www.pwc.com/mu

Internet of things

Prevailing perspective- opportunities and risks

Computer Security Day

Confidential
November, 2016

pwc

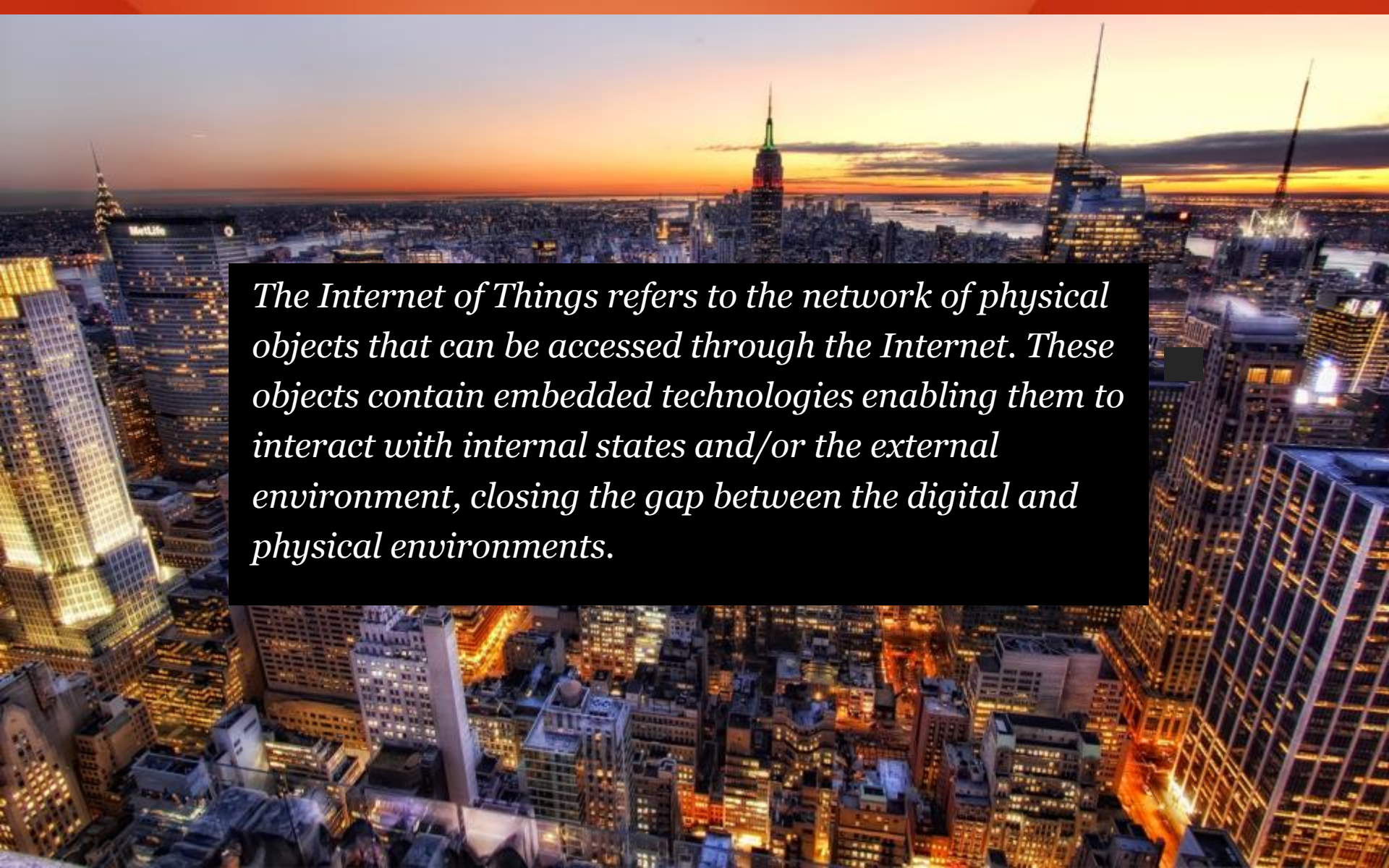
Agenda

PwC – IoT Technology Forecast

Opportunities and risks

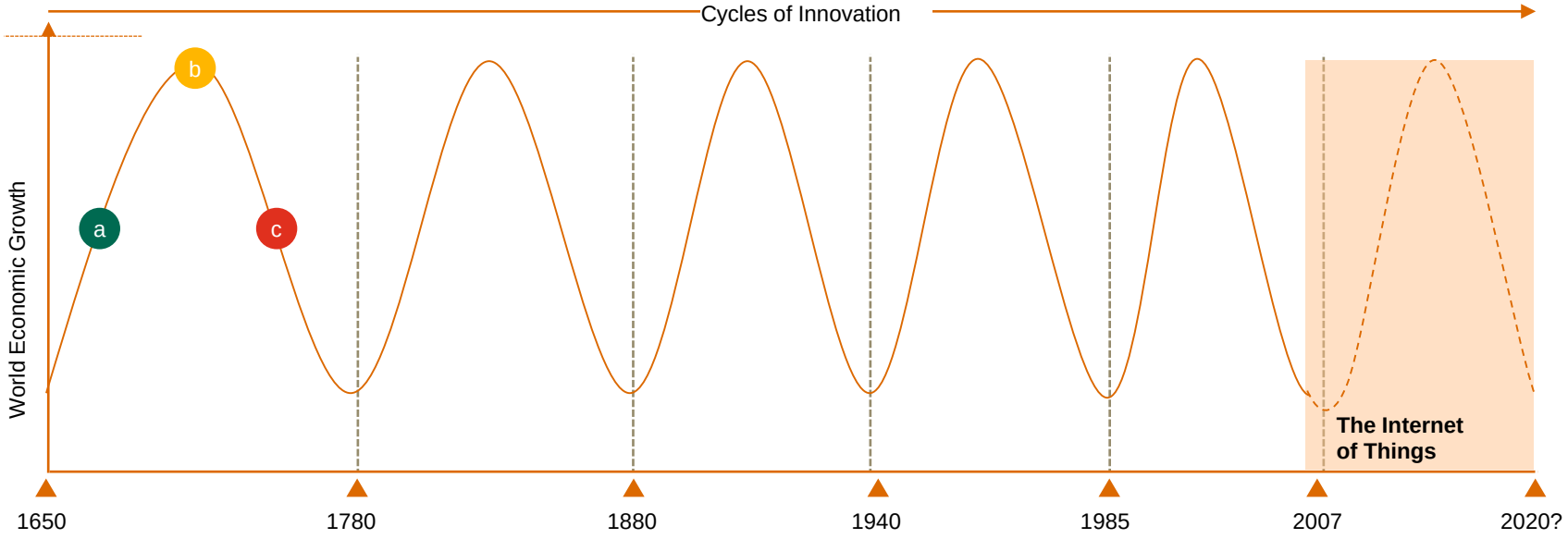
Security Consideration for Internet of Things

PwC Technology Forecast
Internet of Things



The Internet of Things refers to the network of physical objects that can be accessed through the Internet. These objects contain embedded technologies enabling them to interact with internal states and/or the external environment, closing the gap between the digital and physical environments.

Internet of Things, a new innovation horizon – Throughout history, businesses have been transformed by revolutionary innovations, followed by evolutionary applications



Financial-agricultural revolution	Industrial revolution	Technical revolution	Scientific-technical revolution	Information and Telecoms revolution	Internet of Things
• Mechanisation, Four field crop rotation etc	• Steam engine, Cotton-based technology etc	• Steel, Electric motors, Internal combustion etc	• Consumer goods, Semiconductors, Computers, Plastics etc	• Fiber optics, PCs, internet, Biotech etc	• Social media, smart phones, data analytics / intelligence, etc

a **Innovation Phase** – Innovations occur in a practical form and are adopted by early users

b **Application Phase** – number of radical innovations falls and attention turns to incremental innovation, i.e. exploiting and extending existing innovations

c **Stagnation Phase** – a coming to an end of the application phase characterised by economic stagnation ahead of the next wave

*Based on the theories of innovation advanced by Schumpeter which argued that waves of innovation are the platform for economic development, which results in the creation of leading industrial or commercial sectors, and the associated "creative destruction" of the previous established technologies and businesses built on these paradigms

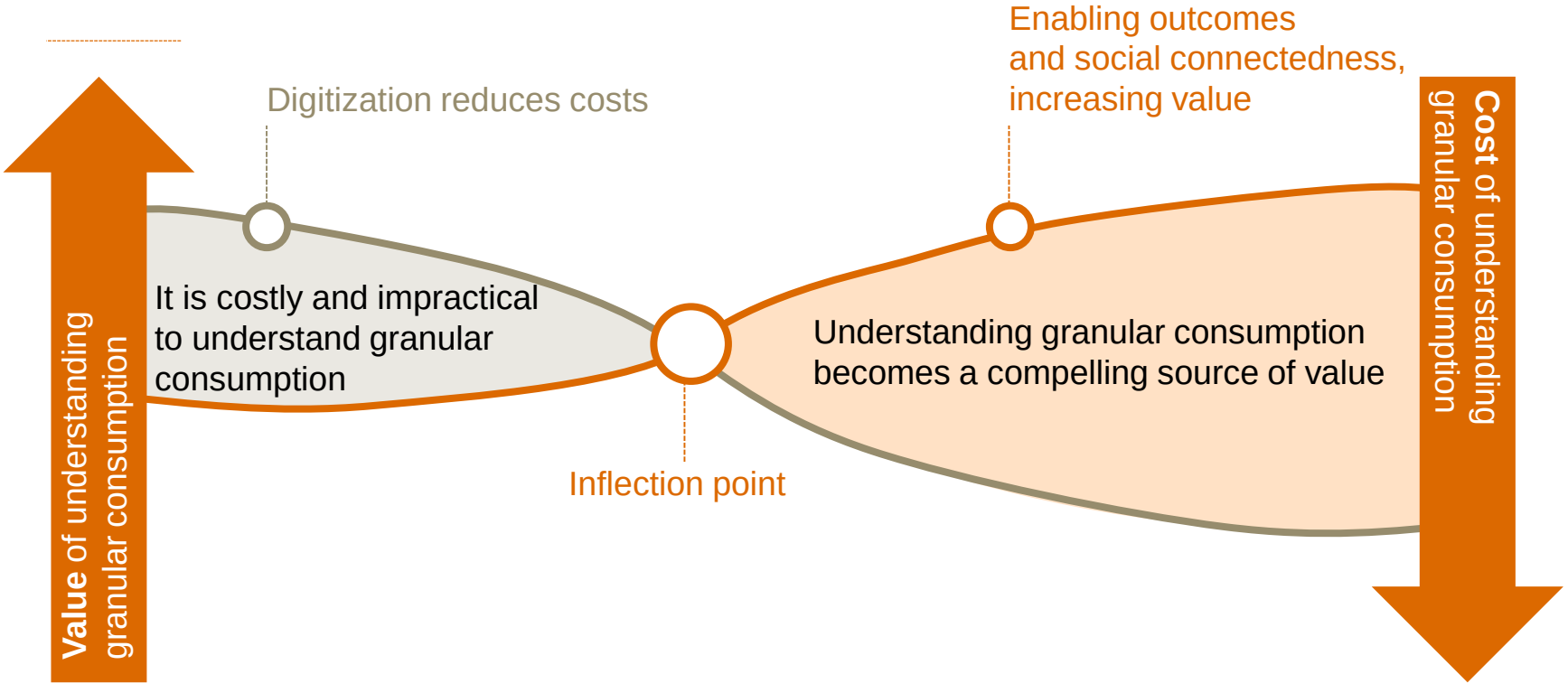
Change – Technology enabled consumer trends

1999-2007	*The 'disruptors'*	*Today's digital ecosystem*
Product digitisation	*Collaborative and social media*	
Process digitisation	*Cloud Computing*	
Pulling and aggregating info		*Integrated*
Creating centralised marketplaces	*Analytics and insight*	*Customer - centric*
Web = another channel to market	*Mobility and anywhere access*	*Continuous interaction*
		Collaboration

- **Revolutionary change to how information-based products are sold**
- **Revolutionary change to how customers are serviced in any sector**

http://www.pwc.com/techforecast

Key Change: Technology trends are digitizing consumption



- ***The costs of digitizing granular consumption is dropping***
- ***The costs of understanding granular consumption is dropping***
- ***The value from understanding granular consumption is rising***

Taking advantage of digitization of consumption: Insurance industry example

Key changes from past:

- *Digitized the consumption*
- *Going beyond transaction (pricing of product)*
- *Augmented experience (real-time feedback while driving)*
- *In internal trials, drivers in safe zone increased from 25% to 75%*
- *Give customer more control on premium and make safer (goals)*

What is possible with Internet of Things that was not possible before?

"The technology now enables companies to help customers achieve the goal that they're buying the product for—as opposed to just selling it to them most cost effectively, which is what businesses have done in the past."

—Fred Cripe, Former EVP, Allstate Insurance

IoT in the FS industry

Payments

- One of the most recognizable IoT solutions for mobile payments is **Apple Pay**.
- Users are able to make payments simply by presenting a supporting Apple product and providing **user authentication**.
- The payment itself is then performed using **near field communication technology** which transmits a customer's payment information to a receiver which processes the payment.
- FS organizations have partnered **with technology companies** to offer **mobile** payments from objects such as watches, fitness trackers, and many more.

Insurance

- Automobile insurance companies are leveraging IoT technology to provide **UBI solutions**.
- By placing a sensor in the driver's car, the **insurance** company is able to **monitor** the customer's driving habits and offer discounts based on certain **safe driving metrics**.
- It is estimated that by 2020, **50 million** drivers will be users of UBI solutions.
- Similarly, IoT technology in homes is able to monitor **customer safety habits.**

IoT in the FS industry

Banking

- IoT technology has enabled banks to **lock automobiles** if a loan is defaulted, **increasing the chances of loan payment** and decreasing banks' cost of **repossession**.
- Additionally, banks are using IoT technology in their internal operations to identify and troubleshoot issues with ATMs. For example, banks can **automatically** shut down ATMs in the case of functionality or security issues.
- Banks are also partnering with certain companies to provide **geographically targeted offers and deals**.
- When a customer uses a credit or debit card, the bank **identifies** the customer's **location** and offers deals at **nearby** stores through text messages or push notifications.

Opportunities and risks

IoT market structure & areas of application

Market stakeholders

Enablement hardware: *ARM, Intel.* These companies create the embedded processing solutions (micro-processors, sensors, etc.) at the heart of IoT.

Network services: *Cisco, AT&T, Orange.* These companies provide connectivity to IoT-enabled objects.

Managed services: *SAP, IBM, Microsoft, Oracle* . These companies offer data and analytics services, mobile and cloud computing and systems applications

Industrial equipment: *GE, Bosch, Siemens*. These companies design and develop software for IoT applications, focusing on mobility, energy management and manufacturing.

Consumer tech companies: *Google - Nest Labs, Apple.* These companies are currently developing IoT software and connected home and healthcare products.

IoT verticals

Smart Cities

- *Maintenance*
- *Utilities*
- *Lighting*
- *Policing & surveillance*
- *Emergency services*
- *Signage*
- *Traffic control*
- *Waste management*

Smart Homes

- *Lighting*
- *Security*
- *Heating*
- *Smoke alarm*
- *Pet feeding*
- *Irrigation controller*
- *Infotainment*
- *Cooking & groceries*
- *Energy monitoring*

Smart Health

- *Patient care*
- *Elderly monitoring*
- *Remote diagnostic*
- *Bio-wearables*
- *Equipment monitoring*

Smart Transport

- *Telematics*
- *Infotainment*
- *Smart parking*
- *Public transport*
- *Airlines/Trains*
- *Shipping*

Smart Industry

- *Production control*
- *Supply chain*
- *Robotics*
- *Energy monitoring*

Smart Buildings

- *Thermostat*
- *Security*
- *Lighting*
- *Electrical*
- *Transit*
- *Occupancy*
- *Energy monitoring*
- *Emergency alerts*

Opportunities and benefits

Increased customer empowerment

Designed to offer **customizable services** with **real-time feedback**, enabling customer to gain **more control** of their daily lives.

Added business value

Help Businesses achieve **operations cost efficiencies** through automation. IoT can also boost **customer experience** through up-sell and cross-sell connected accessories.

Enhanced trust capital

IoT growth creates an **exponential increase** in data flows, brands acting as **ethical custodians** of their customer`s data and offering them personalized data control boosting **brand sustained loyalty**.

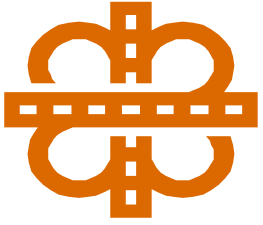
IoT Case Studies – SmartThings

SmartThings

- SmartThings is **a home automation** system that provides hardware, an app, and a cloud service to connect devices and gadgets throughout the home.
- SmartThings devices allow users to connect devices such as doors, lights, and **appliances**, bringing control and **analytical potential** to everyday life.
- **SmartThings raised $1.2m** on Kickstarter in September 2012, then **$12.5m in equity** in November **2013**. Samsung is now moving to acquire the company, similarly to Google's acquisition of Nest earlier this year.
- They are currently pursuing potential partnerships **with home insurance firms**, with the possibility of using the **data** from their devices **to tailor insurance policies** to a much **higher degree of detail**.
- From this initial push towards **hardware integration**, it is predicted that the selling of services in **analysing and utilising** the data will form a much larger part of the business.
- The **Smart Home industry** is predicted to bring in **$17.9bn** in revenue this year, with **$40bn** predicted by **2019**.

IoT Security Challenges and recommendation

Risks and Challenges



Data privacy and security

- Personal and company data are **potentially at risk** as the amount and level of granularity of data transmitted increases exponentially, and the stakes if these fall in **wrong hands** become **even higher**.
- A recent HP study found that **70%** of IoT-enabled devices are susceptible to **hacking**, adding yet more **urgency** to this issue.

Standardisation of connectivity

- Currently, only a **small number** of vendors have IoT solutions for **specific verticals**.
- The spread of vendor-dominated silos could effectively **hinder IoT growth**.
- Efforts to **unite connected devices** across manufacturers are still ongoing.

Processor limitations

- Increased CPU **intelligence** and device autonomy are required to **develop compelling IoT** products within **energy and security** expectations.
- **Cost** may also be a factor in the **equation**.

.

IoT Security Challenges

“IoT Devices to be foothold to gain access to corporate networks and cloud environments”

&

“lack of uniform security standards”

With billions of potentially vulnerable devices connecting to **corporate networks**, both the motivation and abilities of **malicious attackers** will increase greatly over the next decade.
Attacks affecting IoT devices have already been demonstrated, such as the ability to gain access to **internet-connected cars**.

Earlier this year, devices provided by **insurance** companies to provide UM for drivers were found to be severely lacking in **security controls** and open to being exploited by attackers.

One of the basic challenges of IoT cybersecurity is the **lack of uniform security standards**.
This has resulted in the use of multiple operating systems and protocols, winch have proven to be **vulnerable** to cyberattacks.

The Federal Trade Commission decided against enacting regulation for loT device manufacturers, putting pressure on the industry **to regulate** itself and develop **secure** products that **protect** customer information.

IoT Security Challenges

The following are key cybersecurity concerns associated with loT technology:

Attack surface	Hackers can gain entry to a **corporate network** through an loT device.
Perimeter security	loT technology relies on **cloud based services**, so it will be challenging to **implement** effective perimeter defenses.
Privacy concerns	The **pervasiveness** of loT data collection coupled with **advanced analytic** capabilities could potentially result in consumer **privacy violations.**
Device management	Many loT devices currently **do not support implementation** of strong security controls. Additionally, as the **rapid** growth of loT devices expands the attack surface, organizations will face challenges in maintaining a **security baseline**.
Third party risk	Due to the **interconnectivity** of loT systems and the transmission of data through multiple service providers, it is increasingly difficult to identify exposure in the event of a security incidents
Regulatory Compliance	Organizations that do not clearly understand the legal and regulatory **implications** of their IoT usage could be in **violation** of laws and regulations.

Recommended security practices

1. Intel announced that it is developing the **Intel IoT Platform** to **unify** and **simplify** connectivity and **security** of IoT devices.

2. A consortium of **170 companies** across multiple industries formed the AllSeen Alliance to develop a **software framework** for loT technology.

   The framework seeks to make IoT devices **interoperable** by **standardizing** the ways that IoT devices are connected

3. The Cloud Security Alliance's **Mobile Working** Group, an organization of companies from various industries that promotes the use of best practices for cybersecurity in cloud computing, released **security guidance** for organizations developing or **deploying IoT** devices.

   The **guidance recommends** layered defenses to address the various threats associated with loT usage.

Recommended security practices (cont.)

"platform to unit"

"Standardising framework"

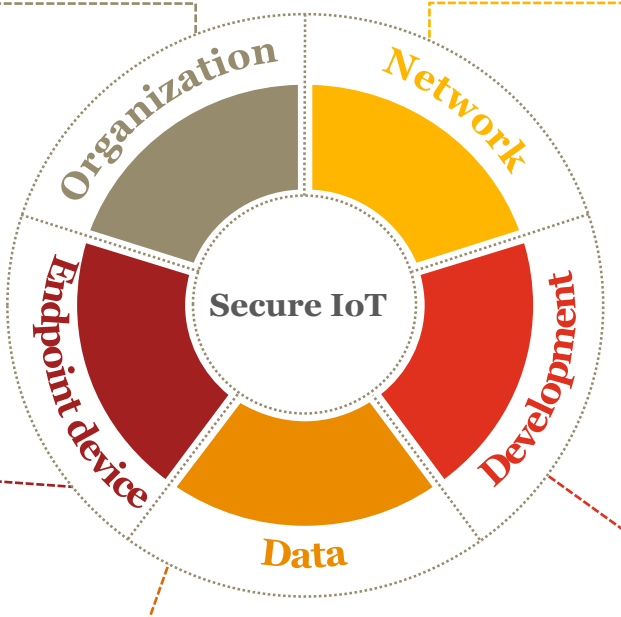
"Universal security guidance"

In order to enhance the cybersecurity programs to cover loT-related challenges, organizations should focus on:

- *Applying secure design concepts during the development of loT products*
- *Extending existing security operations to include the unique aspects of IoT technology*
- *Updating compliance programs to meet loT-related regulatory obligations.*

Security consideration for IoT products

- Understand the legal and regulatory implications of collected data.
- Ensure contractual agreements are in place to protect confidentiality with third parties.
- Assess the impact of loT on risk posture.
- Train employees and customers on loT security.



- Implement trust zones in the network to minimize risk from compromised devices.
- Perform a comprehensive system architecture review and threat analysis
- Determine how loT technology impacts existing network components.
- Extend existing security monitoring processes to include loT devices.

- Consider implementing device trust anchor control.
- Enhance operating system security through secure booting.
- Implement a firewall and host-based intrusion prevention system.
- Limit access to the network to the minimal level to allow normal functioning

- Incorporate secure coding standards during development of loT technology.
- Identify and remediate insecure cloud, mobile, and web interfaces.
- Implement strong authentication and authorization mechanisms.
- Perform penetration testing.
- Build behavioral profiles of devices and users, and monitor for anomalies.

- Implement strong data encryption algorithms.
- Extend existing data loss prevention programs to include loT devices and transmissions.

- Collection of personal information should be limited to identified purposes.
- Enhance data privacy programs to avoid violating privacy rules when data is aggregated.

Thank you

For further information on emerging technologies and risks please reach out to:

Vikas Sharma
Director-Advisory Consulting
PricewaterhouseCoopers Ltd (PwC)
v.Sharma@mu.pwc.com
+230-54973395