# Managing a Cybersecurity Risk in the Medical Devices Industry

AJ-Great Limited

By Dr. Maria Lai-Ling Lam and Kei-Wing Wong

Sponsored by AJ-Great Limited
(global-trade@aj-great.com.hk)

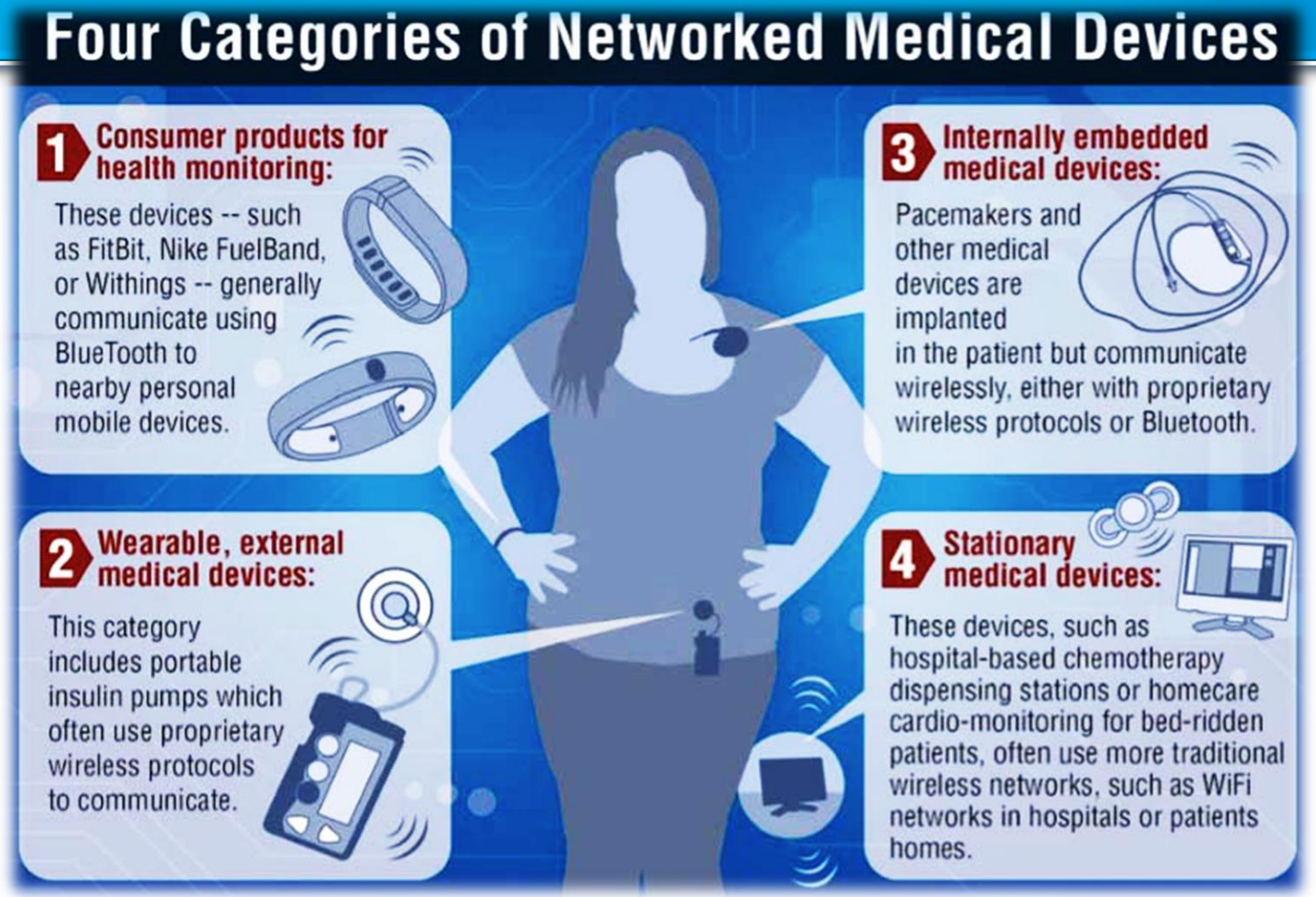
CPCE Health Conference at Hong Kong Polytechnic University in 2017

Calvin College

# Agenda

- Introduction
- Cybersecurity risk in the interconnected medical devices
- Research Questions
- Methodology
- Findings
- Implications

# The health care internet of things: rewards and risks




(source: Jason Healey, Neal Pollard, and Beau Woods (2015).

# ECRI 2016 Top 10 List

10

Misuse of USB Ports Can Cause Medical Devices to Malfunction

Plugging unauthorized devices or accessories into USB ports on medical devices can cause the medical devices to malfunction. Direct effects on medical device operation—for example, causing a physiologic monitor to reboot—have been observed in clinical practice.

Possible problems include instances in which:

- The device shuts down, and the patient does not receive therapy.
- The device settings are changed or performance is compromised.
- A patient monitor ceases to monitor the patient or fails to alarm for problems that require attention.

Uncontrolled access to medical device USB ports could also lead to a security breach, putting the patient's data and the healthcare facility's systems at risk.

Facilities need to develop and implement a policy on the appropriate use of USB ports on medical devices.

**Source: Tood Cooper (2016). Medical Devices Cybersecurity: From Best Practices to Standards**
http://ceitcollaboration.org/docs/Cyber-Security-Part-II.pdf

# Cybersecurity: A growing concern

In 2016, Johnson & Johnson (NYSE:JNJ) became the first medical device manufacturer ever to warn customers about a hacking threat. Meanwhile, St. Jude Medical (NYSE:STJ) saw its stock plummet after allegations that their cardiac devices had serious security vulnerabilities.

**Source: Top Medical Device trends for 2017**

**http://investingnews.com/daily/life-science-investing/medical-device-investing/top-medical-device-trends**

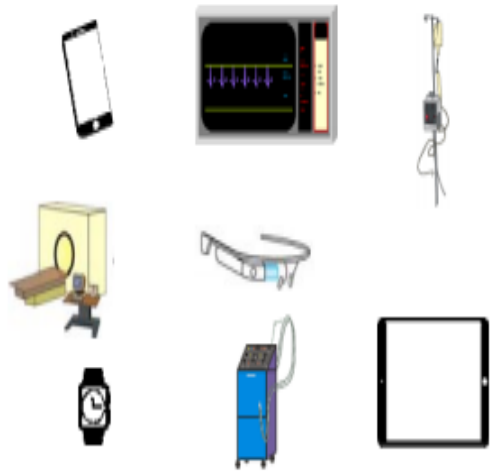
# Research Questions

1. What factors led American medical devices manufacturers not to invest in cybersecurity management?

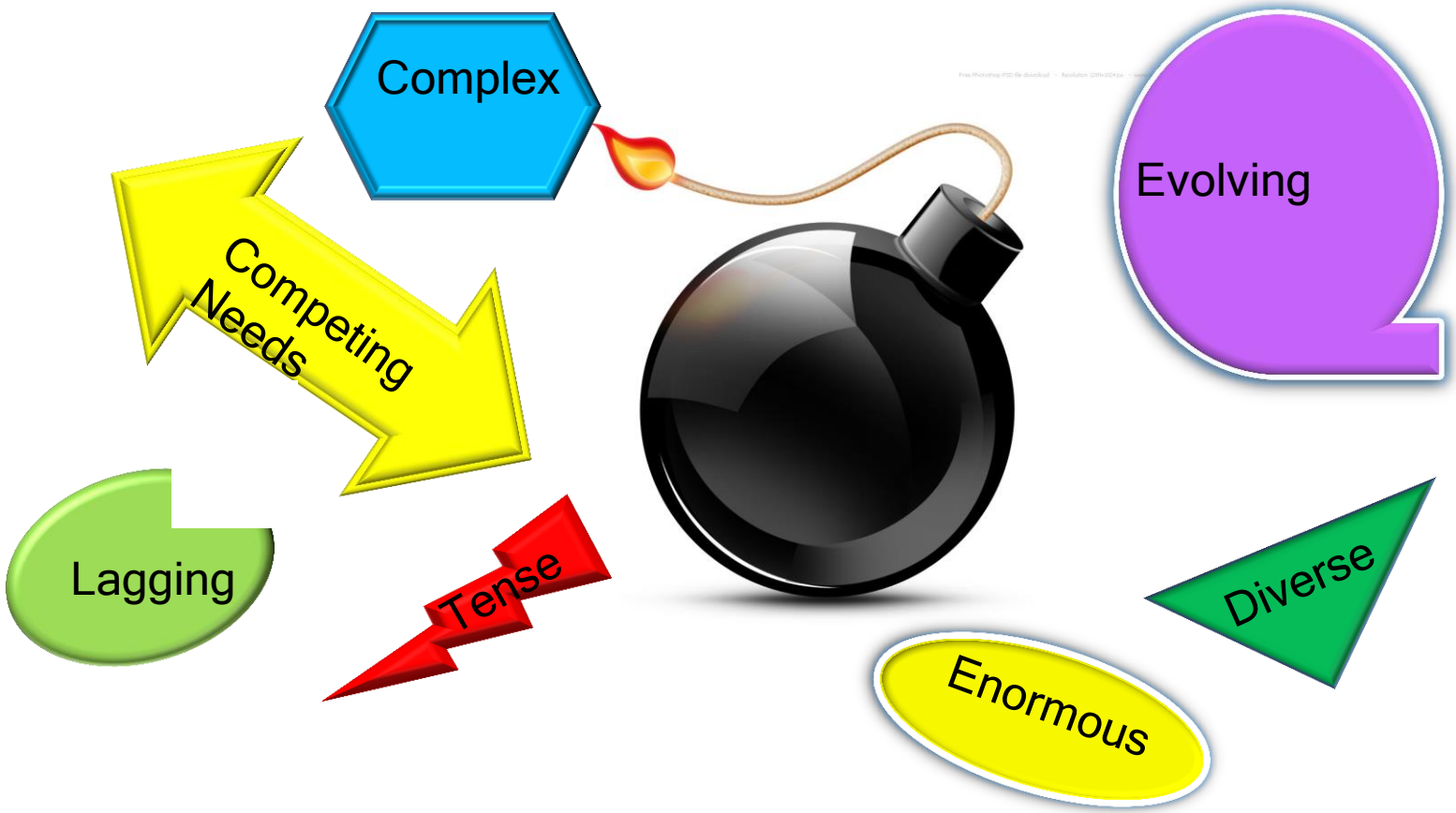
2. Under what conditions will these manufacturers develop their cybersecurity capabilities and increase their digital global competitive advantages?

# Methodology

1. Literature Review
2. Medical Trade Shows in China, Germany, Israel, and U.S. during 2013 to 2016
3. Interview manufacturers, supply chain partners, and health care providers in the international trade shows and Hong Kong.
4. Review Key Medical Devices Manufacturers' documents



# High Uncertainty and Complexity in the Medical Devices Ecology



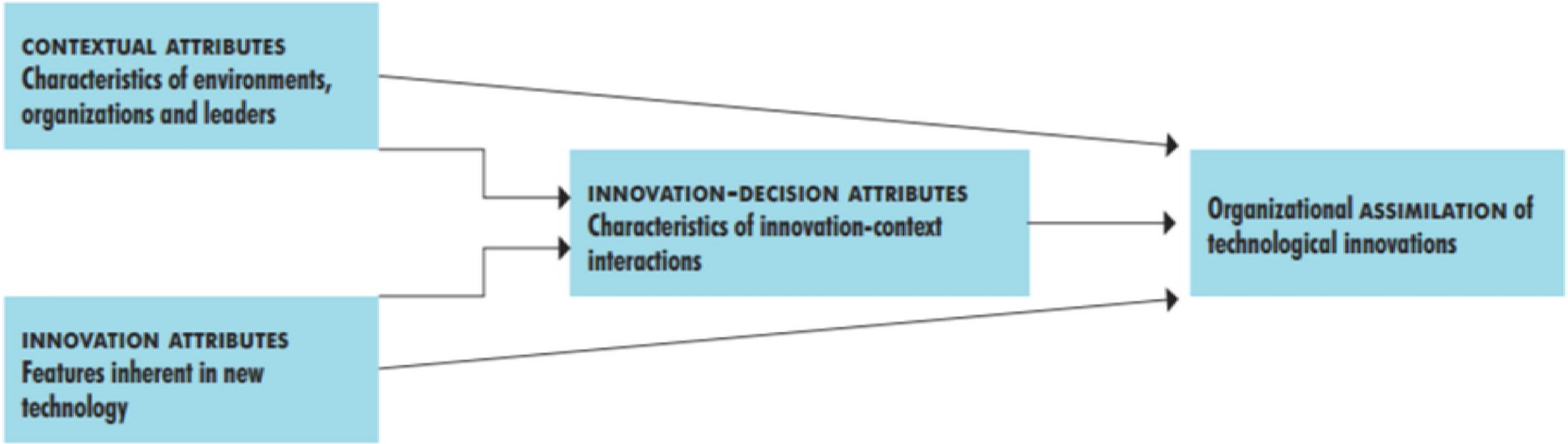

AJ-Great Limited

Source: https://www.youtube.com/watch?v=d9RUHXWWiO8

# What factors led American medical devices manufacture not to invest in cybersecurity investment?

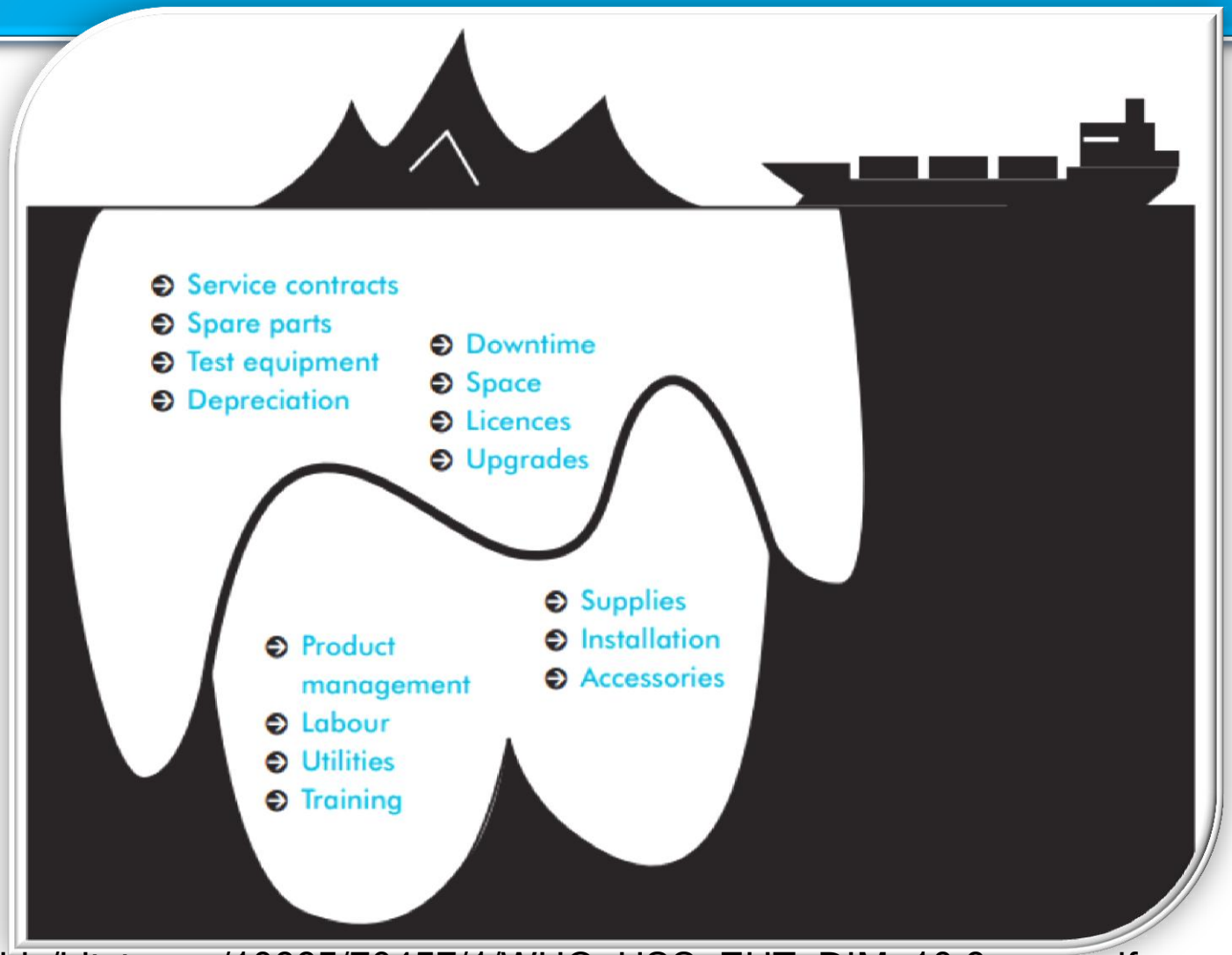
1. Product-oriented Innovation
2. Short life-span for a new product
3. Lack of incentives for management of many players for the security of patients (gap, culture, competence)
4. High cost for the assimilation of Innovation and hidden cost of medical devices.
5. Developing countries–low quality, high volume, different regulations and infrastructure

# A model of innovation assimilation




Source: WHO (2010). Barriers to innovation in the field of medical devices http://apps.who.int/iris/bitstream/10665/70457/1/WHO_HSS_EHT_DIM_10.6_eng.pdf

# Hidden Cost of Medical Devices




Source:
http://apps.who.int/iris/bitstream/10665/70457/1/WHO_HSS_EHT_DIM_10.6_eng.pdf

# Summary: Problems in the System of Medical Devices Industry

I. Conflicted Interests of Multiple Players in the Medical Devices Ecology

II. Quick Innovation

III. High Quality at a lower cost

IV. UnHarmonized Regulations

V. Uncertain and Emerging Medical Services Security

# Under what conditions will these manufacturers develop their cybersecurity capabilities and increase their digital global competitive advantages?

- ✓**Be Proactive, Open, Collaborative**
- ✓**Develop social capacities for resilience and reflections.**
- ✓**Incorporate medical devices as fully as possible into current evolutionary flow of infrastructure security capabilities**
- ✓**Set up learning platforms and experimenting**
- ✓**Develop standards for the industry**
- ✓**Increase users' awareness**

# Core Principles For Improving Critical Infrastructure Cybersecurity

- What processes and assets need protection?
- What safeguards are available?
- What techniques can identify incidents?
- What techniques can contain impacts of incidents?
- What techniques can restore capabilities?


Source: http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM420828.pdf

# Thank you for your listening!


Please contact Dr. Maria Lam (global-trade@aj-great.com.hk)
Or dial 852-24125116