Internet of Things or Internet of Insecurity?

Barbara A. Grewe
Principal Policy Advisor
The MITRE Corporation

WORLD BANK GROUP

OASIS

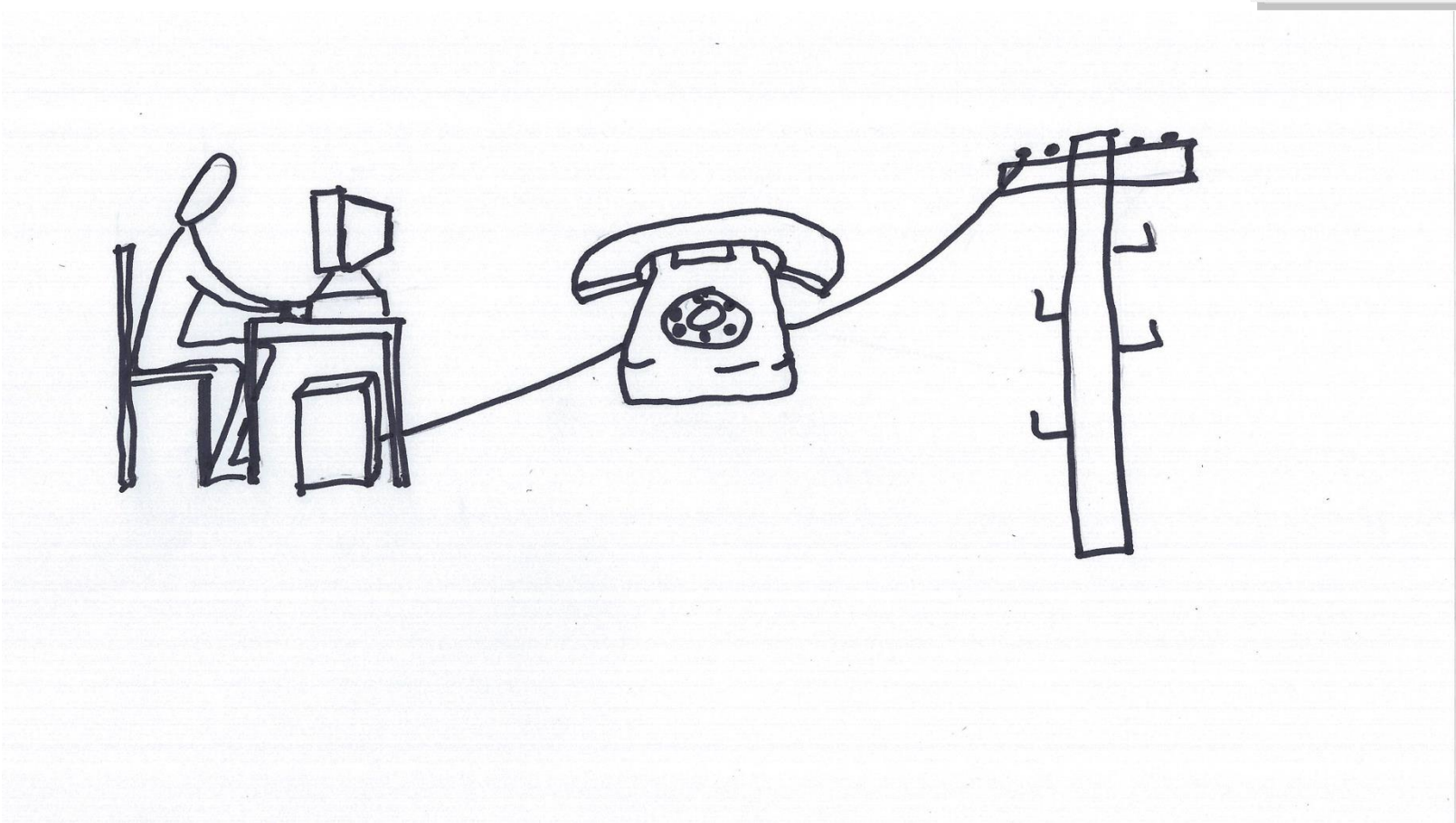
By the numbers

- Cisco predicts by 2019
  - 3.9 billion internet users
  - 24 billion network devices
  - 10.5 billion M2M devices

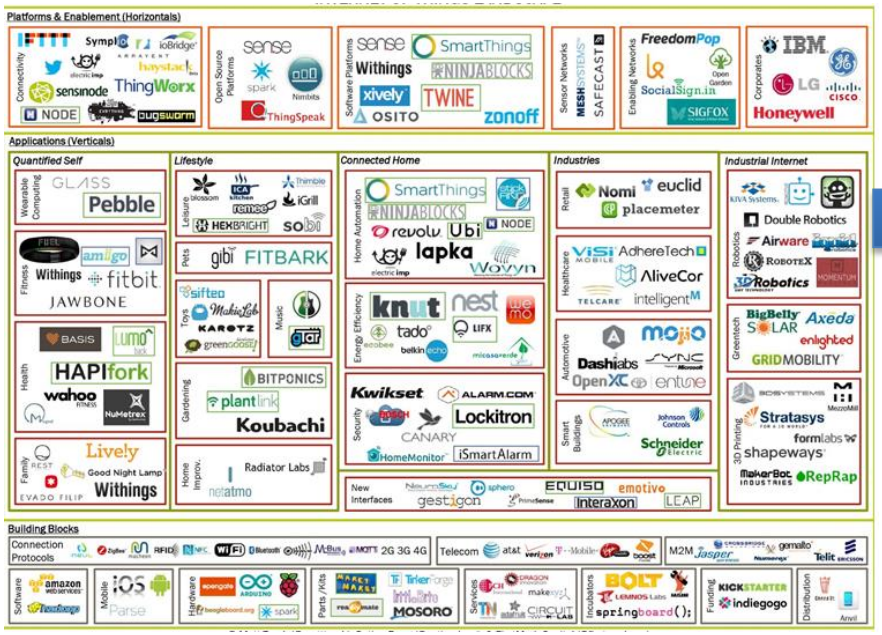
- Gartner predicts by 2020
  - 25 billion connected things
  - Utilities will be the top user, then manufacturing, then government

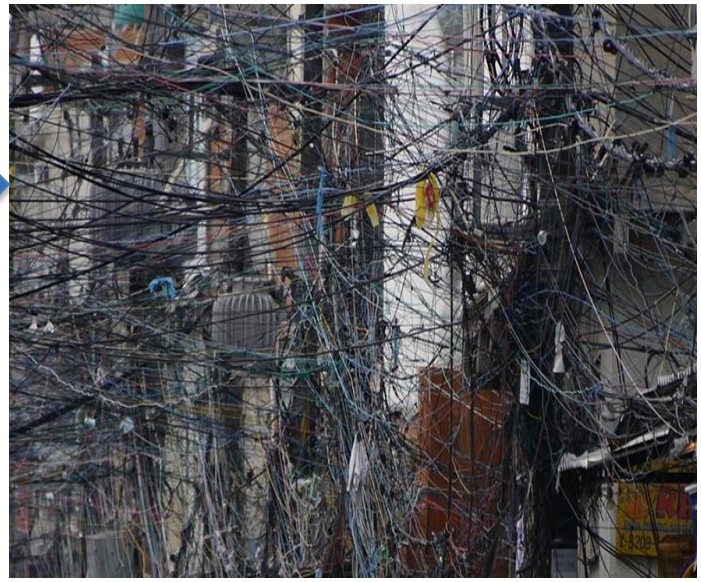
- IDC predicts by 2020
  - 29 billion Internet of Things (IoT) devices (just M2M)

It used to be simple (and slow)



Now its complicated (and fast)





Source: http://www.geek.com/apps/the-spies-in-your-living-room-70-of-smart-appliances-vulnerable-to-cyber-attack-1600725/

WORLD BANK GROUP

OASIS

What is the Internet of Things?

- The Internet of Things (IoT) is “a network of networks of uniquely identifiable endpoints (or "things") that **communicate without human interaction using IP connectivity**.”
  - A key attribute of this definition is autonomous connectivity so it does does not include smartphones, tablets, or PCs.

Source: International Data Corporation (IDC), Press Release, “Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC,” June 2, 2015

- Another view emphasizes that the IoT is physical, connected, and smart:
  - **Physical**: It is, at its essence, everyday devices used by people and organizations to manage their lives and business.
  - **Connected**: Networks connect devices to each other and to shared data and processing services. They also connect their users to one another.
  - **Smart**: Devices, services, and even networks **continually sense, share, and analyze data and information** to enable autonomous or semi-autonomous action.

Source: AFCEA International Cyber Committee, “The Security Implications of the Internet of Things.”

Security implications

- Whole new threat surfaces
- Moving beyond data protection to physical consequences
- Machines acting autonomously – when to escalate to a human?
- Redefined trusted relationships

Real Consequences

- **500 million records**: In the 12 months prior to October 2014, 500 million financial records have been stolen by hackers, according to the FBI. The FBI reported that approximately 35% of the data thefts were from website breaches, and 22% were from cyber espionage.
- **Time is money**: Delayed response may cause increased losses. Target was infiltrated for five weeks before recognizing the problem. Home Depot, was infiltrated over five months before the home improvement retailer discovered the breach. JPMorgan was hacked in June but didn't detect the attack until August.
- **Consequences will only get more serious**: According to the Ponemon Institute, the cost of successful cyber attacks increased to $20.8 million per financial services company in 2014. But as more things get connected it is lives not just money on the line.

Privacy Landscape

Intentional Disclosure	Tacit Approval Disclosure	Illegal Disclosure	Private Undisclosed
			
Facebook Instagram Twitter	Spotify Fitbit	Hacked Data	The Last Frontier?

Privacy Revisited

- Has big data analytics made the concept of privacy a new age dinosaur?
- Who owns YOUR data? (answer – often not you)
- Right to be forgotten? By whom?
- Responsibility for protecting privacy of data?

Liability Implications

- Can a machine have intent?
- No perfect software or security so who responsible when it fails?
- Duty to warn?
- Duty to respond to notice?

Evolving Legal Landscape

Wyndham decision – key aspects

- Allowed storage payment card information in clear readable text
- Failed to monitor system for malware used in previous intrusion
- Did not use common methods to require user ids that are difficult for hackers to access
- Did not use readily available security measures such as firewalls, to limit access between and among hotel property management systems, the Wyndham network, and the internet
- Failed to employ reasonable measures to detect and prevent unauthorized access to computer network or to conduct security investigations

What Can You Do?

- Bake in security from the outset
- Have better system hygiene – individually and organizationally
- Use data to your advantage
- Information sharing
- Develop consistent international standards – cyber seatbelts