ISSA: October 2014
The Internet of Things (IoT)
Agenda

1  Introductions 1
2  Internet of Things 5
3  Security Risks and Challenges 17
4  Key Takeaways 28
5  Q&A 30
Section 1

Introductions
Section 1 – Introductions

Presenters

Caesar J. Sedek
Director

Caesar is a Director in PwC’s IT Security, Privacy and Risk practice. He has extensive experience in delivering complex, multinational projects and specializes in security strategy, information security program management, and industry framework / regulatory compliance including ISO 27001, HIPAA, PCI-DSS and Safe Harbor. Caesar has a decade of experience in the Entertainment and Media industries with expertise in intellectual property and content protection, anti-piracy and privacy. Caesar also holds several industry certifications, including: CISSP, CISM, CIPP/IT and CRISC.

Ying Yang
Senior Associate

Ying is an Information Security professional with PwC and has experience and broad expertise in Data Loss Prevention (DLP) technologies and capabilities, security strategy, data protection capabilities, data classification and retention, security policy and governance, and security assessments. She has over four years of technology consulting experience and has worked on multiple large-scale security projects in the entertainment, pharmaceutical, resources, public sector, financial services and automobile industries. Ying holds a CISSP certification.
Section 1 – Introductions

PwC’s Internet of Things DeepTech Team

Richard Rowe  
Director  
(Digital Solutions)  
richard.rowe@us.pwc.com

John Steggles  
Manager  
(Emerging Technologies)  
john.steggles@us.pwc.com

Diego Sanz  
Senior Associate  
(Insights & Analytics)  
diego.sanz@us.pwc.com

Charmaine Hung  
Experienced Associate  
(Financial Services)  
charmaine.hung@us.pwc.com

Daniel Eckert  
Managing Director  
(Emerging Technologies)  
daniel.eckert@us.pwc.com
Overview

- Elements of the IoT
- Current state of the IoT
- Existing pioneer vendors of the IoT

- Evolution of the IoT maturity
- Growth of the IoT
- Future of the IoT

- Current risks
- Future risks

- Challenges with the IoT

- Risk mitigation

What is the Internet of Things (IoT)?

Why is the IoT important?

What are the most significant security risks and privacy concerns of the IoT?

What are factors that constrain the development of the IoT?

What can we do to prepare for the growth in the IoT space?

Issa: October 2014 • The Internet of Things (IoT)
Section 2

Internet of Things
What is the Internet of Things?
The Internet of Things refers to the network of uniquely identifiable physical objects, accessible through the Internet, and contain embedded technologies that allow them to interact and interconnect with their internal states and/or the external environment.
Why the IoT matters to Consumers

The Internet of Things can help consumers achieve their goals by scaling consumer data collection and processing capabilities in a way that their ability to make better decisions - via augmented intelligence - is significantly increased.

**Theory:**

Metcalfe’s Law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system.

**Reality:**

Walking into a clothing store and being able to see what you look like in anything you select – without having to actually try it on.

Image Source: http://fits.me/solutions/the-fits-me-virtual-fitting-room/
Why the IoT matters for Enterprises

The IoT is the extension of the Internet to the physical world. While the Internet has transformed digital industries, the IoT will transform physical industries.

Theory:
• The IoT helps businesses achieve greater process optimization and efficiencies through real-time data.
• The IoT is closing the information loop and providing insight and feedback.

Reality:
Assets in a manufacturing plant are affixed with wireless sensors. Using remote monitoring technology, plant managers can locate and track production inventory on the plant floor and the supply chain in real-time.
### Elements of the IoT

The IoT adds new elements, people, location, and dynamic services – driving capabilities that enable interactivity and contextual intelligence to connected “things.”

| Sensor / Actuator                  | • Sensors: Embedded in devices or the physical environment and capture relevant events.  
|                                  | • Actuators: Execute a physical change and transmit data. |
| Data                              | • Data: Structured, self-describing and on-demand.  
|                                  | • Data is collected and drives sensors and actuators.  
|                                  | • Enables intelligence. |
| Network                           | • Network: IP-enabled, proximity (NFC), WAN, wireless and/or fixed.  
|                                  | • Creates the backbone of the ecosystem and connects the sensors, actuators and services. |
| Service Platform                  | • Services (i.e. information services and communication services) store information and provide the intelligence engine for analytics and service management for the end user. |
| Infrastructure                    | • Provides the ecosystem management and serves the business.  
|                                  | • Aggregates data, performs intelligence analysis and reporting, and provides the hardware and storage. |
Convergence of the digital world: information, operations and consumer technologies.
Application of the IoT extends beyond consumer products.
Large corporations developing proprietary platforms and ecosystems.
Sector and vendor specific – devices are not compatible across industries or brands.
# IoT Vendors

<table>
<thead>
<tr>
<th>Pioneer Vendors of the IoT</th>
<th>Product Description</th>
</tr>
</thead>
</table>
| **Unified Computer Intelligence Corporation** | • Device (Ubi) that is plugged into the wall and brings voice activation to the home.  
• Remotely control online accounts and smart devices.  
• 24/7 monitoring of surrounding environment. |
| **Revolv** | • Hardware hub and app synchronizes and orchestrates smart home products running on different technologies, network protocols and apps.  
• Enables smart products to integrate together. |
| **SmartThings** | • Internet service platform, hub, application and retail website for purchasing and managing smart products.  
• Aggregates usage patterns of customers to help consumers automate their homes with over 1000 smart products. |
| **Evrythng** | • Software company that provides an identity to physical objects and links to a web profile for the product with details of the customer and relationship, allowing providers to push relevant content to their customers. |
| **BioBeats** | • Collects real-time data on a user’s heartbeat, breathing rate and skin response to help assess the user’s psychological and physiological state to tailor and personalizes musical experiences based on stress level. |

Source: Forrester, Pioneer Vendors: Smart, Connected Products for the Internet of Things
Evolution of the IoT Maturity

Personification of Objects

- Exists and ongoing today.
- Provides an identity and basic functionality to objects creating value for the user through intelligent services and systems (i.e. smartphones and web services) that process and analyze data from the objects.
- Examples include:
  - Push-button start on cars.
  - Unique barcodes on products to unlock rewards or track loyalty programs.

Partially Autonomous Sensor Networks

- Gaining momentum and will roll out over the next five years.
- Objects will begin to develop the ability to sense their surroundings and have the capability to take limited action based on the information gathered.
- May be restricted to a personal network or selected web services.
- Examples include:
  - Controlling smart appliances and devices using smartphone.
  - Forest fire detection via sensor nodes to measure temperature, humidity, etc.

Autonomous and Independent Devices

- Expected to begin to emerge in the next three to five years.
- Objects have the ability to independently sense context and autonomously interact with other devices, services and sensors without the management from another device.
- Examples include:
  - Traffic signals and road signs reroute, divert or update speed of traffic based on traffic throughput.
  - Stores are able to detect items you wear or carry and personalize your shopping experience and communicate offers relevant to you.

Source: Forrester, Prepare Your Security Organization For The Internet of Things
Example Use Case #1: In-store customer interaction

Retailers optimize store layouts and product offerings through connected devices to gather data and enrich customer experience. In-store communications will become more personally relevant as devices recognize customers and deliver customized content.

**Industry:** Retail, bricks-and-mortar, etc.

**Description:** Using an array of in-store sensors ("beacons") to micro-locate the position of a participating customer, retailers can track interest in specific products and services, provide notifications about events and promotions, and enable contactless payments.

**Key Technologies:** Apple iOS and Android devices with Bluetooth 4.0 Low Energy (BLE); Location-based Services.

**Impact:**
- Retailers: Can offer more specific, targeted information to customers, which aids sales and customer service; Obtain hyper-local data regarding customer behavior within a store.
- Customers: New levels of interaction and engagement with a brand; Discounts and promotions more relevant to their interests; Speedier payments and customer service.
Example Use Case #2: Creating the health feed

Captures your vital signs regularly and beams them via Bluetooth to a smartphone app that stores, reports and notifies based on data captured.

**Industry:** Healthcare

**Description:** A smartphone-based medical sensor can read temperature, pulse rate, heart rate, blood oxygenation, etc. This data is transmitted to the cloud where it can be analyzed for anomalies, accessed by your personal doctor, and aggregated with similar data from millions of others.

**Key Technologies:** Wearable or embedded sensor that transmits data via Bluetooth to a smartphone-based app.

**Impact:** Consumers can be empowered to take control of their health and gain direct access to their personal health feed. Instead of capturing an individual’s vital sign data only when they visit their doctor, the sensors collect and store real-time data continuously. Historic personal health data can then be monitored for more accurate predictive health diagnostics.
Over **50 billion** devices are expected to be connected to the **Internet** by the year **2020**.

**IoT** is expected to grow from 1.9 billion devices today to **26 billion devices** by the year **2020**, over double the size of general purpose computing devices and the wearables market.

Growth in IoT can be attributed to lower component costs and advances in technologies.

---

**IoT excludes:**
- Tablets
- PCs
- Smartphones

PCs, tablets and smartphones are expected to grow to **7.3 billion** devices by **2020**.
Future State of IoT Space

• Consumers will expect a consistent and contextual way to control their products, devices and services in a personalized and convenient manner.

• Enterprises will need to evolve their architectures to accommodate aggregation and analysis of large amounts of data streams.

• Endless amount of possible services, products and applications.
Section 3

Security Risks and Challenges
Section 3 – Security Risks and Challenges

Current Risks – Internet of Things Security

HP reviewed the ten most popular IoT devices according to the OWASP Internet of Things Top 10 including: TVs, webcams, thermostats, remote power outlets, sprinklers, device hubs, door locks, home alarms, scales and garage door openers.

Of devices collected at least one piece of personal information.

- 80% Of devices raised privacy concerns especially when using cloud services or transmitting unencrypted personal information.

- 60% Of devices had insecure web interfaces that enable cross-site scripting, weak default credentials and poor session management.

- 60% Of devices failed to encrypt or protect the downloads of update files.

- 90% Of devices had weak password policies – insufficient complexity and length.

- 80% Of devices failed to encrypt network services transmitting data to the Internet and local network.

- 70% HP reviewed the ten most popular IoT devices according to the OWASP Internet of Things Top 10 including: TVs, webcams, thermostats, remote power outlets, sprinklers, device hubs, door locks, home alarms, scales and garage door openers.

ISSA: October 2014 • The Internet of Things (IoT)

Source: HP Enterprise Security, Internet of Things Research Study 2014
A specific type of worm attacked industrial systems configured to control and monitor specific industrial automation processes.

Internet-enabled baby monitors hacked, allowing malicious users to spy and yell at babies.

A luxury yacht was lured off course by researchers who hacked the GPS signal used for navigation.

First generation of RFID tags on US passports were vulnerable to equipment worth $250 to access and read the information.

Hackers have been found to break into the disguised control systems tied to water supplies in the U.S. and other countries.

Researchers were able to hack into two types of cars and wirelessly disable the brakes, turn off the lights and switch the brakes full on beyond the control of the driver.

A security company discovered a new Linux worm that appeared to be engineered to target Internet-enabled devices (i.e. home routers, set-top boxes, security cameras) in addition to traditional computers.

Global attack campaign involving more than 750,000 malicious phishing and spam email communications coming from more than 100,000 everyday consumer gadgets.
The collection of multiple pieces of data could be aggregated to become personal information and used in the context of location, time, recurrence, etc.

Malicious hackers or consumers could leverage vulnerabilities in the devices and gain unauthorized access, impersonate objects or tamper with results.

Data storage, especially cloud, raises the risks around identification, authentication, data access, liability and legislative restrictions.

How data is transmitted and shared across devices will require controls in place to properly and securely distribute the information.

ISSA: October 2014 • The Internet of Things (IoT)
Future Risks – Example: Driverless Cars

Current Capabilities
New cars have the capability to provide real-time status information and the ability to remotely control aspects of the car.

Vulnerabilities
Hackers have demonstrated the ability to gain access to certain areas of the vehicle – will be an issue as more features and technologies are added.

Risks
Consequences of security failure or breach could be fatal. Security becomes a life and death proposition.

Remote connectivity and “always-on” features will make cars more attractive targets for malicious users and increased exploitation.

Consumer and public safety will be one of the main drivers toward legislation and standards for securing devices that make up the IoT.
Challenges with IoT

Standardization across components (communication protocols, messaging formats, data models) between manufacturers and brands to enable interoperability.

Policies and standards to address security, privacy, governance and safety around the IoT – controls and established protocol for the objects expected to connect to the Internet.

Successful global adoption and deployment of IPv6 to accommodate the large address space required for objects and implementation of M2M technologies.

Higher density for power sources and improved battery life within limited size constraints to enable embedded devices to function without constant recharging.

Improved wireless technologies to allow devices to communicate over greater distances without any data loss and excessive power consumption.
Challenges with IoT – Big Data Aggregation

IoT generates massive volumes of data for analysis.

The estimated 50 billion objects that will be connected to the Internet by 2020 will producing a massive volume and variety of data at unprecedented velocity.

The *Brontobyte* \((10^{27} \text{ bytes of information})\) is expected to be the measurement to describe the type of sensor data that will be generated from IoT devices.

Big Data tools will be used to collect, store, analyze and distribute these large data sets to generate valuable insights, create new products and services, optimize scenarios, etc.
Challenges with IoT – Reality Check

- Three characteristics of an ideal solution or product.
- Combination of all three is unrealistic.
- Choose two out of the three:
  - Freedom/Security
  - Freedom/Convenience
  - Security/Convenience
Risk Mitigation

Overall Areas of Focus

- Standardization of data models, data messaging formats, communication protocols, data collection, etc. will allow for interoperability between devices.
- Prevent malicious users from exploiting vulnerabilities in unsupported devices and unpatched systems.
- Understand how various services will interact with each other which may create unsafe or undesirable situations and plan process architecture to include failsafe mechanisms.
- Enable and define integrity checks and accountability for data and devices.
**Risk Mitigation for Enterprises**

As more devices are created and connected to the Internet, enterprises should:

- Develop a multi-layer approach to security by building object level security from the bottom up (e.g., secure SDLC, multiple test cycles).
- Deploy technologies after risks are fully understood and manageable.
- Understand the security capabilities of their business partners and third parties to limit downstream liability.
- Implement policies and procedures to address shared threats that result from interconnected technologies.

**Holistic Security Model**

- Identify Stakeholders / Determine Scope
- Conduct Risk Assessment
- Determine Business Impact
- Develop Plan to Integrate Security
- Continuous Monitoring
Risk Mitigation for Consumers

As more devices are created and connected to the Internet, consumers should understand and be aware of:

- The interoperability between the devices and technologies.
- How information is shared/transferred between devices and applications.
- The privacy terms and conditions of various devices.
- The risks to sharing information on devices and social media.
- The implications of linking social media accounts.
Section 4

Key Takeaways
Summary

• The IoT delivers the data and services, creating an ecosystem that provides information and intelligence and drives contextual awareness about you and your surroundings.

• The IoT will create streams of data, contributing to the Big Data challenge.

• The IoT will transform the landscape for business and society – though the IoT will make the world more connected and efficient, it will also create new attack vectors for hackers.

• Standards and best practices will need to be created to adapt to the growth of the IoT.

• Security must be considered in the design and built-in as a foundation for the IoT.
Section 5

Q&A
Questions?

Caesar J. Sedek  
PwC, Director  
(213) 407-1810  
caesar.j.sedek@us.pwc.com

Ying Yang  
PwC, Senior Associate  
(347) 415-2872  
ying.yang@us.pwc.com