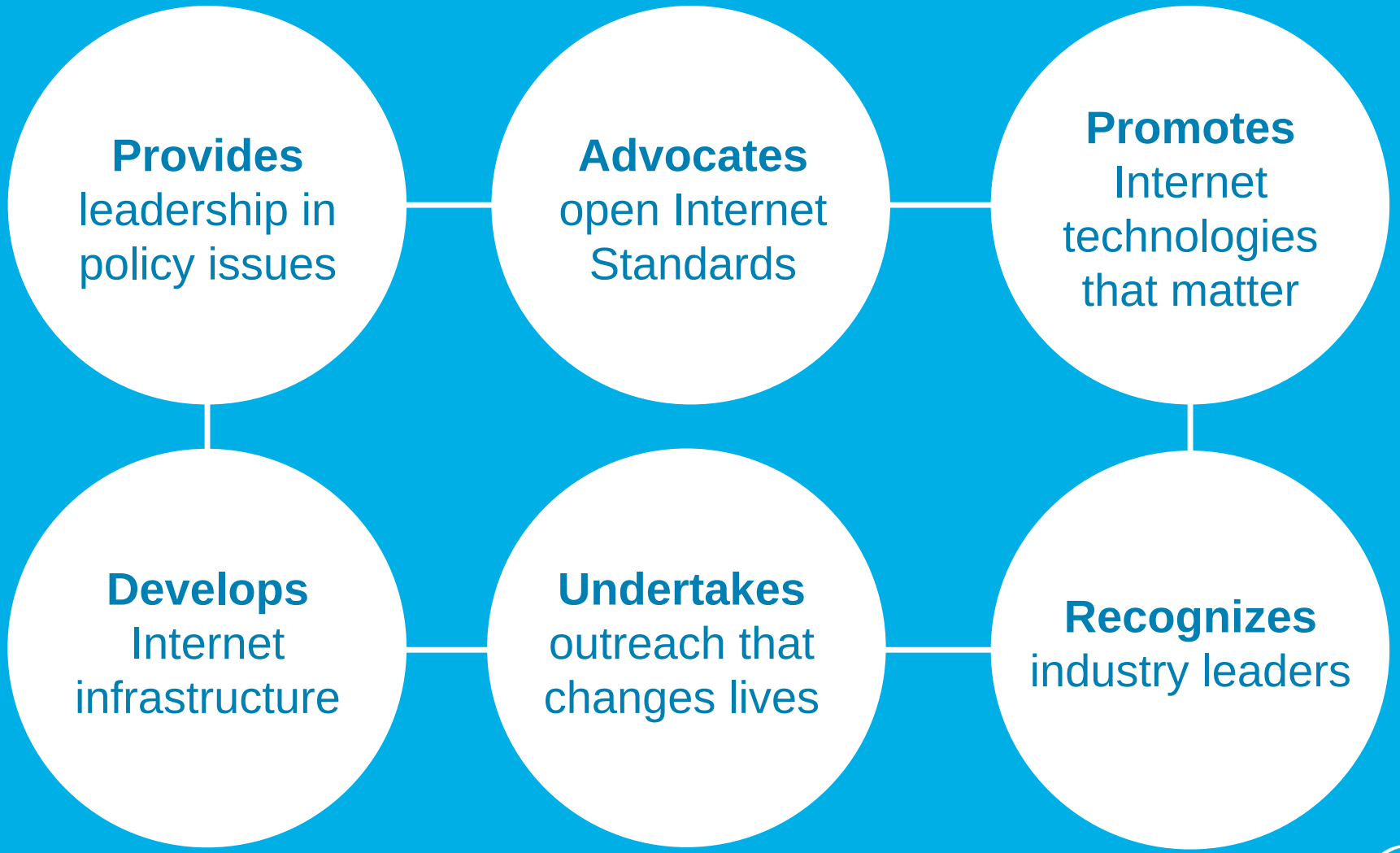

Internet Society
Collaborative Security and the IoT era

Our Mission

To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.

Internet Society

The Internet Society at Work



Global Presence

110
Chapters Worldwide

78k+
Members and Supporters

146
Organization Members

5
Regional Bureaus

20
Countries where ISOC staff are present

Asia-Pacific

20 Chapters

Australia
Bangladesh Dhaka
Hong Kong
India Bangalore
India Chennai

India Delhi
India Kolkata
India Trivandrum
Indonesia Jakarta
Japan

Malaysia
Nepal
Pacific Islands
Pakistan Islamabad
Philippines

Republic of Korea
Singapore
Sri Lanka
Taiwan Taipei
Thailand

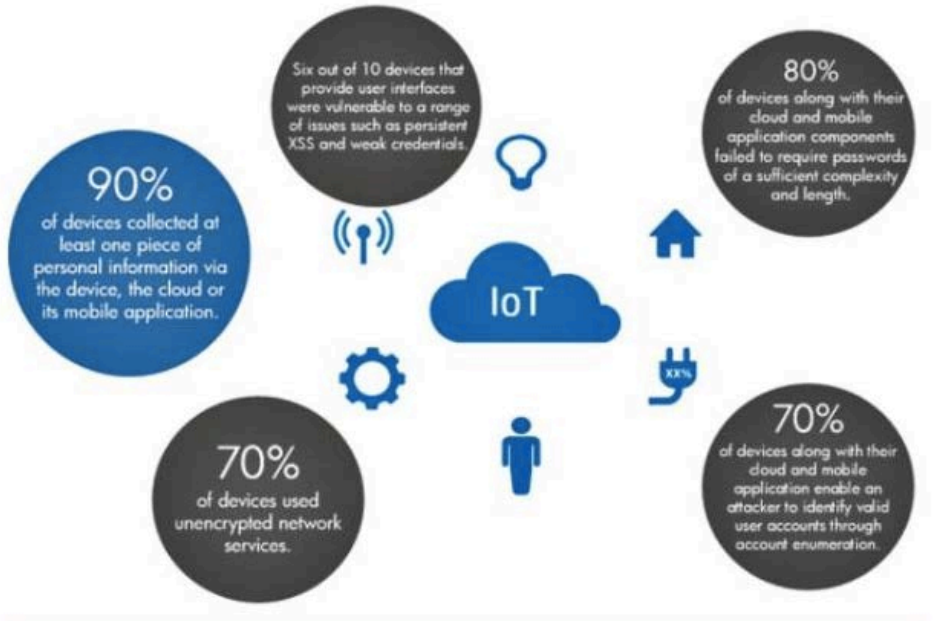
The Internet of Things in APAC

- Gartner estimates that there will be 25 billion connected ‘things’ by 2020
- By 2025, there is expected to be 26 fully operational smart cities globally. In APAC, Singapore, China and South Korea are among those actively pursuing smart city development
- The proliferation of connected devices, networks, platforms and applications understandably translates to more vulnerabilities and potential for malicious attacks

Source: iotsecurityevent.com

Security and IoT

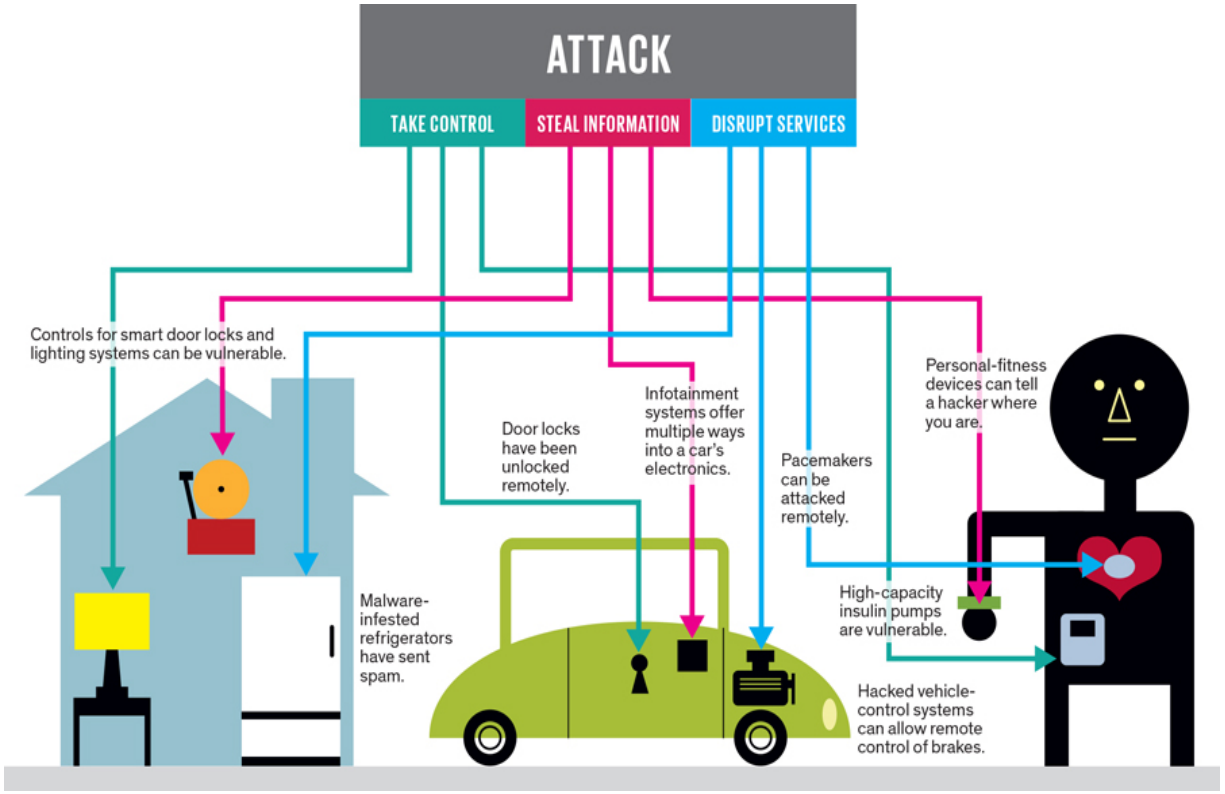
A recent HP study reported that the average IoT gadget has 25 security flaws, and 70% have at least one vulnerability



Source: Hewlett Packard

Security and IoT – its also going to get personal

Many of the risks that we will encounter may be addressed by existing solutions, but many will also require new approaches by various stakeholders



Source: IEEE

Current and Emerging Trends tell us there is…

Increased centralisation of data

Machine-to-machine connectivity intensifies data collection and aggregation → bulk of this data is about users

Such a surge in the volume of centralised data is bound to have a profound impact on individual privacy

Increased third party mediation

IoT gives rise to models and approaches that undermine human agency

The devices that we use for specific tasks may be doing other things without our knowledge or consent, but which could affect us directly or indirectly

With IoT, much of our offline activities could be digitally mediated as well

Growing diversity of non-human agents

More and more day-to-day decisions can (will?) be made using algorithms

The algorithms will increasingly be adaptive—and capable of autonomy

This can pose further challenges to our awareness of - and control over - what our devices gather and share about us

As connected machines start to ‘talk’ to each other, it will increasingly be difficult to maintain separate online personas

Five elements of Collaborative Security

Internet Society

Number 1

Preserving opportunities and building confidence

Traditional approaches to security were mainly concerned with external and internal threats, and the impact they may have on one's own assets

The Internet enables opportunities, for human, social and economic development on a global scale –this can only be realised if users trust the Internet enough to use it for their needs and innovations

The objective of security is to foster confidence in the Internet, rather than simply to prevent perceived harm

Internet Society

Number 2

Collective responsibility

As networks are interconnected and interdependent, one stakeholder acting alone can make little difference, even in protecting its own resources

Internet security depends not only on how well participants manage security risks they face, but also, how they manage security risks that they may pose to others

Number 3

Security solutions should be fully integrated with rights and the open Internet

Any security solution is likely to have a positive or negative effect on the Internet's operation and development, as well as user's rights and expectations

It is crucial that these solutions do not degrade the Internet's fundamental properties--its integrity, accessibility and global reach—which have made it such a valuable global resource

Internet Society

Number 4

Security solutions need to be grounded in experience and evolutionary in outlook

Security solutions need to be flexible enough to evolve over time, as technology changes and threats adapt

New efforts and solutions that build on “lessons-learned” make the Internet more resilient to threats

A collection of incremental solutions may be more effective in practice than a grand design

Internet Society

Number 5

Targeting the point of maximum impact

Security requires different players (within their different responsibilities and roles) to take action, closest to where the issues are occurring.

Typically, for greater effectiveness and efficiency, solutions should be defined and implemented by the smallest, lowest or least centralized competent community

…at the point in the system where they can have the most impact

Points to ponder

- Security in IoT is more complex than in existing networks and applications: At the device and sensor level, the challenge is around identification, authentication and authorisation; at the networks, the risks are mainly at the interface between systems
- There are at present many initiatives to secure different parts of the IoT, but there needs to be more joined up approaches to fostering trust, and ensuring end-to-end security
- IoT cuts across different sectors and platforms, underlining the need for cooperation and joint action by all those involved
- Many of the devices that will make up IoT will be dedicated and designed to perform specific tasks, but also embedded in more complex networks. Security solutions thus need to be specialised, but also flexible to protect diverse and dynamic systems

Rajnesh Singh

Regional Director, Asia-Pacific

singh@isoc.org

INTERNET SOCIETY ASIA-PACIFIC

9 Temasek Boulevard
#09-01 Suntec Tower Two
Singapore 038989

T: +65 6407 1470
F: +65 6407 1501
E: apac@isoc.org

Follow us on Twitter: twitter.com/isocapac
Follow us on Scoopit!: www.scoop.it/t/internet-in-asia-pacific
Read our blog: www.internetsociety.org/blog/asia-pacific-bureau