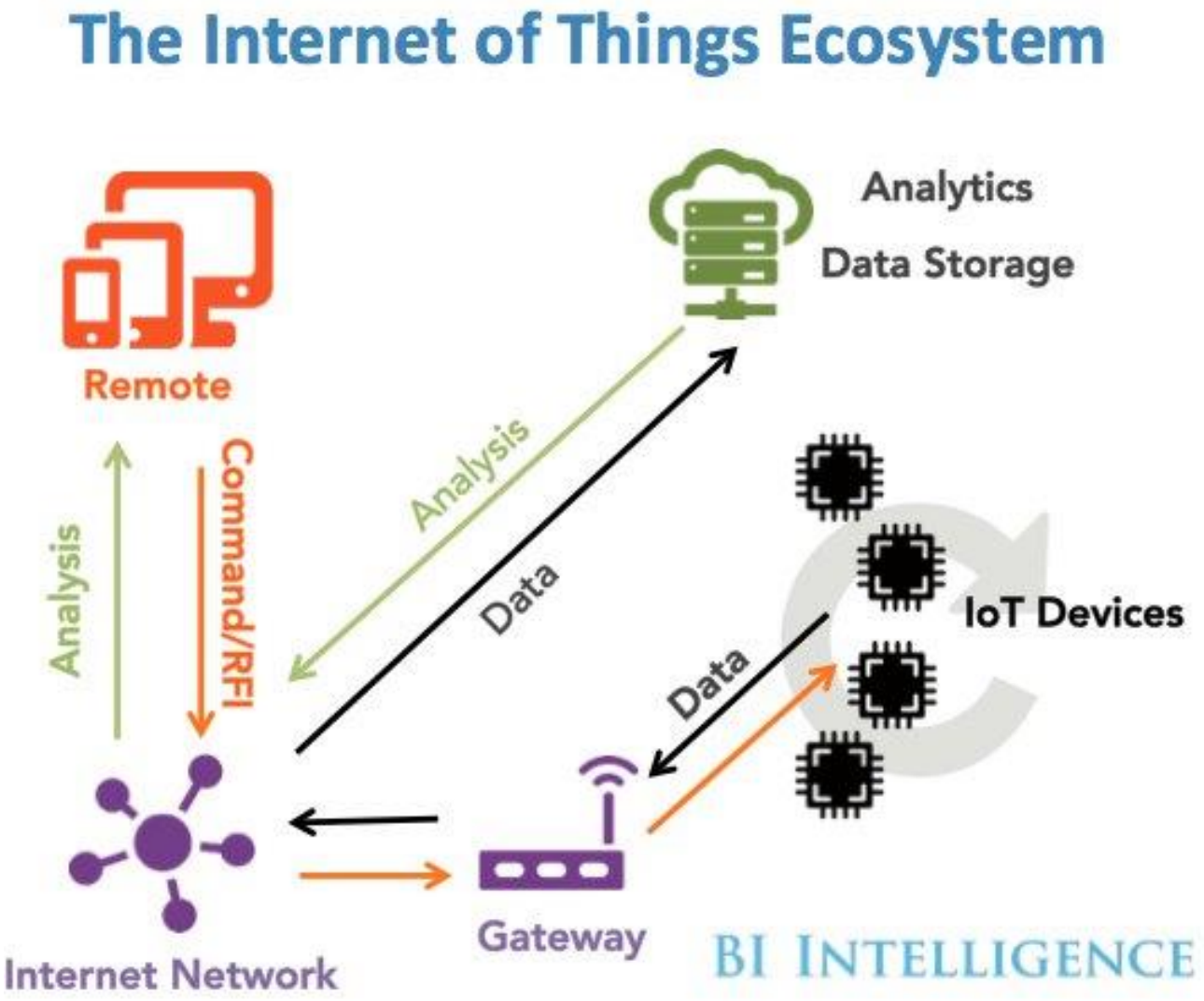
10 times more than all IP traffic generated in 2008[4]

$14.4 trillion value at stake

How Big is the "Internet of Things"?



IoT Ecosystem



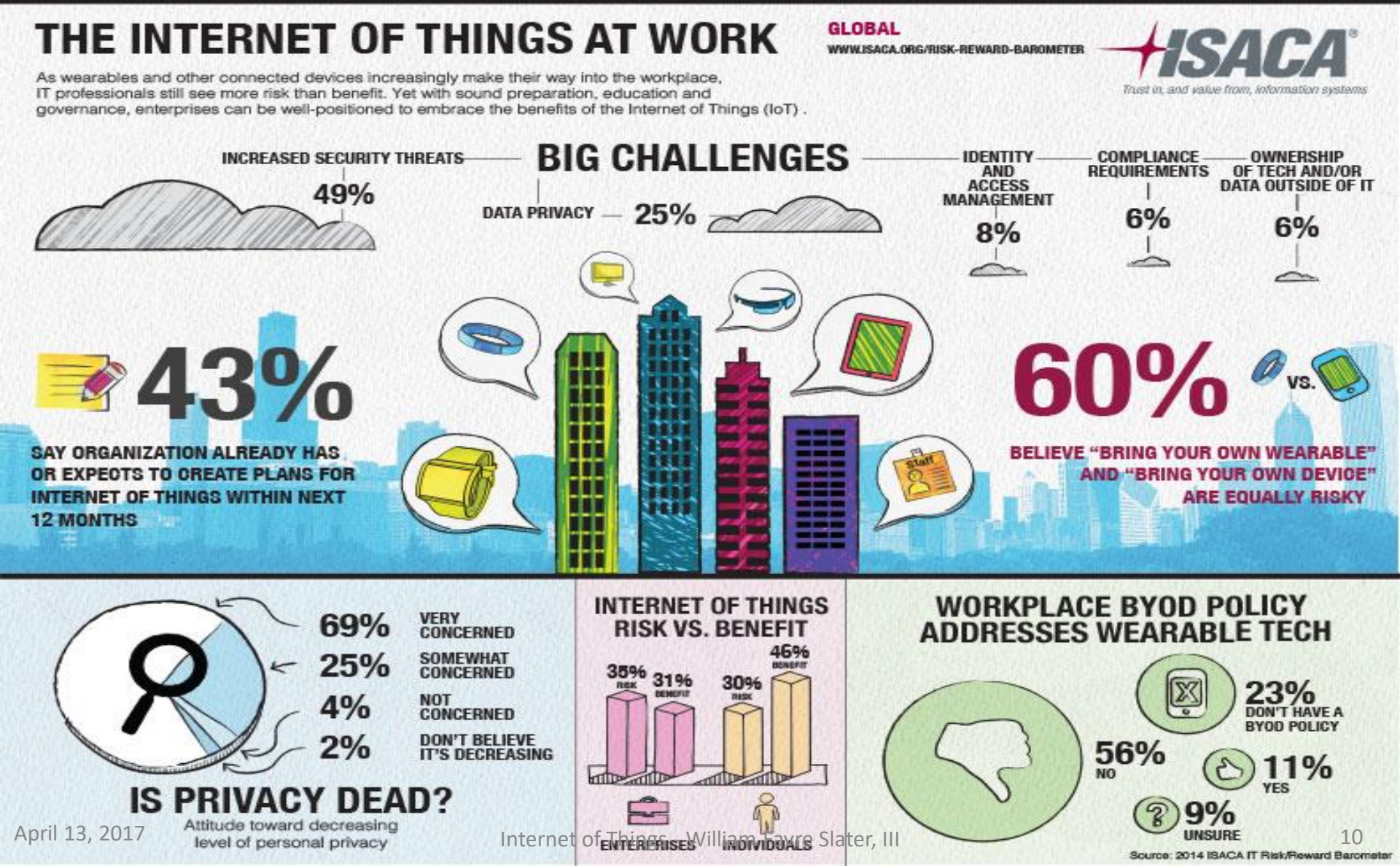
IoT Enabling Technologies

- The Internet
- The Cloud
- High bandwidth
- Web technologies
- Switching technologies
- High performance networking
- Lower cost, high-power CPUs
- Low-cost or no-cost operating systems
- Development tools
- Service Oriented Architecture
- Data Centers
- Network security
- Related management technologies

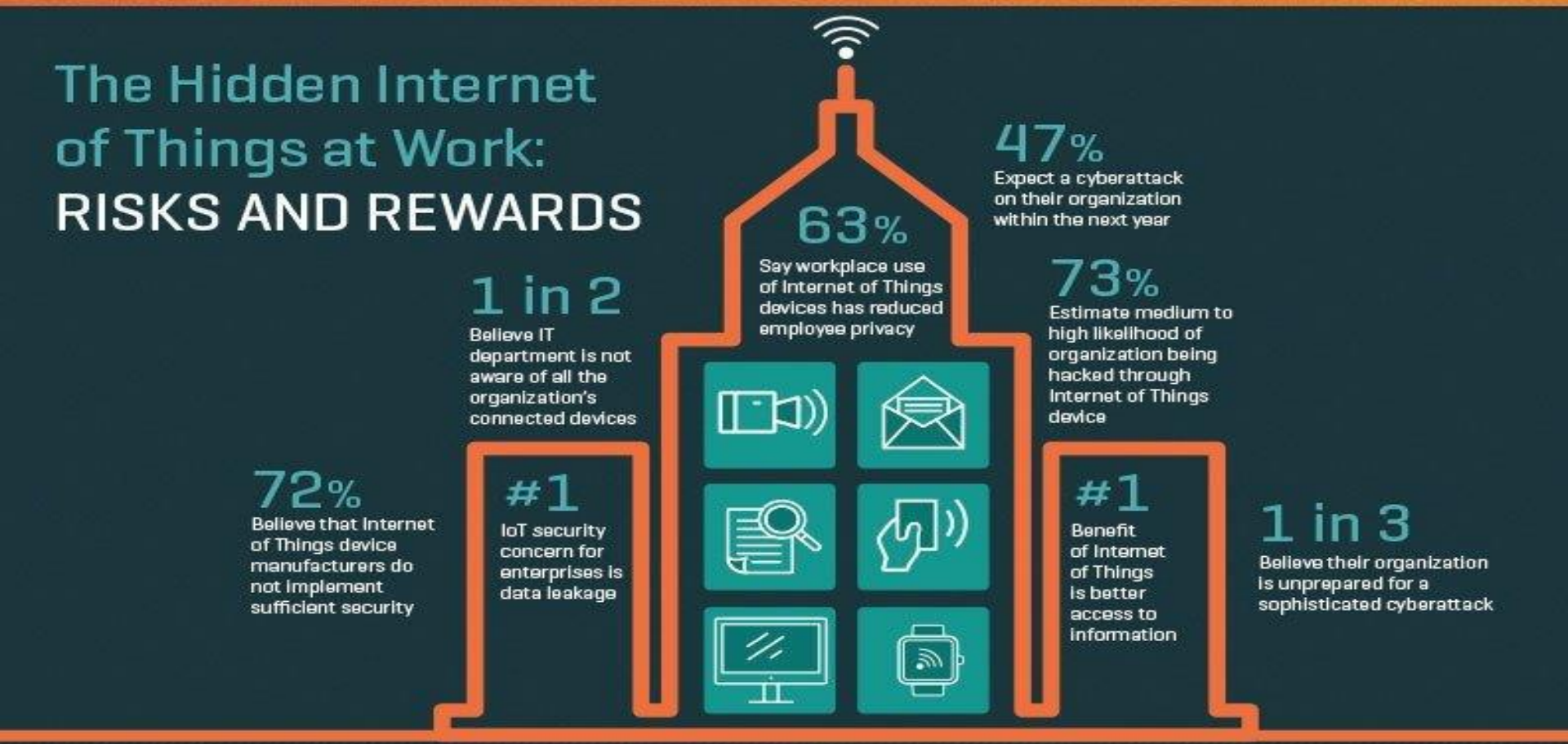
IoT Devices

- CCTV cameras
- DVRs
- Digital TVs
- Home routers
- Printers
- Alexa
- Security systems
- Garage doors
- Industrial systems
- Medical systems
- Home appliances
- Cars
- Other stuff

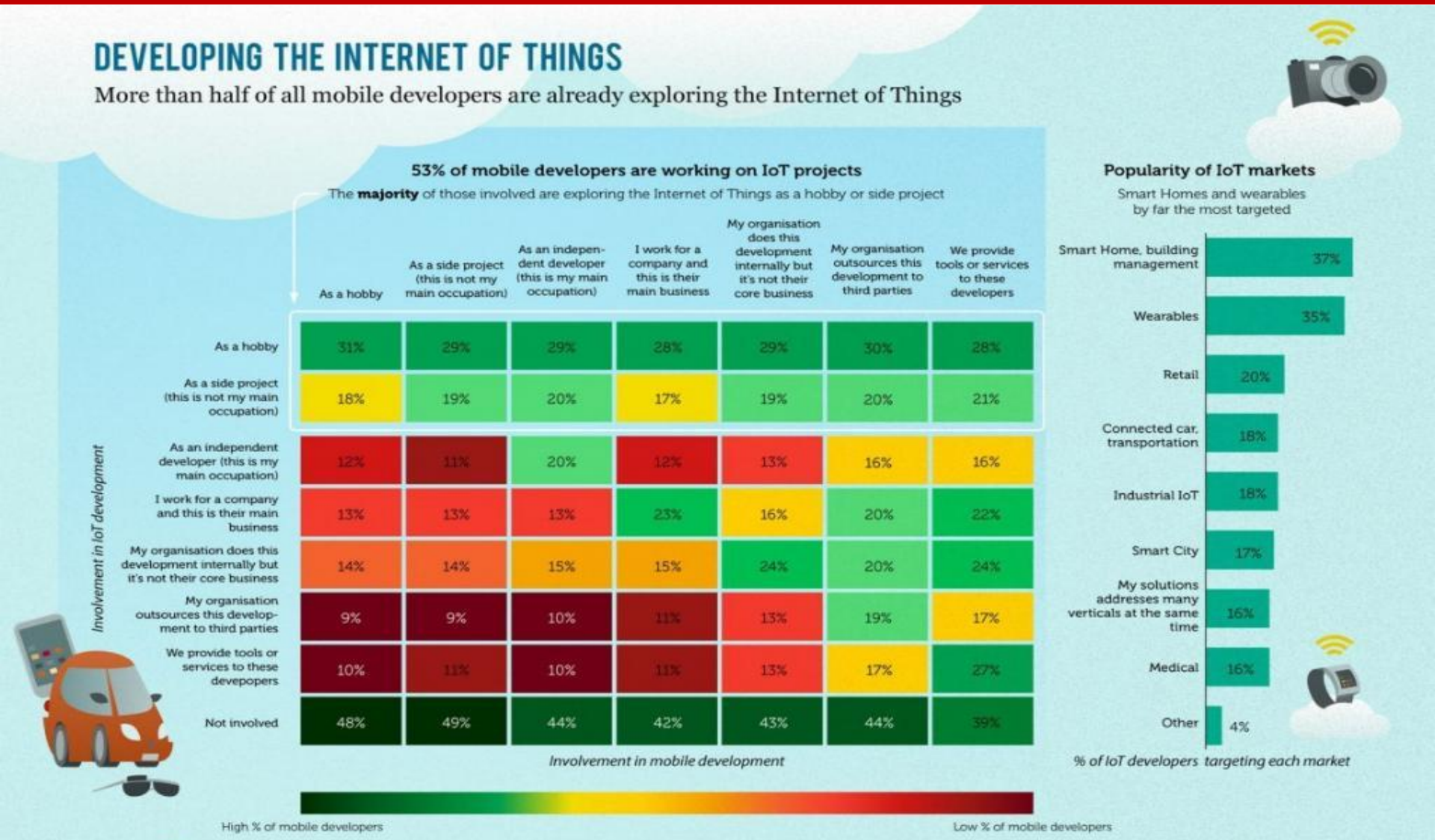
IoT at Work


THE INTERNET OF THINGS AT WORK
As wearables and other connected devices increasingly make their way into the workplace, IT professionals still see more risk than benefit. Yet with sound preparation, education and governance, enterprises can be well-positioned to embrace the benefits of the Internet of Things (IoT) .
GLOBAL
WWW.ISACA.ORG/RISK-REWARD-BAROMETER
ISACA
Trust in, and value from, information systems
BIG CHALLENGES
INCREASED SECURITY THREATS 49%
DATA PRIVACY 25%
IDENTITY AND ACCESS MANAGEMENT 8%
COMPLIANCE REQUIREMENTS 6%
OWNERSHIP OF TECH AND/OR DATA OUTSIDE OF IT 6%
43%
SAY ORGANIZATION ALREADY HAS OR EXPECTS TO CREATE PLANS FOR INTERNET OF THINGS WITHIN NEXT 12 MONTHS
60% VS.
BELIEVE "BRING YOUR OWN WEARABLE" AND "BRING YOUR OWN DEVICE" ARE EQUALLY RISKY
69% VERY CONCERNED
25% SOMEWHAT CONCERNED
4% NOT CONCERNED
2% DON'T BELIEVE IT'S DECREASING
IS PRIVACY DEAD?
Attitude toward decreasing level of personal privacy
INTERNET OF THINGS RISK VS. BENEFIT
35% RISK
31% BENEFIT
30% RISK
46% BENEFIT
ENTERPRISES
INDIVIDUALS
WORKPLACE BYOD POLICY ADDRESSES WEARABLE TECH
23% DON'T HAVE A BYOD POLICY
56% NO
11% YES
9% UNSURE
Source: 2014 ISACA IT Risk/Reward Barometer

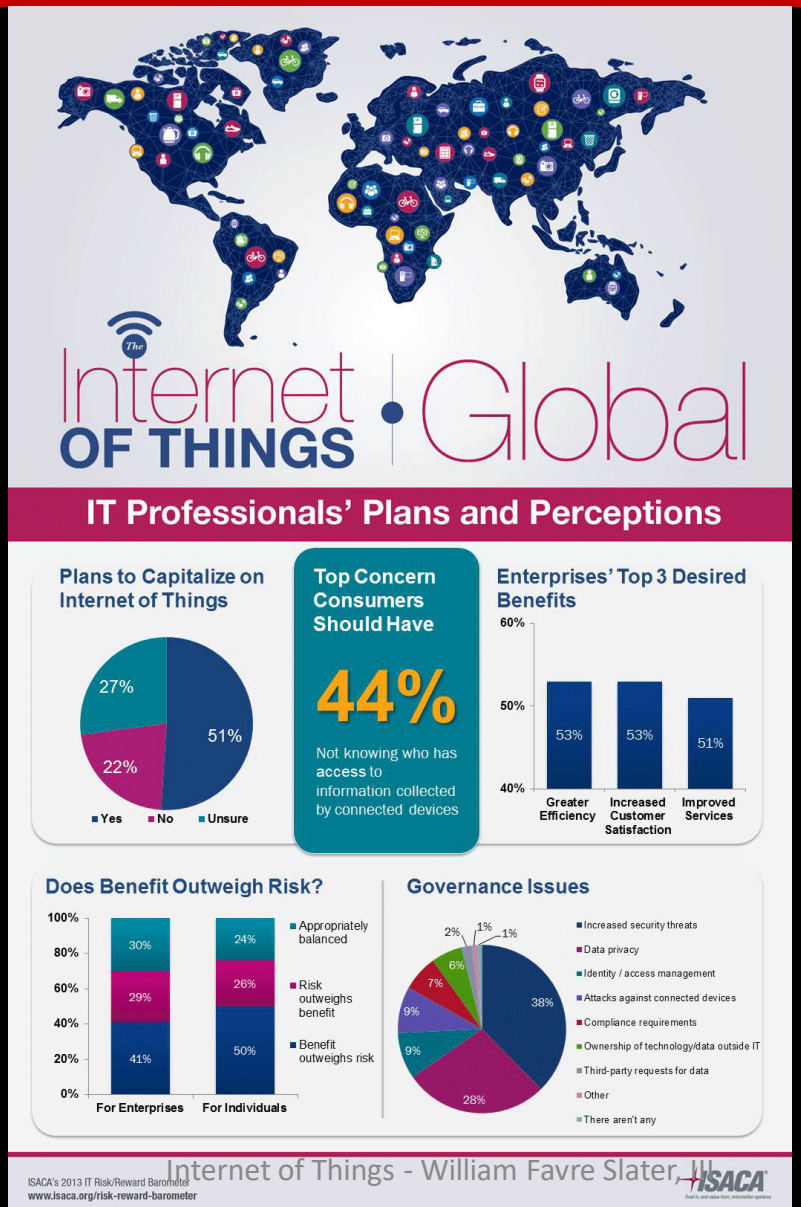
Hidden IoT at Work



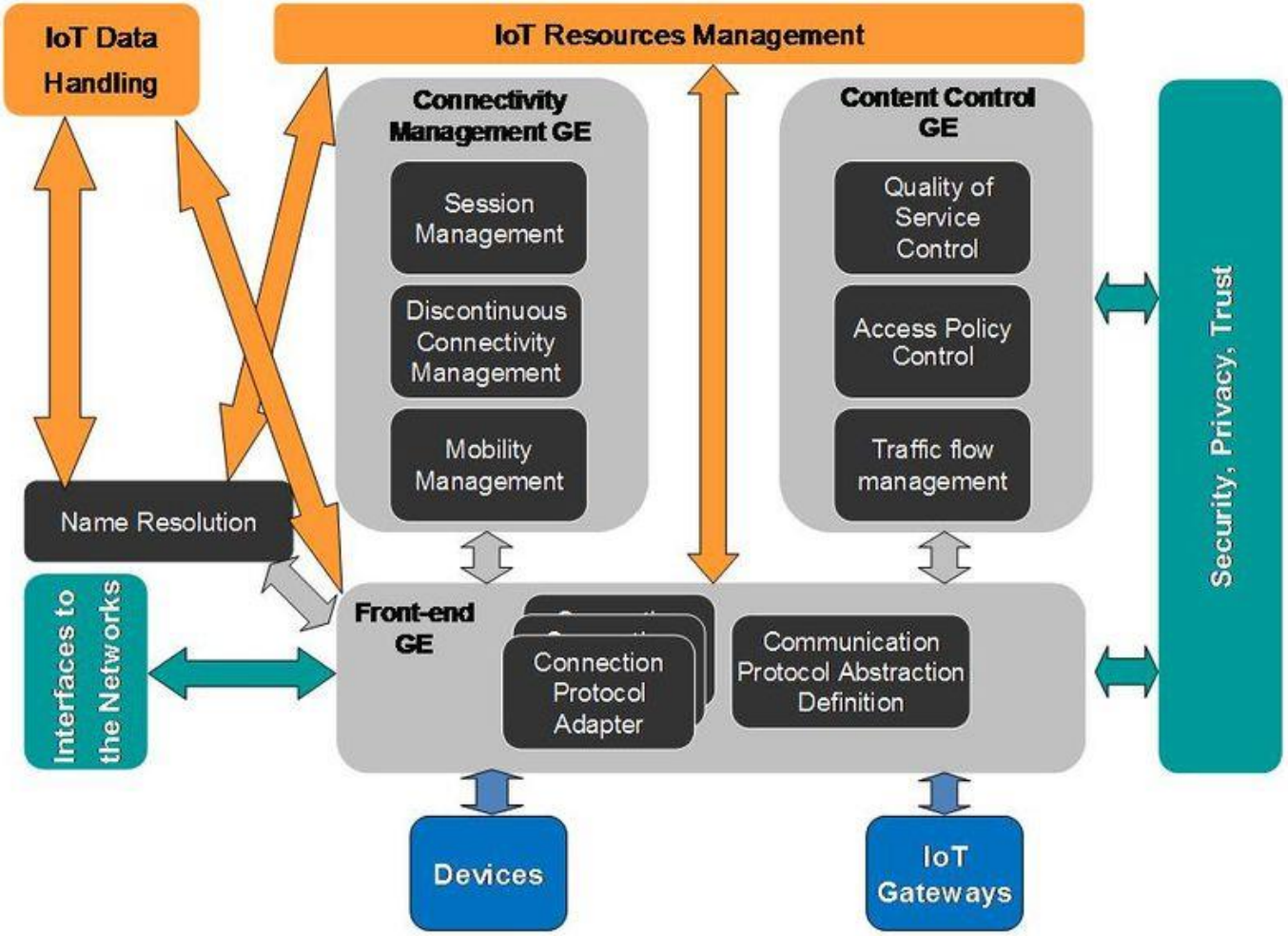
Developers and IoT



IT professionals and IoT



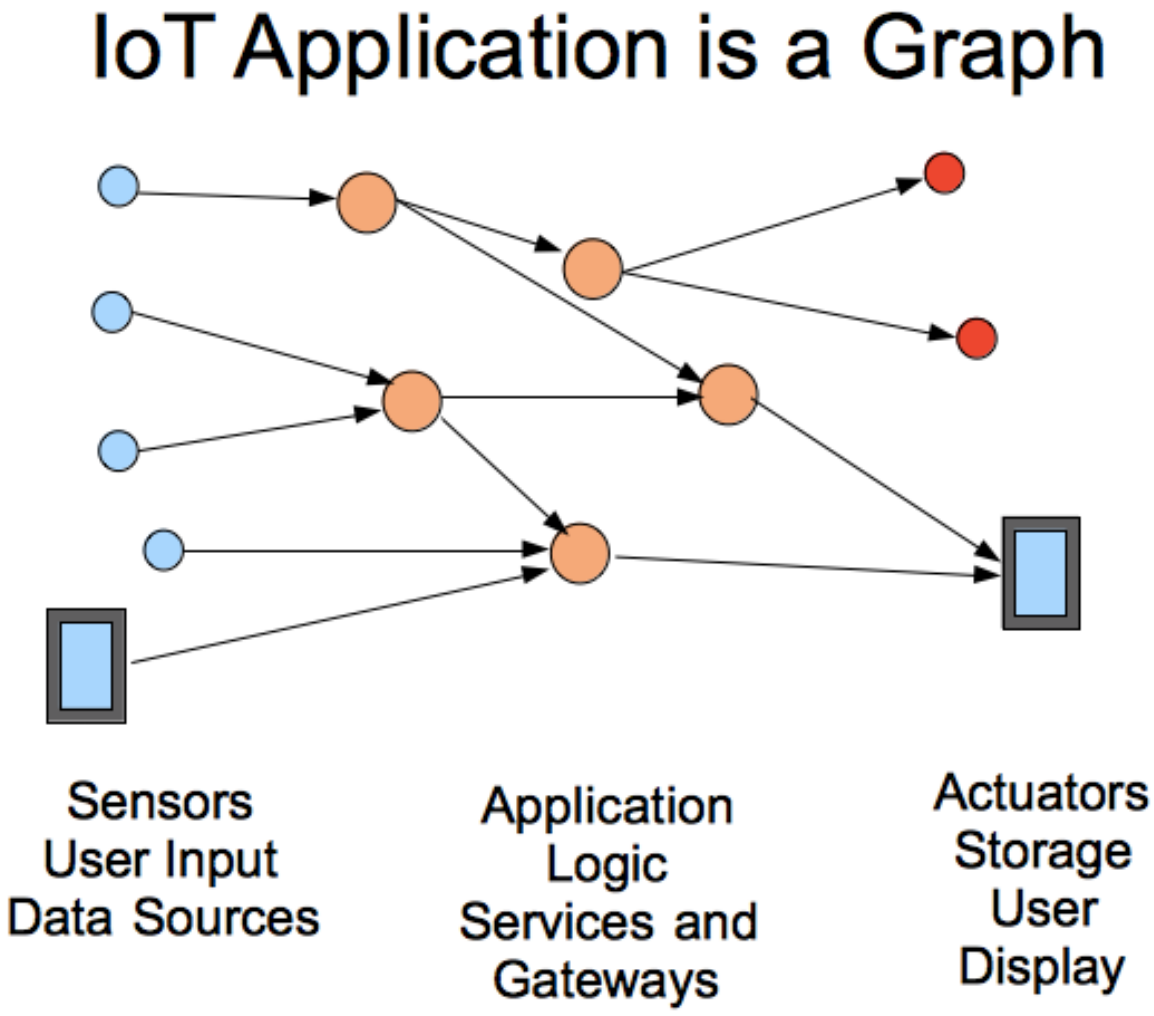
IoT Architecture Diagram



Internet of Things

ILLINOIS INSTITUTE OF TECHNOLOGY

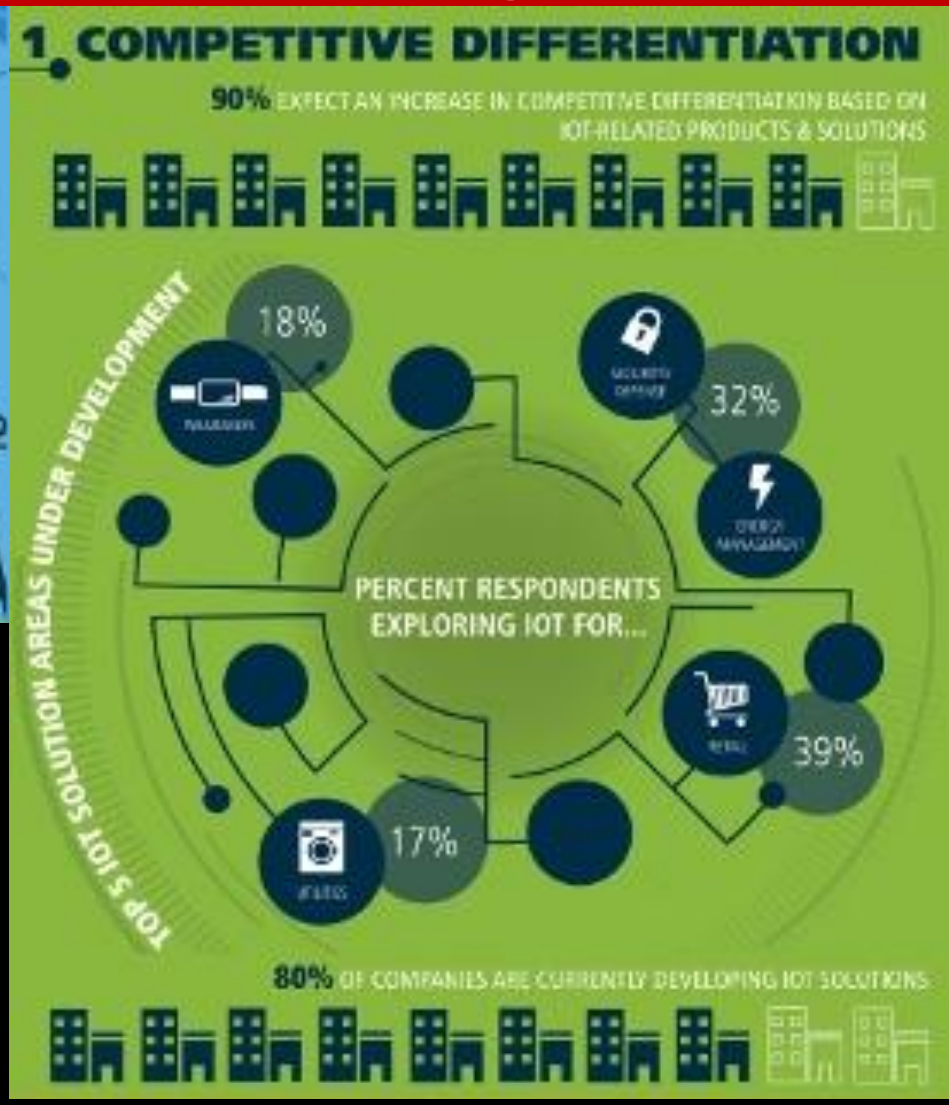
IoT Application Architecture



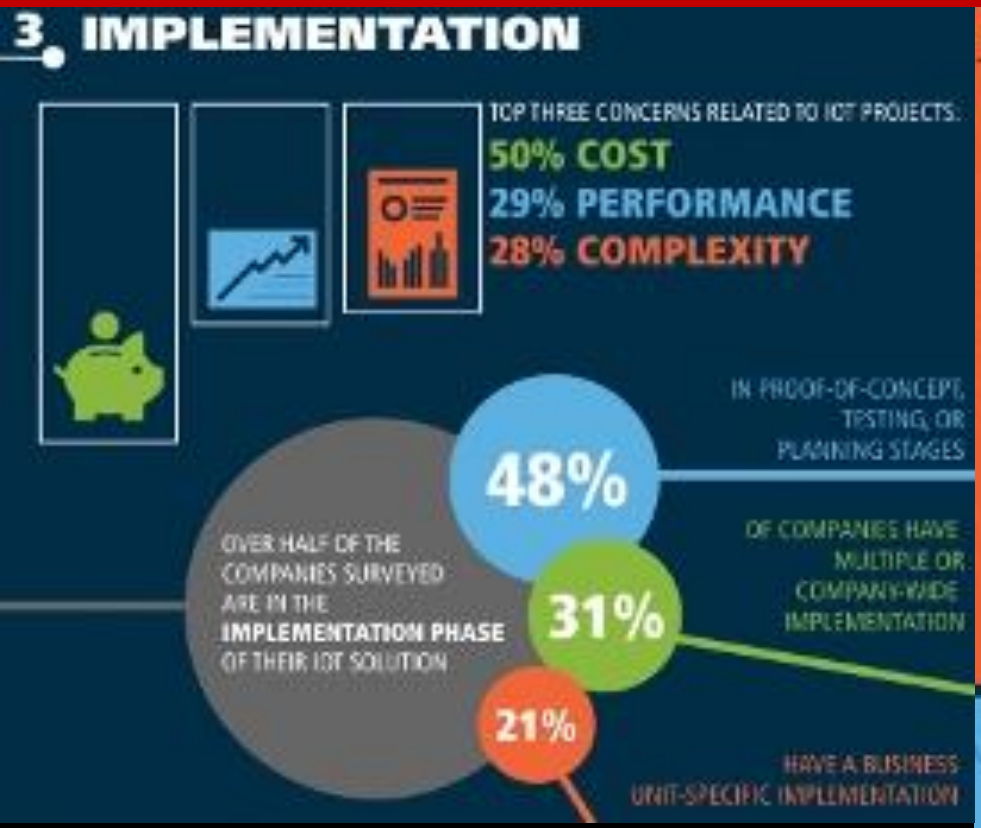
Internet of Things

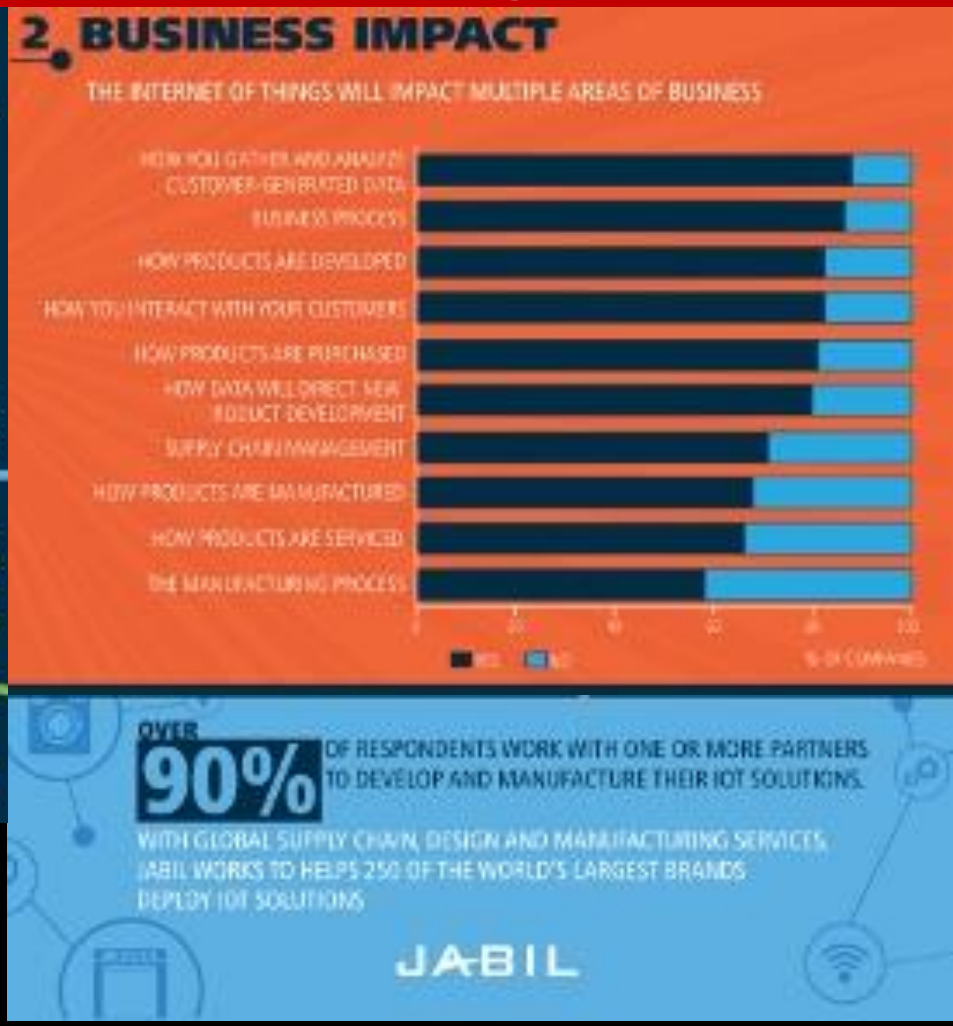
ILLINOIS INSTITUTE OF TECHNOLOGY

Business Value and the Internet of Things

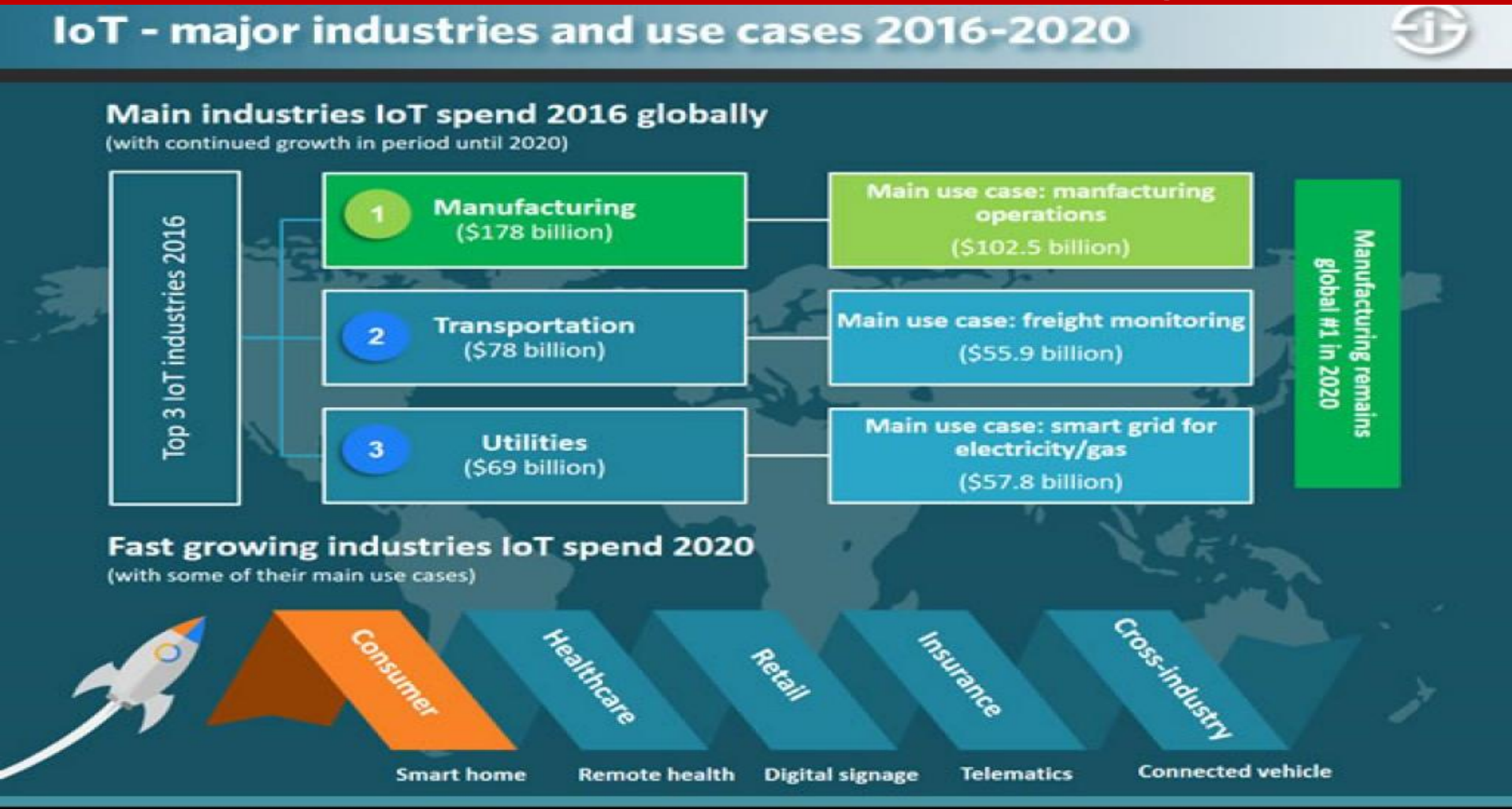


Business Value and the Internet of Things





Business Investments and the Internet of Things



Consumer Interest in the Internet of Things

- The Internet of Everything (IoE) is changing shopping behavior.

Consumer Interest in IoE-Enabled Solutions

3 Key Value Drivers

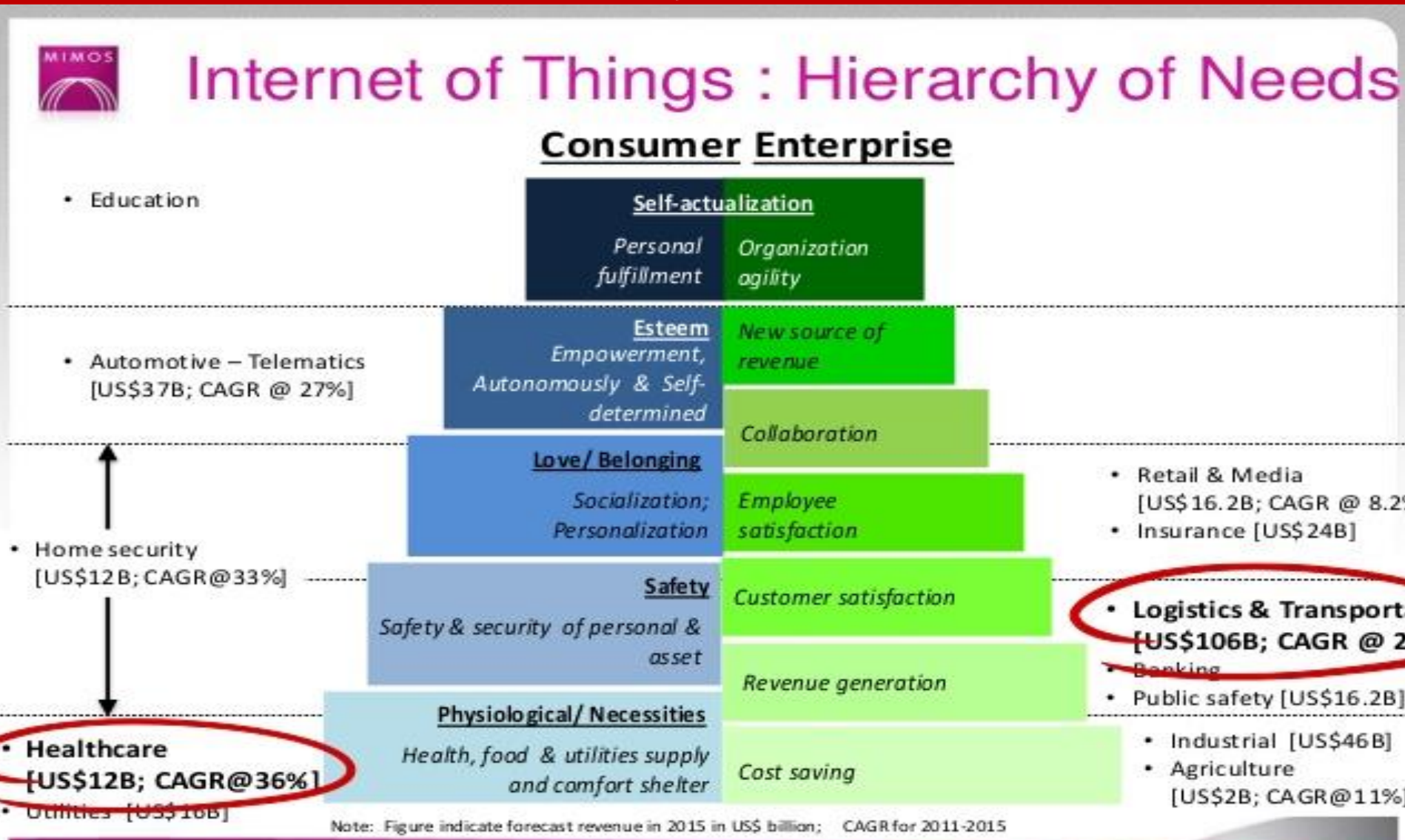
IoE-Enabled Solutions

1. general in-store offers [digital signage]
2. special offers [augmented reality]
3. targeted offers [digital signage]

4. checkout optimization
5. in-store guidance [digital signage]
6. in-store guidance [augmented reality]
7. scan-and-pay [smartphone]
8. drive-thru pickup
9. same-day delivery

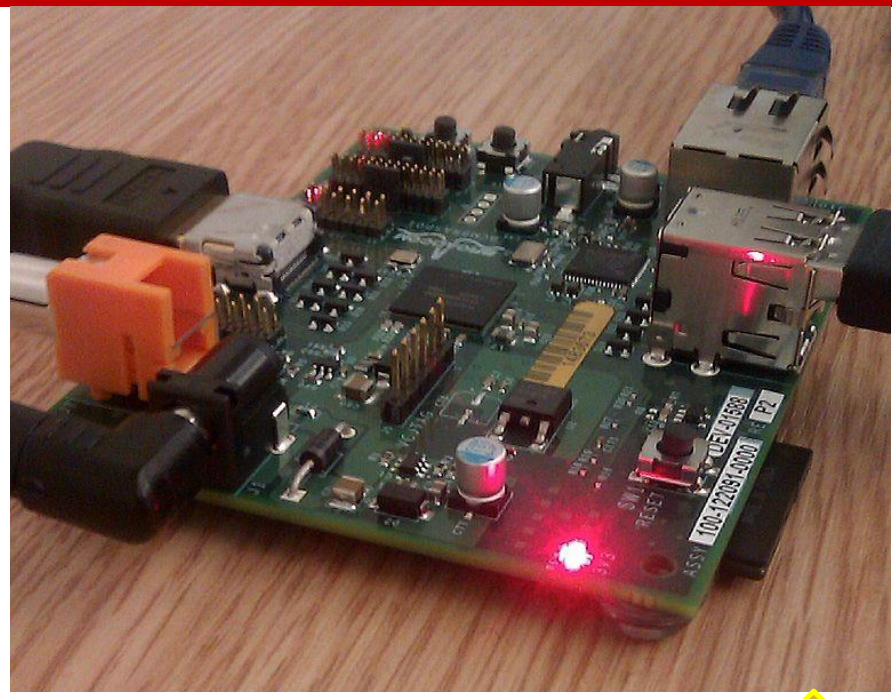
10. reviews [augmented reality]
11. in-store advertising
12. product recommender [augmented reality]

Internet of Things: Hierarchy of Needs

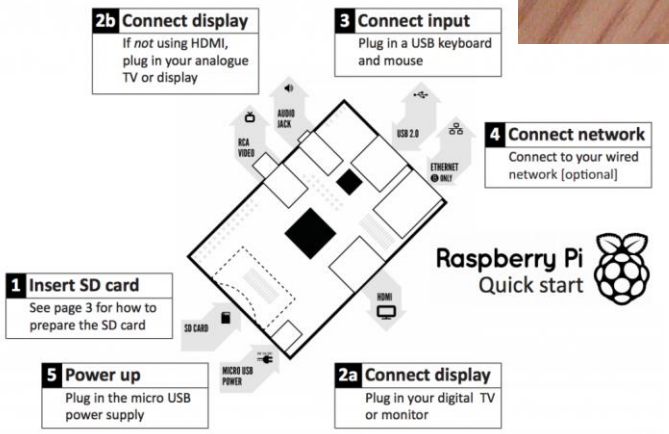


Rasberry Pi

Buy a Raspberry Pi CanaKit



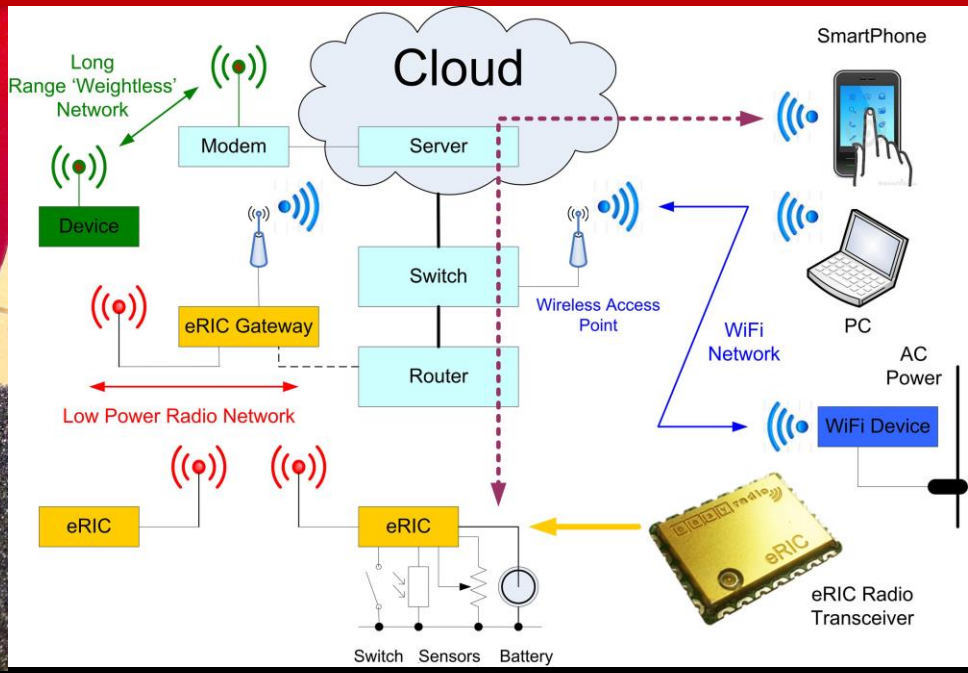
Connect



Power up and Go!

ILLINOIS INSTITUTE OF TECHNOLOGY

easyRadio Integrated Controller (eRIC)



eROS
easyRadio Operating System

Introduction to eROS (easyRadio Operating System)

eROS, the easyRadio Operating System is used within eRIC, the easy Radio Integrated Controller RF transceiver module.

eRIC's processor memory (32k) is partitioned and eROS provides a simplified and elegant means of configuring and programming a complex microcontroller and the multiple control registers of the RF transceiver. The other partition provides an optional user accessible application code area.

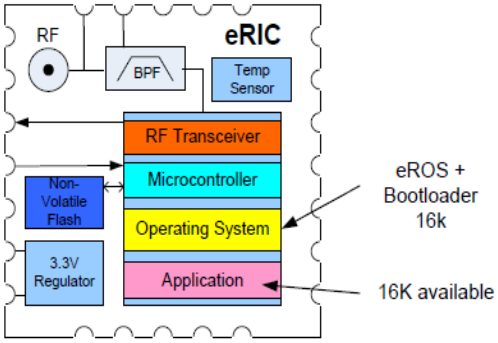


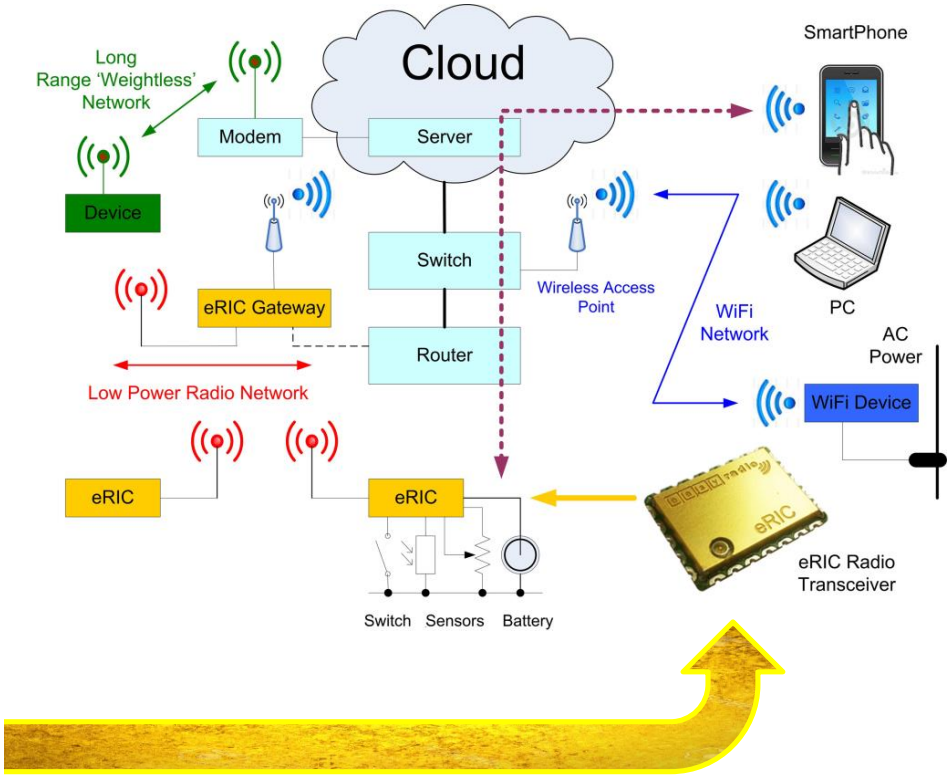
Figure 1 eRIC Transceiver Block Diagram

Radio parameters such as frequency, channel, output power and data rate are passed to the OS by the application code and radio data is sent and received by simply calling predefined functions.

The eROS API replaces low level chip specific code with intuitive pin commands that allow the multiple general purpose I/O pins and internal function blocks to be configured and interfaced to external hardware. These built in functions make customisation easy for the novice and powerful for advanced programmers.

Code is written in 'C' and currently supports the CC4305137 System-on-Chip (SoC) RF transceiver IC from Texas Instruments (TI).

This architecture eliminates the need for a separate application microcontroller and thus minimises cost and power consumption for simple 'sense and control' RF nodes such as might be employed within the 'Internet of Things'.



ILLINOIS INSTITUTE OF TECHNOLOGY

The Security Economics of Internet of Things (IoT)

Basically, it's a size vs. size game. If the attackers can cobble together a fire hose of data bigger than the defender's capability to cope with, they win. If the defenders can increase their capability in the face of attack, they win.

What was new about the Krebs attack was both the massive scale and the particular devices the attackers recruited. Instead of using traditional computers for their botnet, they used CCTV cameras, digital video recorders, home routers, and other embedded computers attached to the Internet as part of the Internet of Things.

Much has been written about how the IoT is wildly insecure. In fact, the software used to attack Krebs was simple and amateurish. What this attack demonstrates is that the economics of the IoT mean that it will remain insecure unless government steps in to fix the problem. This is a market failure that can't get fixed on its own.

Our computers and smartphones are as secure as they are because there are teams of security engineers working on the problem. Companies like Microsoft, Apple, and Google spend a lot of time testing their code before it's released, and quickly patch vulnerabilities when they're discovered. Those companies can support such teams because those companies make a huge amount of money, either directly or indirectly, from their software -- and, in part, compete on its security. This isn't true of embedded systems like digital video recorders or home routers. Those systems are sold at a much lower margin, and are often built by offshore third parties. The companies involved simply don't have the expertise to make them secure.

Even worse, most of these devices don't have any way to be patched. Even though the source code to the botnet that attacked Krebs has been made public, we can't update the affected devices. Microsoft

https://www.schneier.com/blog/archives/2016/10/security_econom_1.html 1/22

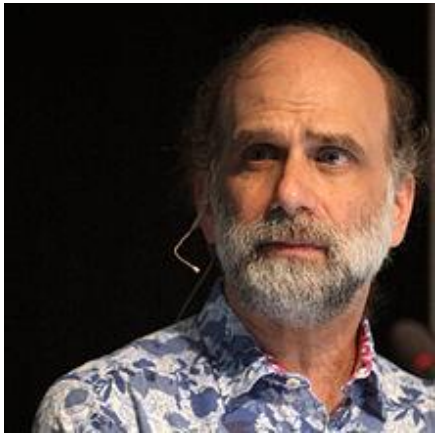
10/14/2016 Security Economics of the Internet of Things - Schneier on Security

delivers security patches to your computer once a month. Apple does it just as regularly, but not on a fixed schedule. But the only way for you to update the firmware in your home router is to throw it away and buy a new one.

The security of our computers and phones also comes from the fact that we replace them regularly. We buy new laptops every few years. We get new phones even more frequently. This isn't true for all of the embedded IoT systems. They last for years, even decades. We might buy a new DVR every five or ten years. We replace our refrigerator every 25 years. We replace our thermostat approximately never. Already the banking industry is dealing with the security problems of Windows 95 embedded in ATMs. This same problem is going to occur all over the Internet of Things.

Sources: https://www.schneier.com/blog/archives/2016/10/security_econom_1.html

Excellent Commentary about IoT, Economics, and Security by internationally known Security Writer and Researcher, Dr. Bruce Schneier

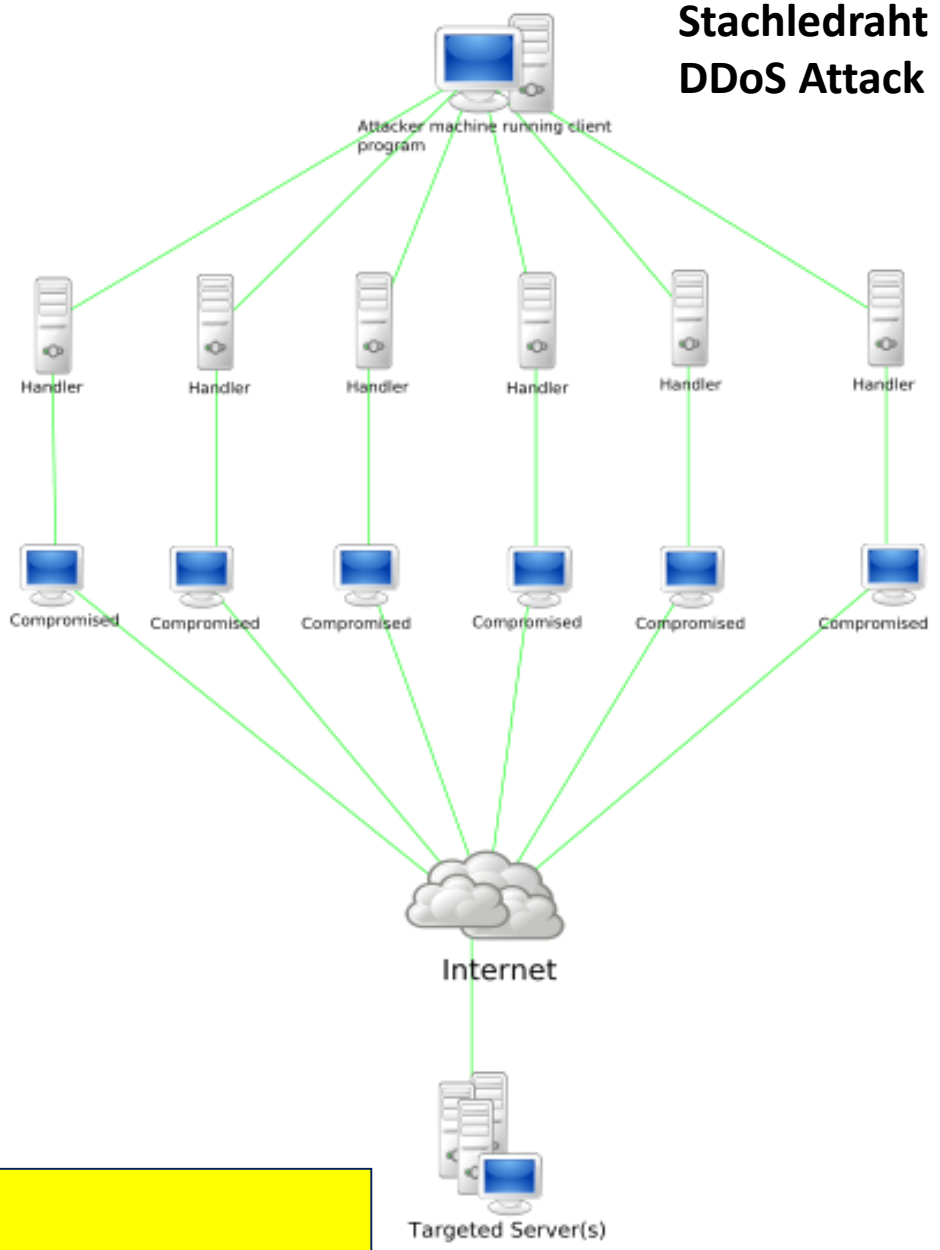


Bruce Schneier

ILLINOIS INSTITUTE OF TECHNOLOGY

What is a Botnet?

- A ***botnet*** is a number of Internet-connected devices used by a botnet owner to perform various tasks. Botnets can be used to perform Distributed Denial Of Service Attack, steal data, send spam, allow the attacker access to the device and its connection. The owner can control the botnet using command and control (C&C) software. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.
- ***Botnets have been around since 2004.***
- Attacker machines are usually running the ***Linux operating system***.



Sources:
Wikipedia https://en.wikipedia.org/wiki/Botnet
Cheng, G. (2005) . http://www.giac.org/paper/gcih/229/analysis-ddos-tool-stacheldraht-v1666/102150

DDoS Attacks

A Denial of Service (DoS) attack is an attack that can make your website or application unavailable to end users. To achieve this, attackers use a variety of techniques that consume network or other resources, disrupting access for legitimate end users. In its simplest form, a DoS attack against a target is executed by a lone attacker from a single source, as shown in Figure 1.

Figure 1: Diagram of a DOS attack

In the case of a Distributed Denial of Service (DDoS) attack, an attacker uses multiple sources—which may be compromised or controlled by a group of collaborators—to orchestrate an attack against a target. As illustrated in Figure 2, in a DDoS attack, each of the collaborators or compromised hosts participates in the attack, generating a flood of packets or requests to overwhelm the intended target.

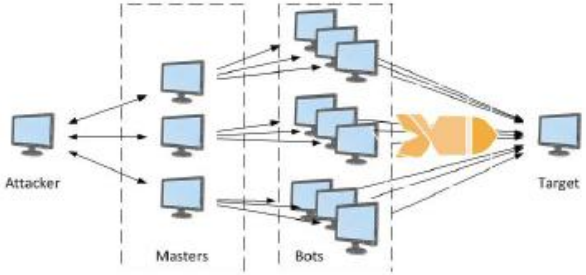
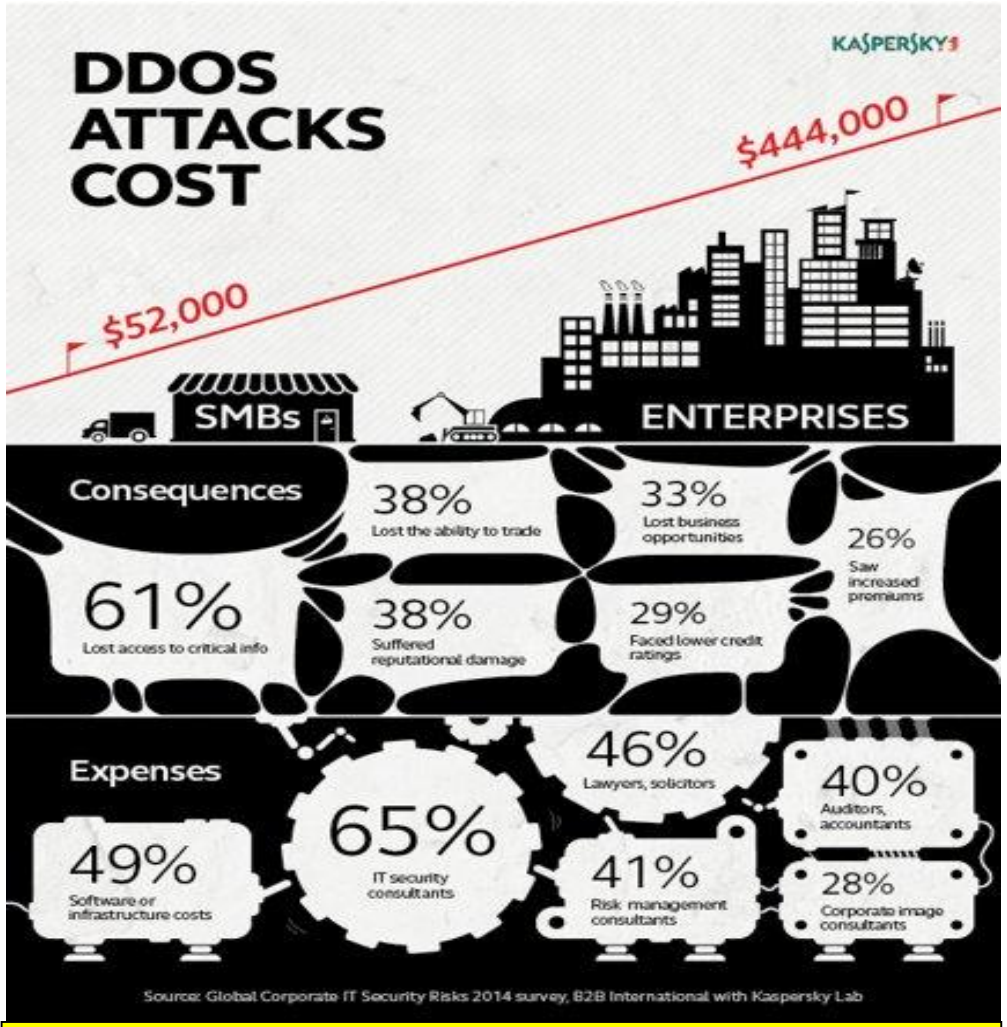


Figure 2: Diagram of a DDOS attack

Source:
AWS Best Practices for DDoS Resiliency
https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

ILLINOIS INSTITUTE OF TECHNOLOGY

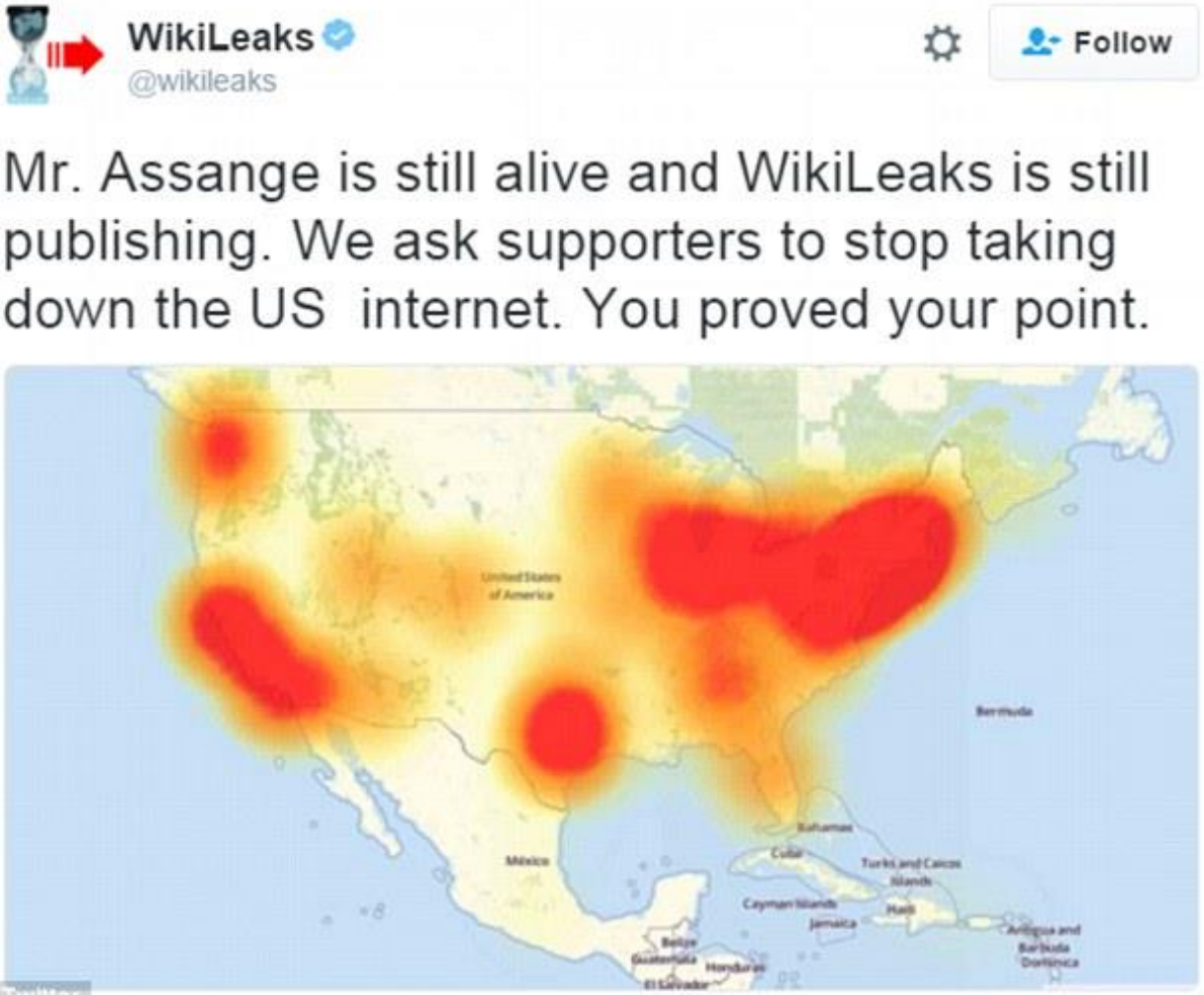
DDoS Attack Costs
Money, Time and Risk Brand Damage



Source:
Kaspersky

ILLINOIS INSTITUTE OF TECHNOLOGY

DDoS Attacks of October 21, 2016



The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

ILLINOIS INSTITUTE OF TECHNOLOGY

WHAT DID THE MIRAI BOTNET DO IN OCTOBER 2016?

ILLINOIS INSTITUTE OF TECHNOLOGY

DDoS Attacks of October 21, 2016 - The Major Internet-Related Businesses Affected

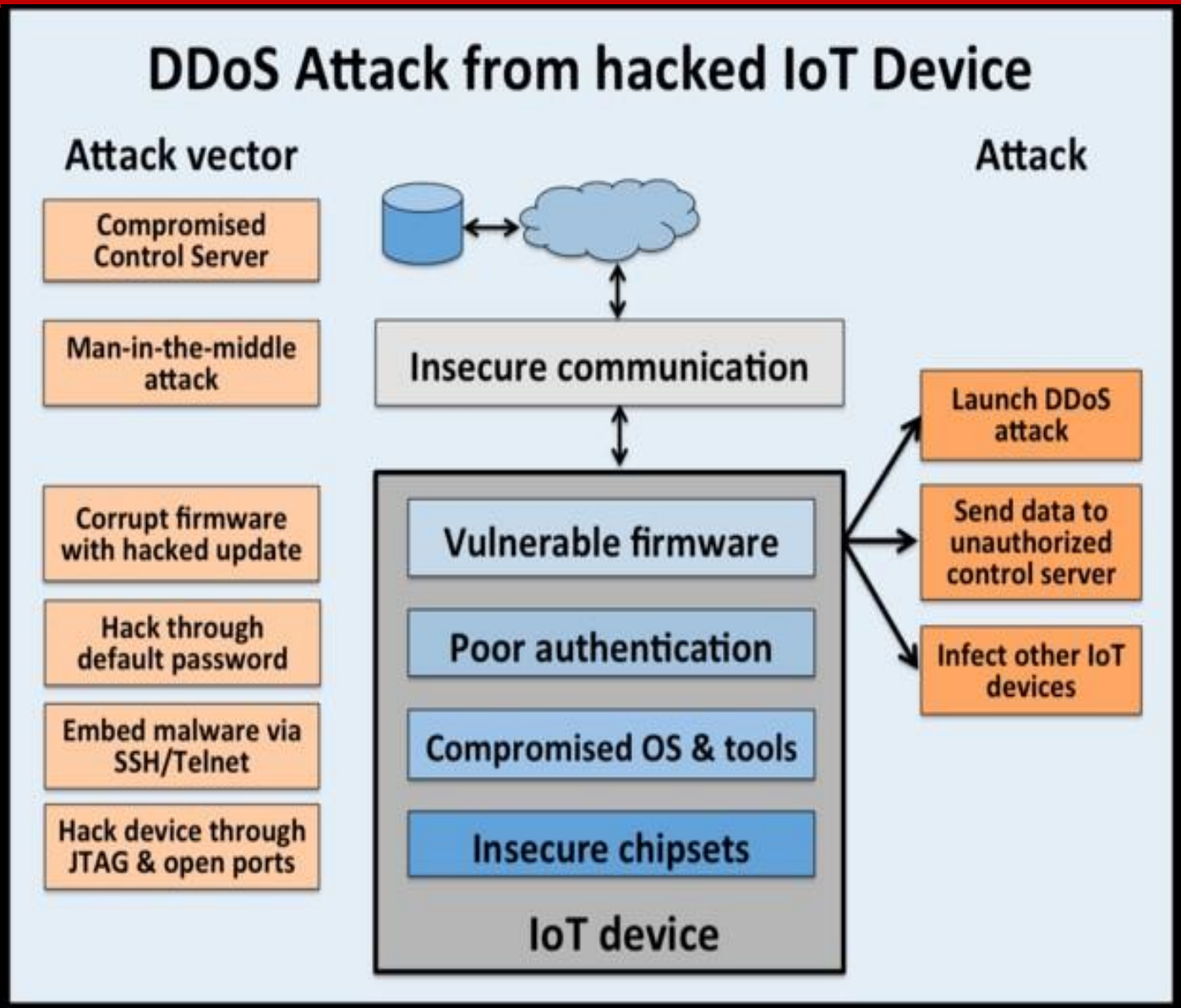
WHO WAS HIT BY THE ATTACK?

Thousands of sites were hit, including:

Twitter
Reddit
Spotify
Esty
Box
Wix Customer Sites
Squarespace Customer Sites
Zoho
CRM
Iheart.com (iHeartRadio)
Github
The Verge
Cleveland.com
hbonow.com
PayPal
Big cartel
Wired.com
People.com
Urbandictionary.com
Basecamp
ActBlue
Zendesk.com
Intercom
Twillo
Pinterest
Grubhub
Okta
Starbucks rewards/gift cards
Storify.com
CNN
Yammer
Playstation Network
Recode Business Insider
Guardian.co.uk
Weebly
Yelp

ILLINOIS INSTITUTE OF TECHNOLOGY

How Did Mirai Work?
DDoS Attacks of October 21, 2016

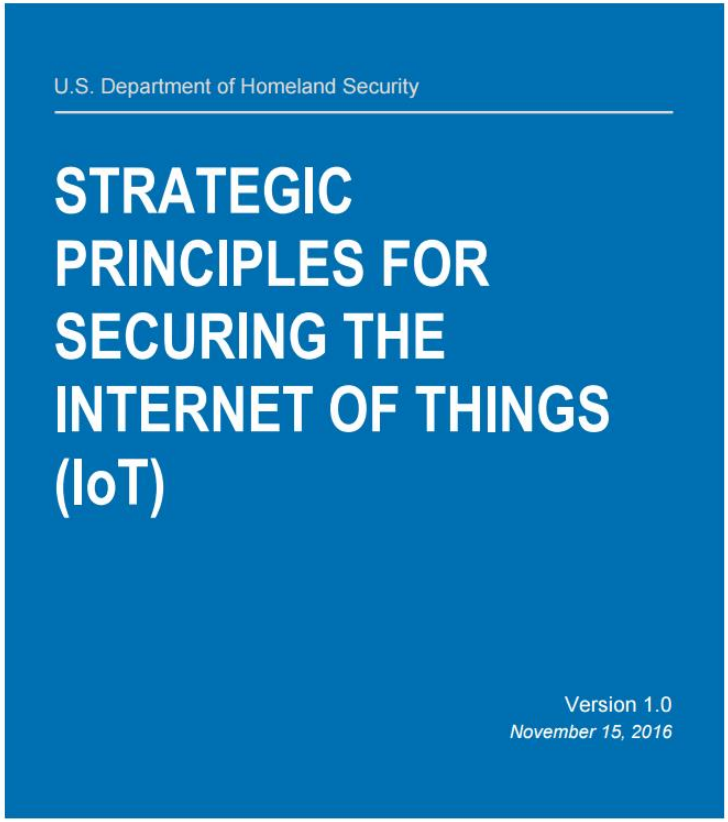


How Can an Organization Protect Against Mirai and Other DDoS Attacks?

- Take this seriously
- Read up on the ***DHS Strategic Principles for Securing IoT***
- Actively design, engineer, and implement security, from the beginning, not after the fact
- Set or Change the default passwords on IoT devices
- **Have an alternate DNS provider**
- Add DDoS attack scenarios into your Incident Management and Response Plans
- Use DDoS scenarios in your Disaster Recovery / Business Continuity Exercises
- Simulate DDoS attacks on your digital infrastructure to stress-test, evaluate, and continually improve your digital infrastructure

ILLINOIS INSTITUTE OF TECHNOLOGY

Read: DHS Strategic Principles for Securing Internet of Things



Published about 25 days AFTER the Mirai Botnet attack…

Source: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Homeland Security

ILLINOIS INSTITUTE OF TECHNOLOGY

Read: DHS Strategic Principles for Securing Internet of Things

These principles are intended to equip stakeholders with tools to comprehensively account for security as they develop, manufacture, implement, or use network-connected devices. Specifically, these principles are designed for: IoT Developers, Manufacturers, Service Providers, and industrial and business-level consumers.

Incorporate Security at the Design Phase: Security should be evaluated as an integral component of any network-connected device. While there are notable exceptions, economic drivers motivate businesses to push devices to market with little regard for security.

Promote Security Updates and Vulnerability Management: Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies.

Build on Recognized Security Practices: Many tested practices used in traditional IT and network security can be used as a starting point for IoT security. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.

Prioritize Security Measures According to Potential Impact: Risk models differ substantially across the IoT ecosystem, as do the consequences of security failures. Focusing on the potential consequences of disruption, breach, or malicious activity is critical for determining where in the IoT ecosystem particular security efforts should be directed.

Promote Transparency across IoT: Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Increased awareness can help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies.

Connect Carefully and Deliberately: IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption.

Published about 25 days AFTER the Mirai Botnet attack…

Source: DHS IoT Factsheet
https://www.dhs.gov/sites/default/files/publications/IOT%20fact%20sheet_11162016.pdf

ILLINOIS INSTITUTE OF TECHNOLOGY

Staying Secure in the World of Internet of Things

The Mirai Botnet Five Takeaways

1. Not just one attack
2. The attack was sophisticated
3. IoT is to blame
4. This isn't the end
5. The IoT industry needs stricter standards

Source:
http://www.techrepublic.com/article/dyn-ddos-attack-5-takeaways-on-what-we-know-and-why-it-matters/

ILLINOIS INSTITUTE OF TECHNOLOGY

Conclusion

- The Internet of Things (IoT) represents one of the greatest opportunities as well as the greatest challenges in modern computing.
- IoT devices are becoming ubiquitous and are in everything from CCTVs, to medical devices, to everyday home appliances and even cars.
- The Mirai Botnet made history because of its size, power, bandwidth consumption, and impact the Internet-based businesses and people connected to the Internet.
- Because the Mirai has been shared as Open Source and has been openly shared on the web, it is being studied and is evolving.
- The rapid evolution and spread of IoT Devices provides Mirai and its variants an ever-expanding target-rich environment
- The more people and organizations pay attention to the Mirai Botnet code and how to survive DDoS attacks, the better off we will be as an Internet-connected Society.
- Remember that ***CIA (Confidentiality, Integrity, and Availability)*** are the simplest principles of Security, and that Mirai and DDoS attacks can and will reduce the ***Availability*** of your digital infrastructure.

ILLINOIS INSTITUTE OF TECHNOLOGY

Questions

Presenter Bio: William Favre Slater, III

- **Project Manager / Sr. IT Consultant at Slater Technologies, Inc. , and Adjunct Professor at the Illinois Institute of Technology -** Working on projects related to:
  - Security reviews and auditing
  - ISO 27001 Project Implementations
  - Developing Applications for Risk and Compliance
  - Subject Matter Expert for Government Proposals and Contracts related to technical services management and measurement
  - SME for preparing Risk Management and Security Exams at Western Governor's State University in UT
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Developing and presenting technical training materials for undergraduate and graduate students at the ***Illinois Institute of Technology*** in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.
  - Providing Summer Internships to IIT Students via his company, Slater Technologies, Inc.
  - Doing Internet of Things Projects

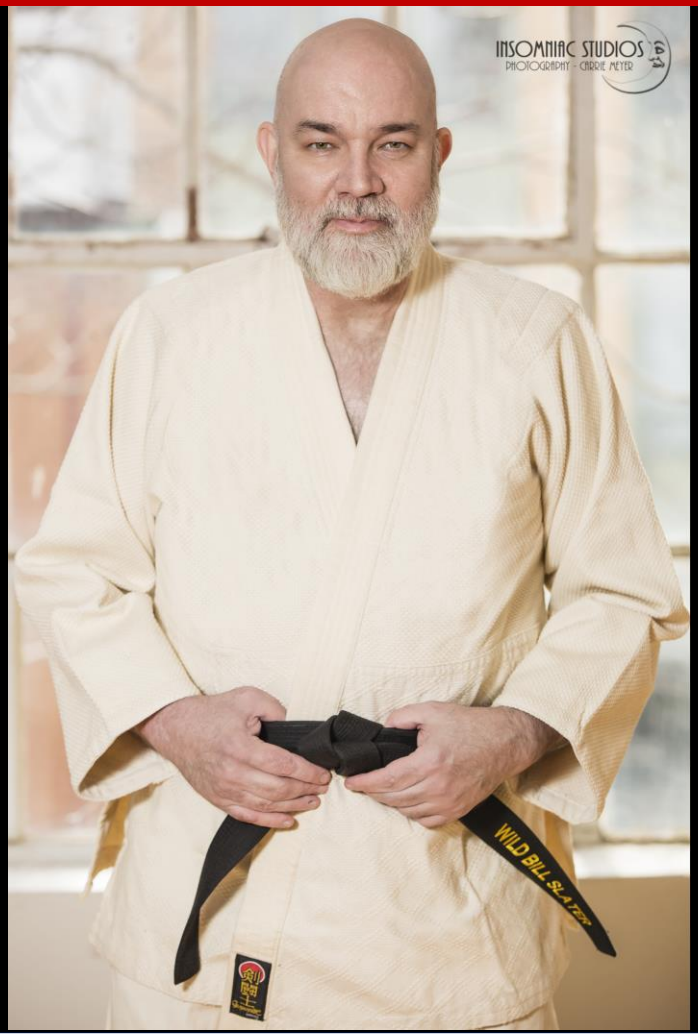
ILLINOIS INSTITUTE OF TECHNOLOGY

William Favre Slater, II

- 312-758-0307
- slater@billslater.com
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America

William Favre Slater, III

Thank You!


INSOMNIAC STUDIOS
PHOTOGRAPHY - CARRIE MEYER
WILD BILL SLATER