



Sensor Networks: Enlarging the Attack Surface

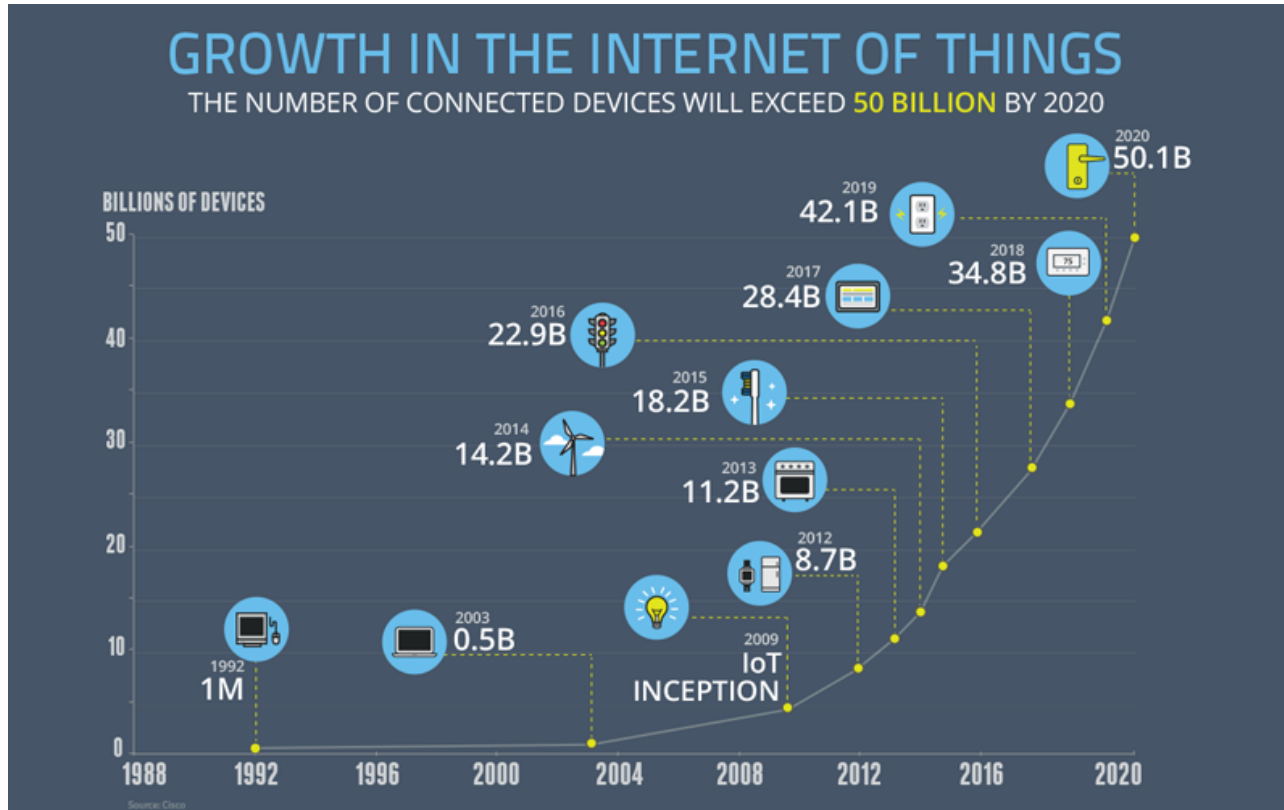
SensorNetworks Conference

Nancy Cam-Winget

Distinguished Engineer, Cisco Security Business Group

February 2017

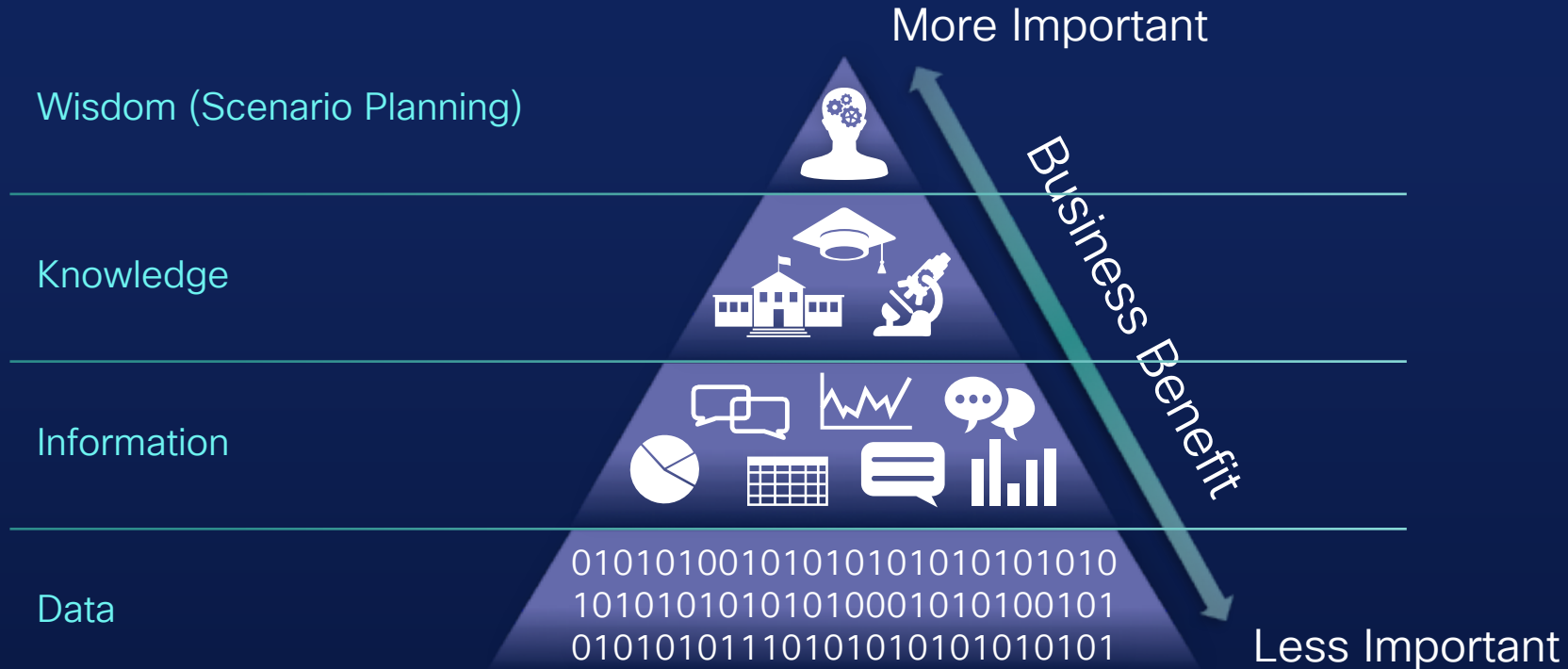
By 2020, IoT Devices will Account for 83% of All Internet Connections



... Building a Hyperconnected World: IoE

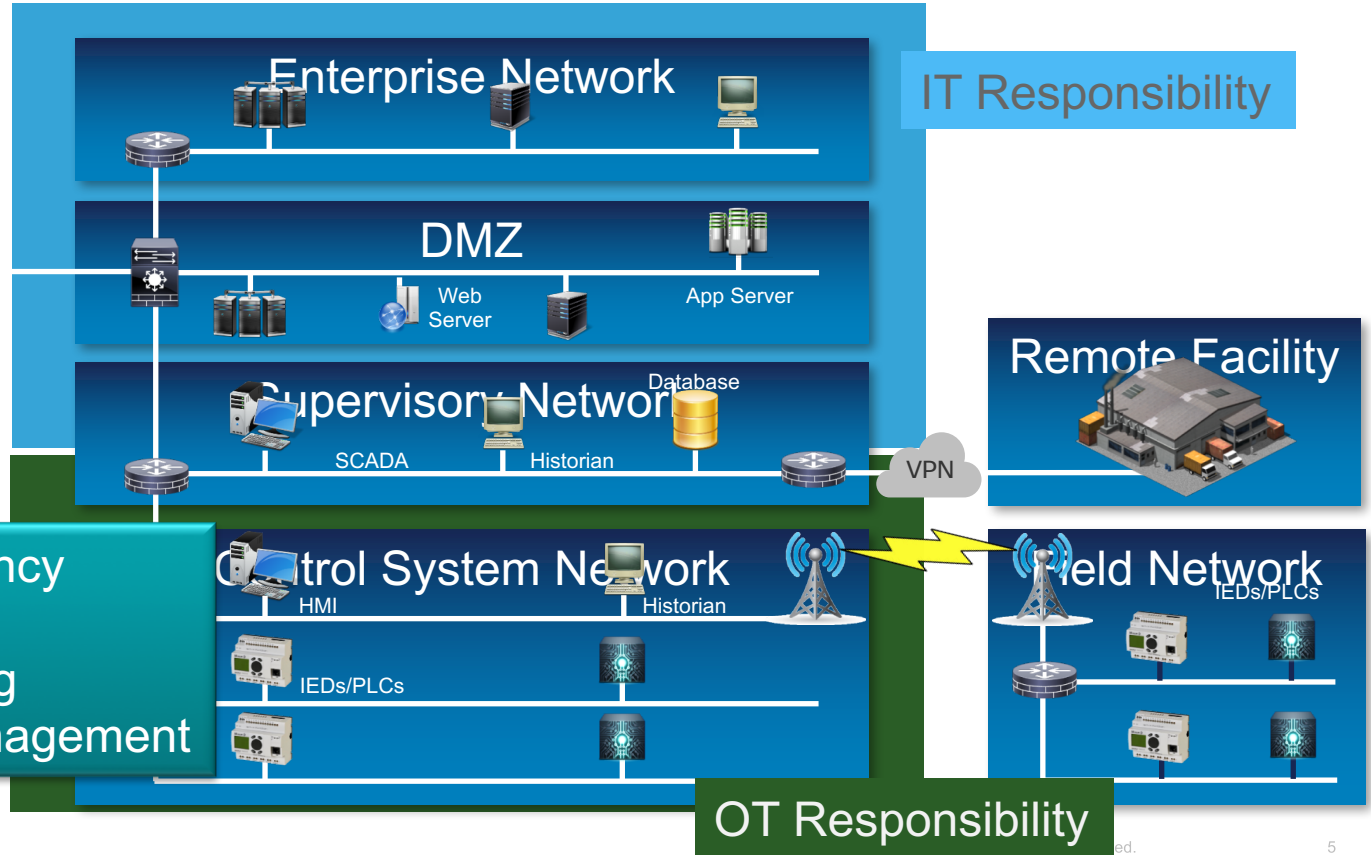
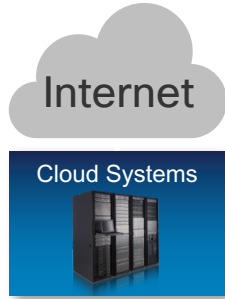


IoT can Enable Data into Wisdom



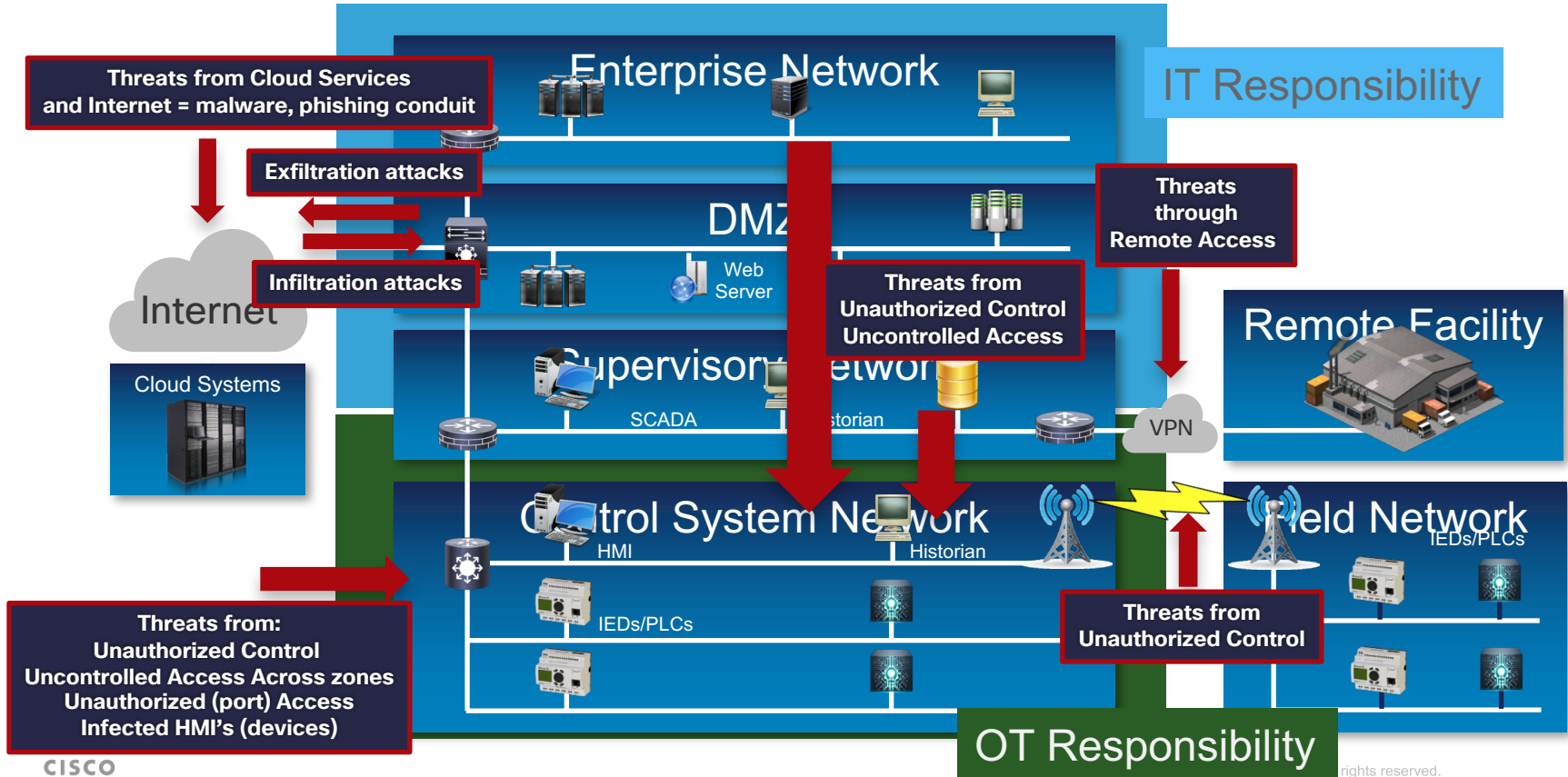
Big Data becomes Open Data for Customers, Consumers to Use

Improving Business and Operational Efficiencies





- ↑ Operations Efficiency
- ↑ Productivity
- ↑ Resource Planning
- ↑ Supply Chain Management

With a Growing Attack Surface



IoT Security Awareness



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 10, 2015

Alert Number
I-091015-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables. such as fitness devices

The Security Challenge



McAfee Labs

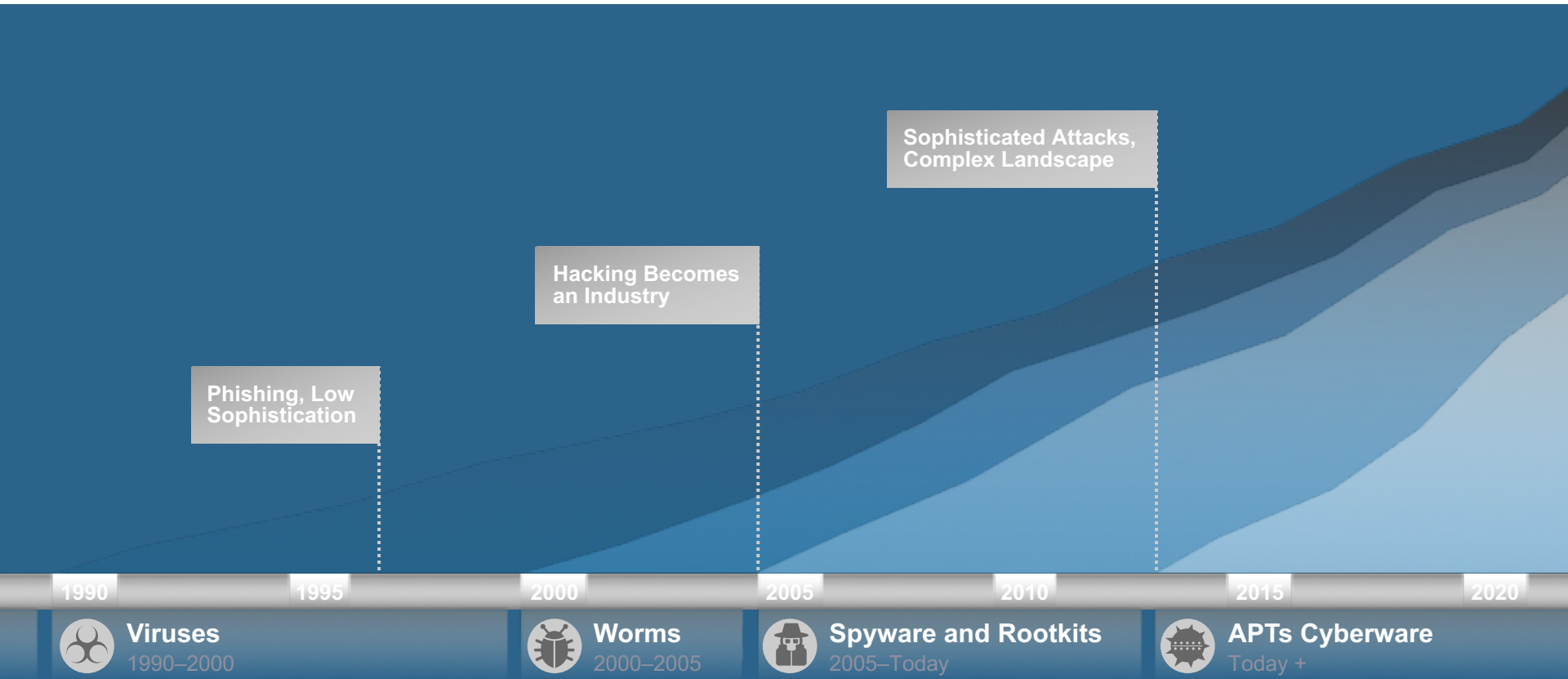
2017 Threats Predictions

November 2016

Threats and breaches

IoT devices are attractive to cybercriminals or nation-states for one or two reasons: They are a potential source of data or metadata, or a potential attack vector to cause damage.

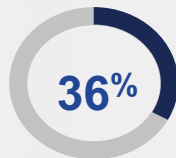
The Industrialization of Hacking



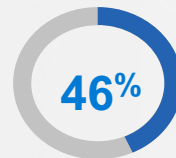
Growing number Breaches and Threats

Experienced Security Risks

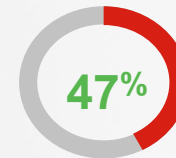
Source: Forrester – Security, The Vital Element of IoT; Q1 2015



Deployed and Expanding IoT today



Planning to Expand in Next 3 Years



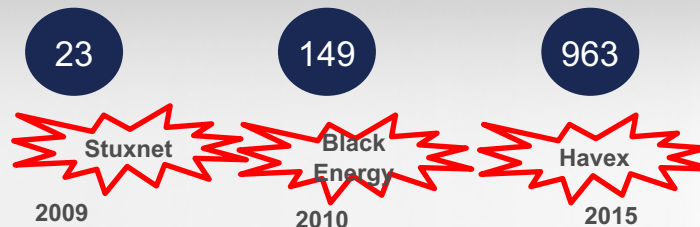
Have Experienced a Security Breach

Increasingly Hostile Threats

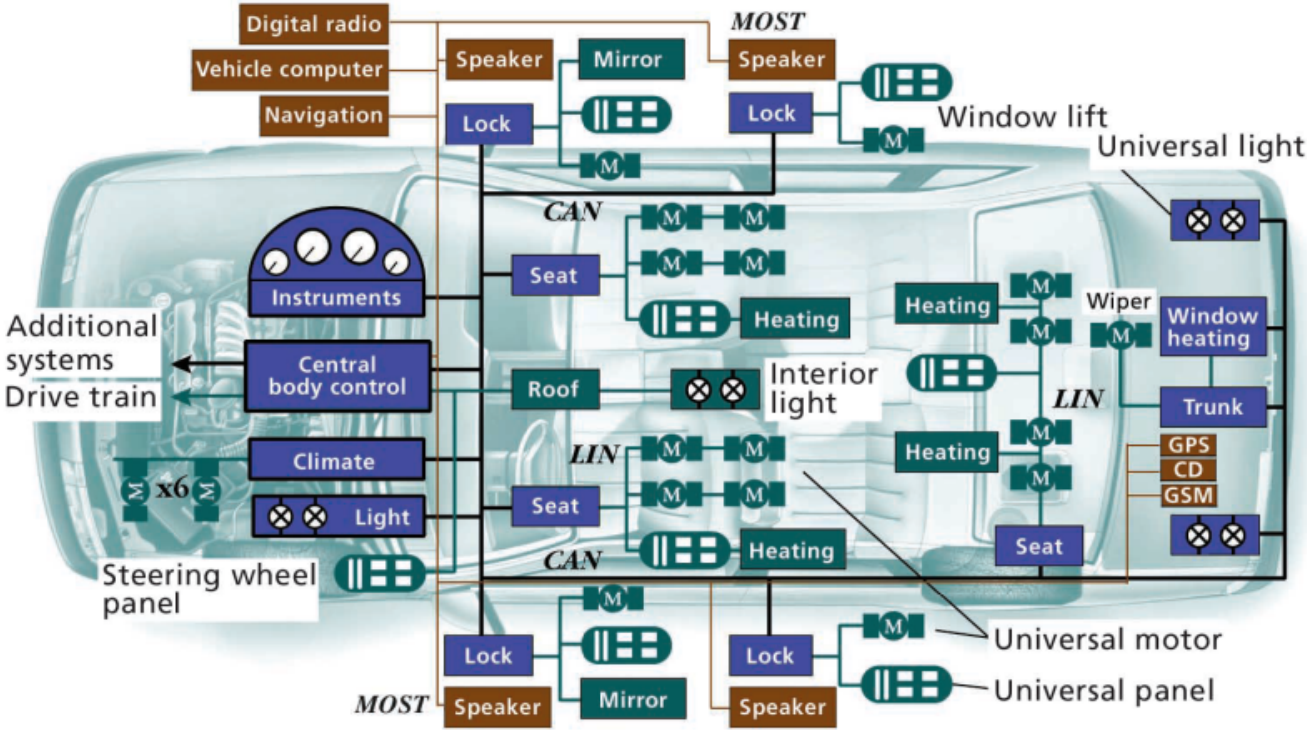
Source: Dept. of Homeland Security; ICS-CERT

Disclosed ICS Vulnerabilities*

High Profile Attacks



Case Study: Vehicle Attack Surface



- Trends:
- Increased # ECUs
 - Assisted driving
 - WiFi Hotspot
 - OTA

CAN Controller area network
 GPS Global Positioning System
 GSM Global System for Mobile Communications
 LIN Local interconnect network
 MOST Media-oriented systems transport

<http://www.intechopen.com/source/html/42787/media/image1.png>


Attacks on Vehicles



Car Hacking Guide: <http://illmatics.com/Remote%20Car%20Hacking.pdf>

Broader Scope Attacks

<https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/>



Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things

Mirai Attack Timeline¹

KrebsOnSecurity.com target of record-breaking 620Gbps DDoS attack

Source Code of IoT Botnet Mirai Released on Hackforums.net by Anna-senpai

9/21

10/21

9/20

French web hoster OVH targeted by 1Tbps DDoS attack

9/30

Dyn's managed DNS infrastructure in the US-East region under assault:

- 2 impacting waves: 7:00 AM EDT, 11:52 AM EDT (3rd wave mitigated)
- Impacting many websites and services including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix

Mirai Code disclosures

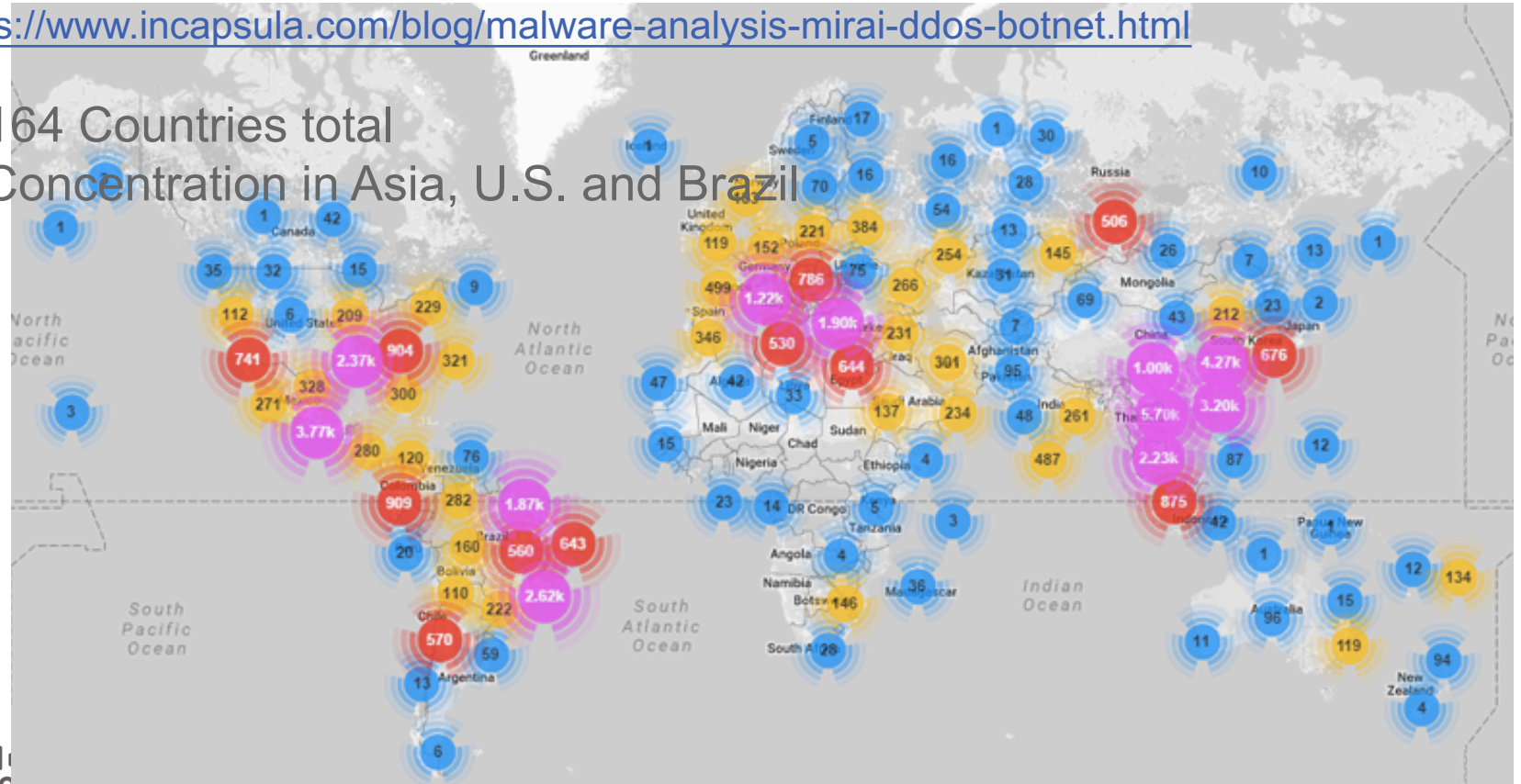
Targets (68) devices
by using default
username/password
S

| Username/Password | Manufacturer | Link to supporting evidence |
|-----------------------|--------------------------------|---|
| admin/123456 | ACTi IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/anko | ANKO Products DVR | http://www.cctvforum.com/viewtopic.php?f=3&t=44250 |
| root/pass | Axis IP Camera, et. al | http://www.cleancss.com/router-default/Axis/0543-001 |
| root/vizxv | Dahua Camera | http://www.cam-it.org/index.php?topic=5192.0 |
| root/888888 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/666666 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/7ujMko0vizxv | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| root/7ujMko0admin | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| 666666/666666 | Dahua IP Camera | http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C |
| root/dreambox | Dreambox TV receiver | https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/ |
| root/zlxx | EV ZLX Two-way Speaker? | ? |
| root/juantech | Guangzhou Juan Optical | https://news.ycombinator.com/item?id=11114012 |
| root/xc3511 | H.264 - Chinese DVR | http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15 |
| root/h3518 | HiSilicon IP Camera | https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/ |
| root/klv123 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/klv1234 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/jvbsd | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/admin | IPX-DDK Network Camera | http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/ |
| root/system | IQinVision Cameras, et. al | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/meinsm | Mobotix Network Camera | http://www.forum-use-ip.co.uk/threads/mobotix-default-password.76/ |
| root/54321 | Packet8 VOIP Phone, et. al | http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411/ |
| root/00000000 | Panasonic Printer | https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html |
| root/realtek | RealTek Routers | |
| admin/1111111 | Samsung IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/xmhdipc | Shenzhen Anran Security Camera | https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI |
| admin/smcadmin | SMC Routers | http://www.cleancss.com/router-default/SMC/ROUTER |
| root/ikwb | Toshiba Network Camera | http://faq.surveillixdvr.support.com/index.php?action=artikel&cat=4&id=8&artlang=en |
| ubnt/ubnt | Ubiquiti AirOS Router | http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm |
| supervisor/supervisor | VideoIQ | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/<none> | Vivotek IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/1111 | Xerox printers, et. al | https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/ |
| root/Zte521 | ZTE Router | http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html |

Success of Global Scope

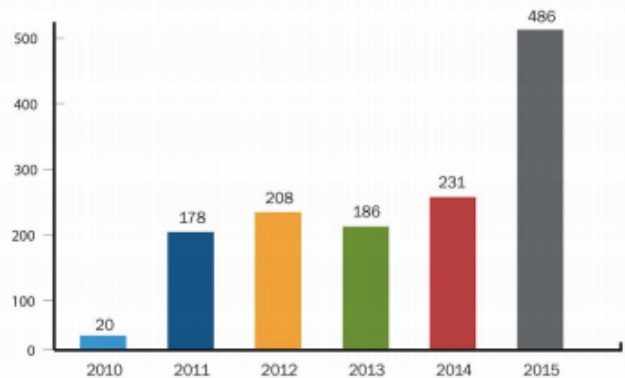
<https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>

- 164 Countries total
- Concentration in Asia, U.S. and Brazil



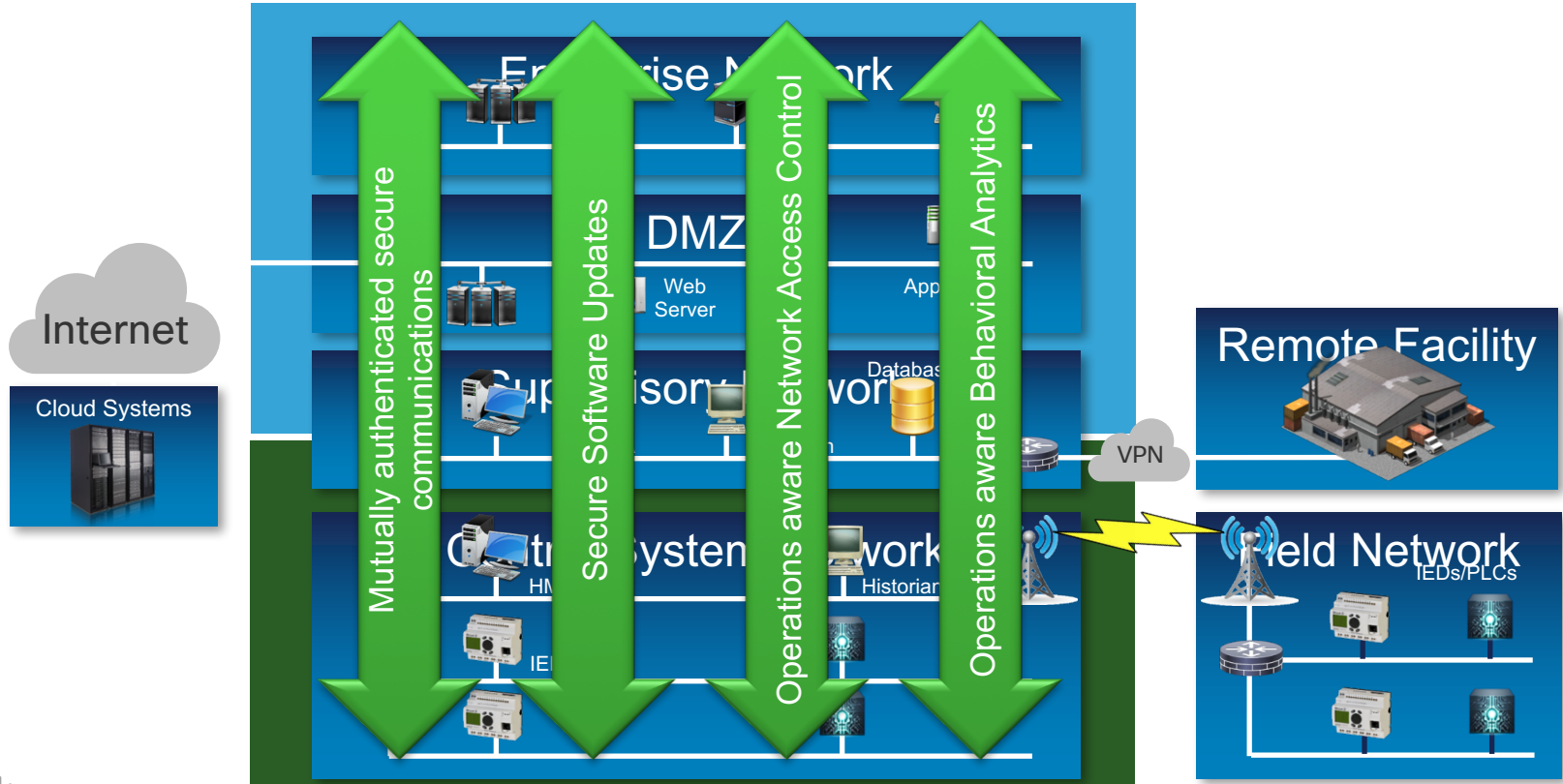
Vulnerabilities published at the rate IoT devices are introduced:

<http://www.pcworld.com/article/2472772/your-living-room-is-vulnerable-to-cyber-attacks.html>



*How do I build
a Secure
System?*

Addressing the IoT Attack Surface



But challenges will persist

- Physical Constraints: Low CPU, Memory and/or Power
- M2M Protocols are beginning to address security
 - Many still lack confidentiality and integrity
 - Most lack a root of trust
- Poor Design or Implementations:
 - Lack of Device Hardening: secure boot, anti-tampering, posture checks
 - Software bugs: buffer overflows, et al
- Telematics can be used as threat vector for loss of privacy and other attacks

Many Standards Forums and Consortia¹ addressing security

Technology Architecture Focused

Link / Comms

Core / Session / Transport / Messaging / Semantic

Multilayer

Vertical Focused

| | Connected Body | Connected Home | Connected City / Buildings | Transportation | Industrial IoT |
|----------|---|---|---|--------------------------|--|
| Protocol | HealthKit | HGI Home Gateway Initiative, HOMEPLUS, Z-WAVE 1.1 ALLIANCE, HomeKit | enOcean alliance For M2M, Building & Cities | GENIVI | Modbus, HART COMMUNICATIONS FOUNDATION |
| Industry | Wireless Life Sciences Alliance, Continua | THREAD GROUP | THE CONNECTED LIGHTING ALLIANCE, SBA | Open Automotive Alliance | Industrial Internet CONSORTIUM |

Marketing / Education



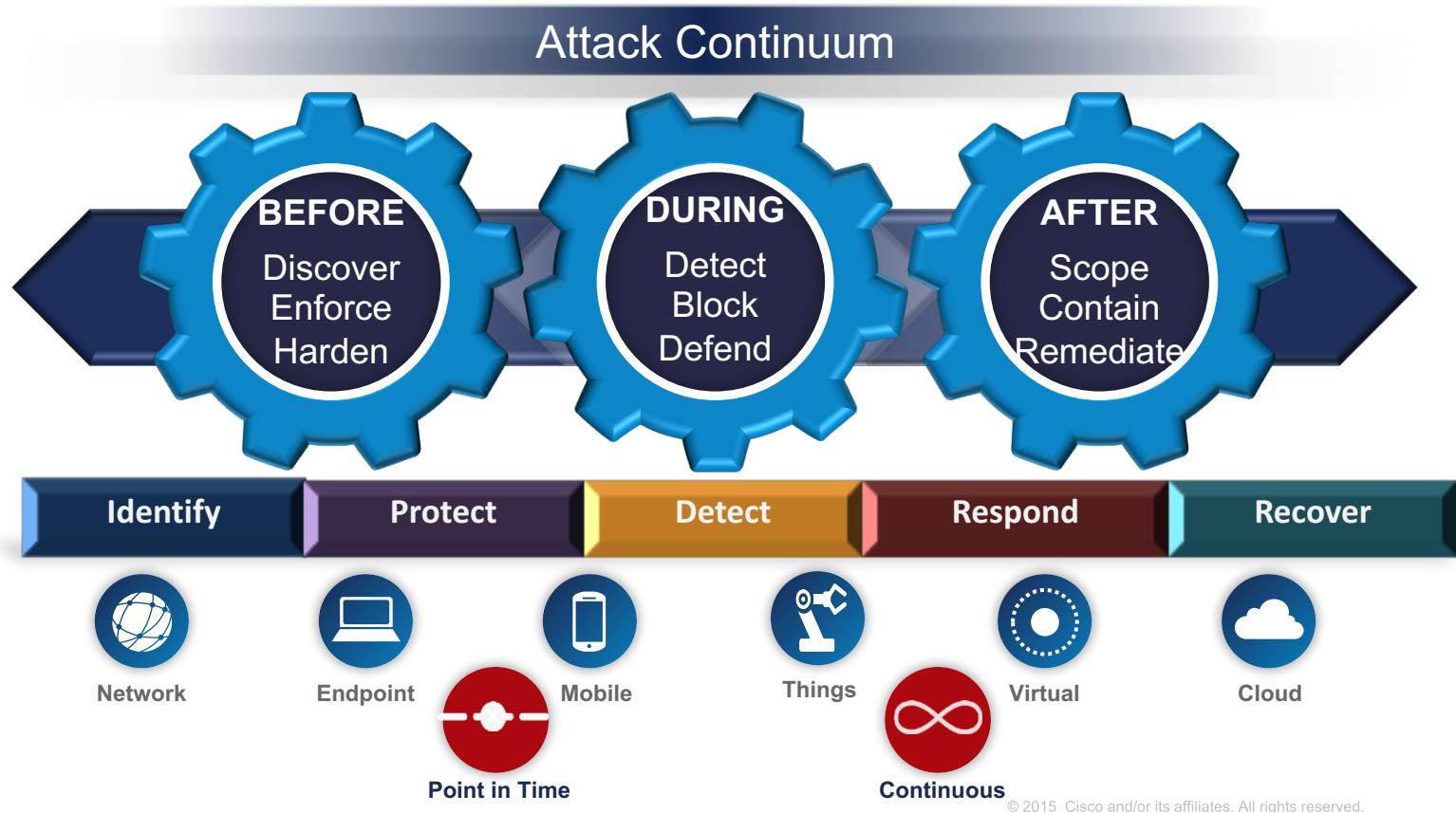
¹<http://www.postscapes.com/internet-of-things-alliances-roundup/>

Proactive Industry and Governments Define a Cybersecurity Framework

| Identify | Protect | Detect | Respond | Recover |
|--------------------------|-------------------------|--------------------------------|-------------------|-------------------|
| Risk Assessment | Access Control | Anomalies & Events | Response Planning | Recovery Planning |
| Risk Management Strategy | Data Security | Security Continuous Monitoring | Analysis | Communications |
| Asset Management | Information Protection | Detection Process | Mitigation | Improvements |
| | Awareness & Training | | Improvements | |
| | Protective Technologies | | | |

¹ <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

IoT Security Approach



Thank you.

