Security & Privacy Adventures in the IoT

Michele D. Guel, Distinguished Engineer & IoT Security Strategist
Cisco Systems
@MicheleDGuel

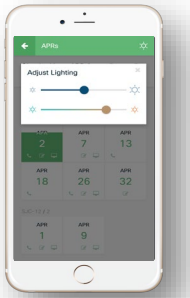
How did we get here?

Key Enablers

- IPv6 Addressing Space
  - Scales our addressing capabilities from < 4billion to 3.4 x 10^{33}
- Wireless technology advances
  - Smaller, longer battery life
  - Faster and more scalable – 802.11ac
  - Explosion of cloud providers and business models
- Advancements in Big Data Analytics, AL, ML
- Industry demand…

New Capabilities in the workplace

Connected Lighting	Room Check-in signs	Kiosk	Digital Signage
Connected Lights in Executive suites. Theme based lighting controls from Cisco Smart Spaces Application.	**PoE powered Audio Privacy Room (APR) check-in signs with color coded presence indicator**	**Kiosk with way finding, Indoor navigation, APR Check-in, people finder and Conference room booking**	**Dynamic context specific content to users in the workplace**



Cisco SMARTSPACES

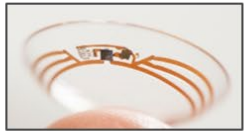













The Connect Day is now a reality

”The [Internet of Things] will allow for attacks we can’t even imagine.”

Bruce Schneier July 25,2016

MAJOR BANK Today

150K
Employees

866K
Devices

8.2K
IT Staff

105
Devices per IT Person

MAJOR RETAILER Today

340K
Employees

605K
Devices

2.8K
IT Staff

216
Devices per IT Person

MAJOR BANK

5,025,000
New IoT Devices

47,857
New IT Staff

MAJOR RETAILER

4,274,600
New IoT Devices

19,789
New IoT Staff

However…Breakdown

374

new devices per second

10 min

to connect and define policy

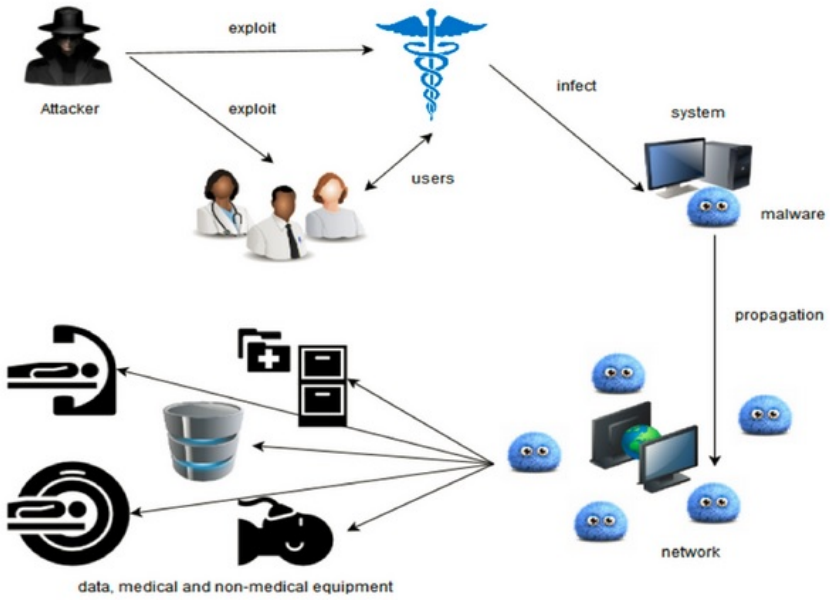
7.8

person-days of effort per second

245.8M

person-days of effort per year

Let us Look at Healthcare



Patient Data is everywhere…

- EMR
- Medical device
- Patient status boards
- Financial records
- Test Results
- Computer screens
- Fax sheets
- Records provided to patients
- Data used for research purposes
- Patient identification bracelets
- Prescription bottle labels
- Detailed appointment reminders left on voicemail
- Photograph or video recordings of a patient

“Medical information can be worth ten times more than credit card numbers on the deep web. Fraudsters can use this data to create fake IDs to buy medical equipment or drugs, or combine a patient number with a false provider number and file fictional claims with insurers.”

http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

Some Realities…

- “A survey by security company ZingBox found that U.S. hospitals on average have between 10 and 15 connected devices per bed. “
- “A Trend Micro survey found that more than 36,000 medical devices can be scanned and found by a tool called Shodan”
- “An exploit called MedJack was found to inject malware into a medical device, which then snakes through a network.”

Security Challenges with IoT

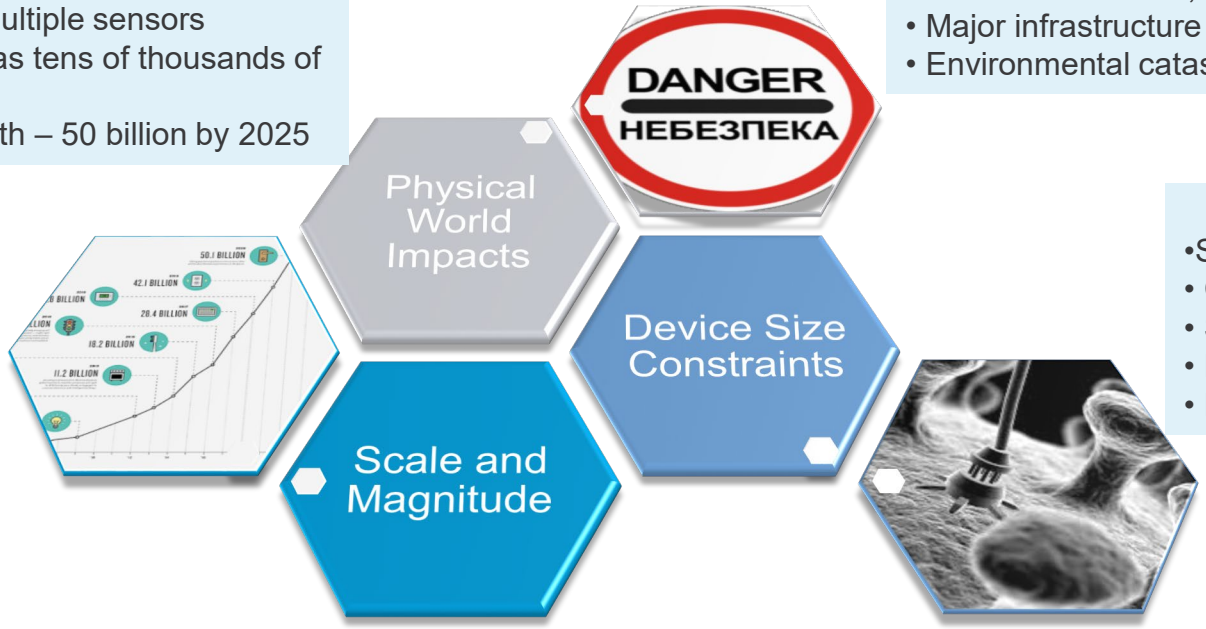
What is different about IoT?

SCALE

•Typical car has 300 different micro-processors, with multiple sensors
• City Singapore has tens of thousands of sensors
• Exponential growth – 50 billion by 2025

IMPACT

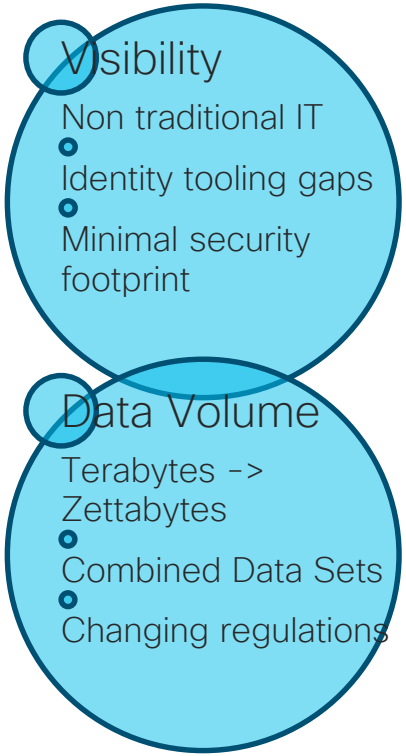
•Harm to human life,
• Major infrastructure outage
• Environmental catastrophe



Form Factor

•Smaller size,
• Cheaper to build
• Smaller memory,
• Less processing power
• Battery limitations

New Challenges in IoT



The problems in IoT are compounded;

- Visibility is reduced
- Data volume is increased
- Lower costs means security footprint and capabilities are reduced
- Higher risk means more security is needed
- More data means more scale for security investigations
- Privacy concerns are escalated, especially with GDPR.

Are the Threat Actors Different for IoT?

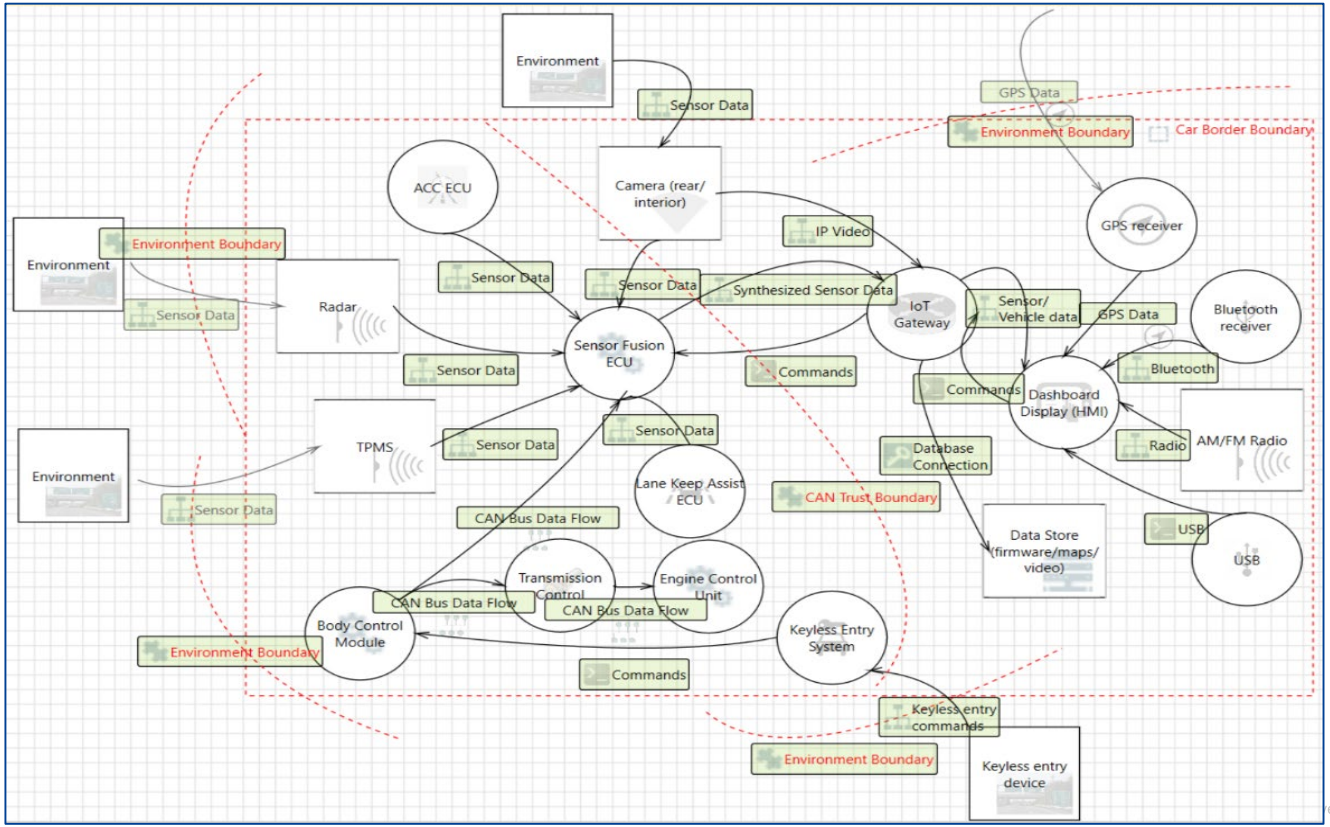
- Pranksters
- Chaotic Actors
- Hacktivist
- Researchers/Gray Hats
- Cybercriminals
- Cheaters/Gamers
- State Sponsored (APT)
- Security Agencies
- Insiders
- Corporate Espionage
- Terrorist

Common Attack Patterns

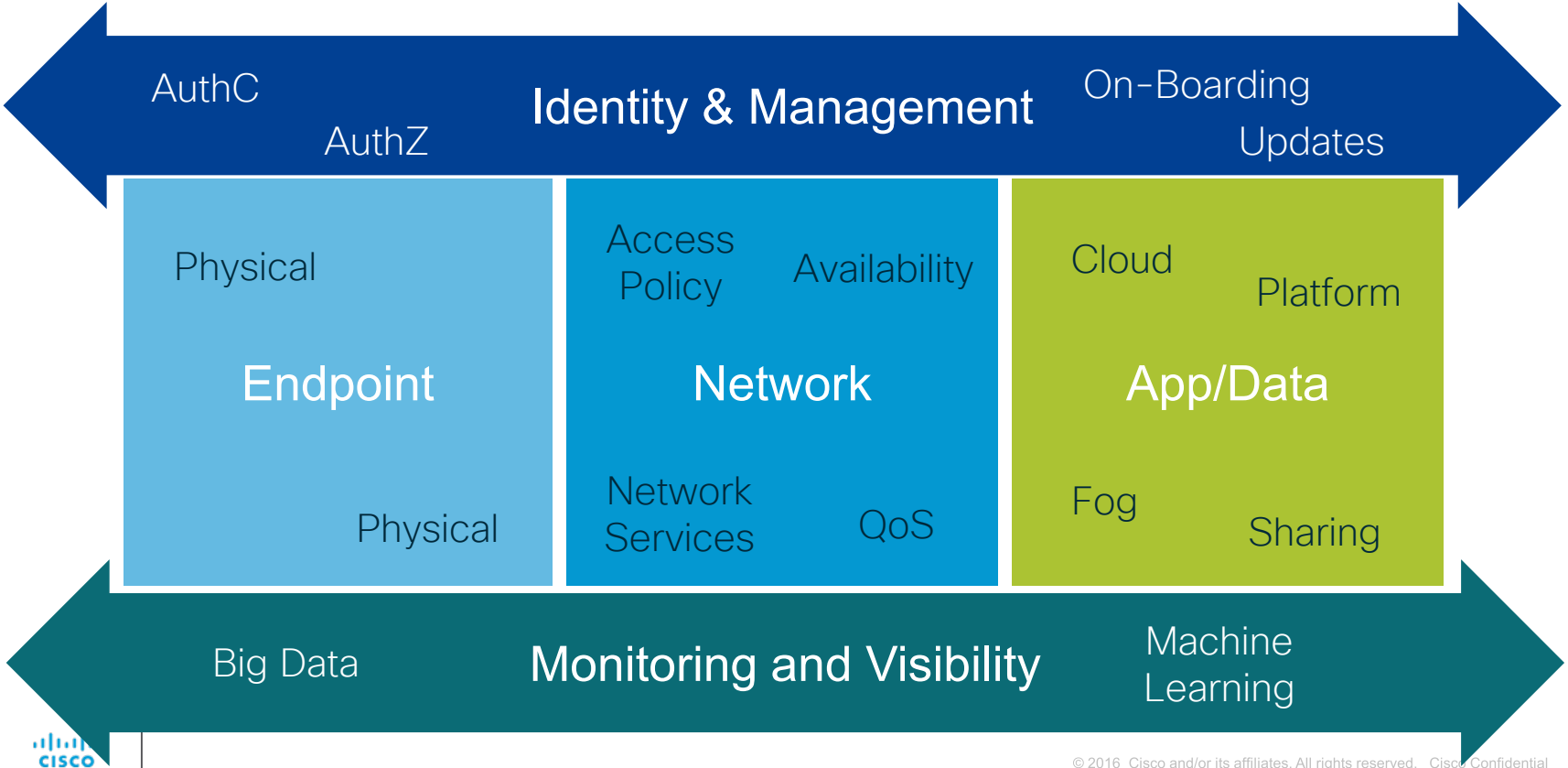
- Identity spoofing/Elevation of privs
  - Known default credentials
  - Pivot attack
  - Botnets
- Denial of service
  - Repeated actions (light switch)
- Web/Cloud Services
- Physical tampering
  - Forced reboot – interrupt
  - Add-on or remove elements
- Trojaned firmware
  - Altered firmware
  - Old /vulnerable firmware
- Communication channels attacks

An Integrated Architecture Approach

Threat Model Complexity



IoT Security Layers



Identity and Access Management Controls

- All devices must require authentication with strong passwords or multi-factor prior to user or administrative access.
- Endpoint devices must not contain default user/password combinations (e.g. “admin/admin”) that are easily guessed or accessible.
- All devices must be on boarded in a secure manner.
- Principe of least access should be used for all administrative functions.

Baseline Security Requirements for IoT Endpoints

- Secure boot & system integrity
- Hardened and secure system
- Secure communications
- Ensure data privacy
- Network identity
- Secure web interfaces
- Minimize threat surface
- Log critical events
- Minimal security operations
- Secure Firmware/OS updates

Baseline Security Requirements for a Secure IoT Network

- Authenticate devices allowing them to join to network
- Limit network access
- Provide network telemetry
- Provide threat detection and mitigation
- Provide authenticated time distribution (NTP)
- Provide audit capability
- Limit unnecessary services

Application Layer Security Controls

- Strong Cryptographic Support
- Strong Authentication & Authorization
- Ensure Data Privacy
- Ensure Data Separation
- Hosted Services Hardening
- Log Critical Events
- Basic Operational Processes
- Strong Session Management
- Strong Web Security
- Strong Supply Chain Security

Monitoring and Visibility Controls

- Visibility of endpoints in the echo systems
  - Understanding of their baseline expected behavior
  - Identify compromise endpoints
- System Event Logging
  - Read/write endpoint state, update firmware
  - excessive unauthorized access attempts
  - excessive or inappropriate use of the Endpoint
- Declarative and heuristic mechanisms to detect attacks on the infrastructure
- Automated mitigation through policy updates

Data Privacy in IoT

How much data are we generating?

- 2.5 quintillion bytes of data a day (18 zeros)
- > 500K tweets/day
- > 40K Google search/second, 5 billion/day worldwide all engines
- > 600 million Instagrammers
- > 1.2 trillion photos
- Estimated 200 billion devices by 2020

Would you change your behavior if every aspect of your life was digitally captured?

The 2013 Wake-Up Call

- The volume of personal data collected and stored, and the global availability of this data.
- The maturity and complexity of big data analytics around privacy data, and the new relationships (trends that have been discovered.
- The increase in number and complexity of cybersecurity threats that impact data privacy.
- The number of people, both good and back “actors” that have access to personally identifiable information, and the capability to expose it either accidentally or intentionally.
- The rapid increase of Things.

A few “adventures” to consider

- The Connected Car
- Connected Parking Solutions
- DNA Data (23&Me, Ancestry.com, GEDMatch
- Smart Watch Geolocation Data & Other data

Our Love of Data

A Data Romance Life-Cycle

- Data Tantalization
- Data Realization
- Data Minimization
- Data Anonymization
- Data Monetization

Is the situation hopeless?

Privacy engineer to the rescure...

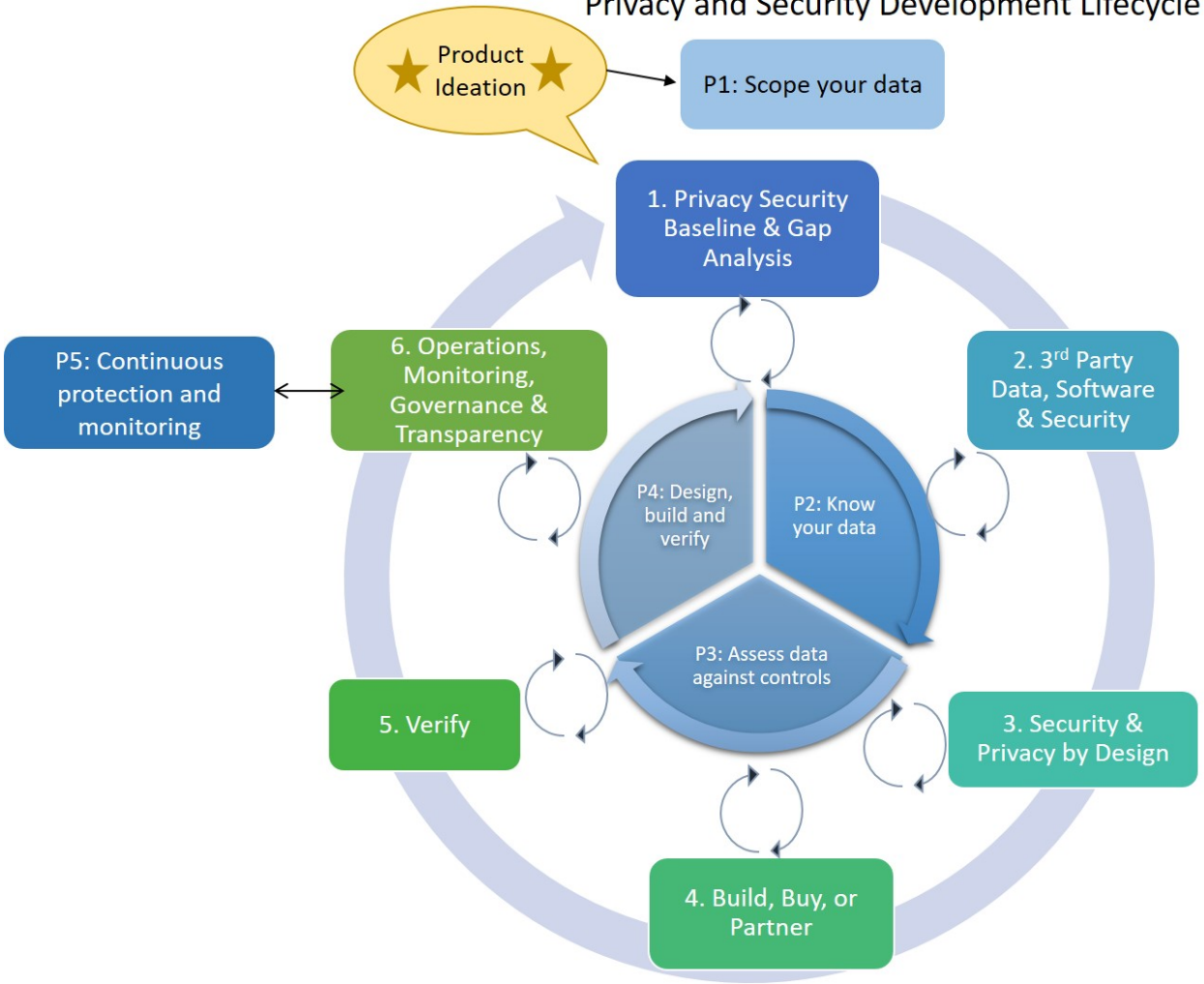
Privacy Fundamentals

- Organizational privacy guidelines and policies
- Privacy Impact Assessment
- Data Flow Diagrams or Data Ontologies
- Use Case Development
- Threat Modeling
- Privacy Procedures & Processes
- Privacy Mechanisms or Privacy Enhancing Technology
- Privacy Risk Assessment
- Privacy Training
- Testing & Quality assurance

A Privacy Framework

- Data Context
- Legal Basis
- Collection Limitations
- Transparency
- Proportionality
- Use Limitation
- Data Minimization
- Security
- Retention & Deletion
- Onward Transfer
- Individual Rights
- Accountability & Operations Requirements

Privacy and Security Development Lifecycle



Key Take Aways

Security is key to digital disruption and innovation

Develop a risk methodology for IoT solutions

Look at the solution end to end:

- Purchase from a trustworthy vendor
- Segment the network, apply policy dynamically
- Manage and operate securely

Instrument the network for visibility, detection and response

Breach will happen

Thank You

Updated May 2017