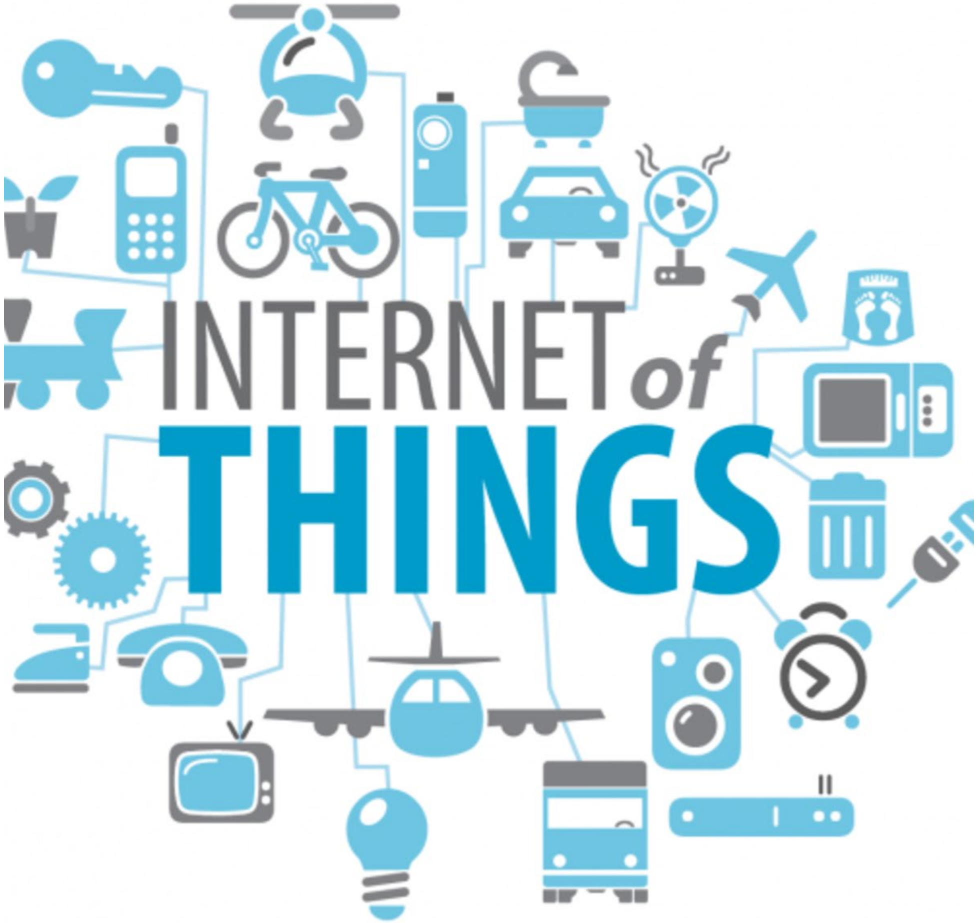
How IoT is Changing the Cybersecurity Landscape

Tahseen Ahmad Khan

Vice Chair, UN/CEFACT



Cyber Security in IoT

- IoT is a network of physical objects that contain embedded technologies to communicate and sense or interact with their internal states or external environment
- IoT is leading change in the digital landscape and is fast becoming a must have element of business technology
- Some areas where IoT is already playing the role of a change agent

Smart Cities

Innovations to improve quality of life in cities encompassing energy, water, environment, security management

Smart Manufacturing

Automation in factory, logistics, transportation, asset monitoring, supply chain management, resulting in improved efficiency

Smart Mobility

Urban mobility and transportation solutions for reliable transportation

Smart Agriculture

Farming solutions that aid in better yield management, trace and track, environmental monitoring and disaster control

While connected network of devices offers huge benefits in creating business opportunities, they open themselves to cybersecurity risks

Rise of Cyber Security Threats

70% of commonly used IoT devices contain vulnerabilities

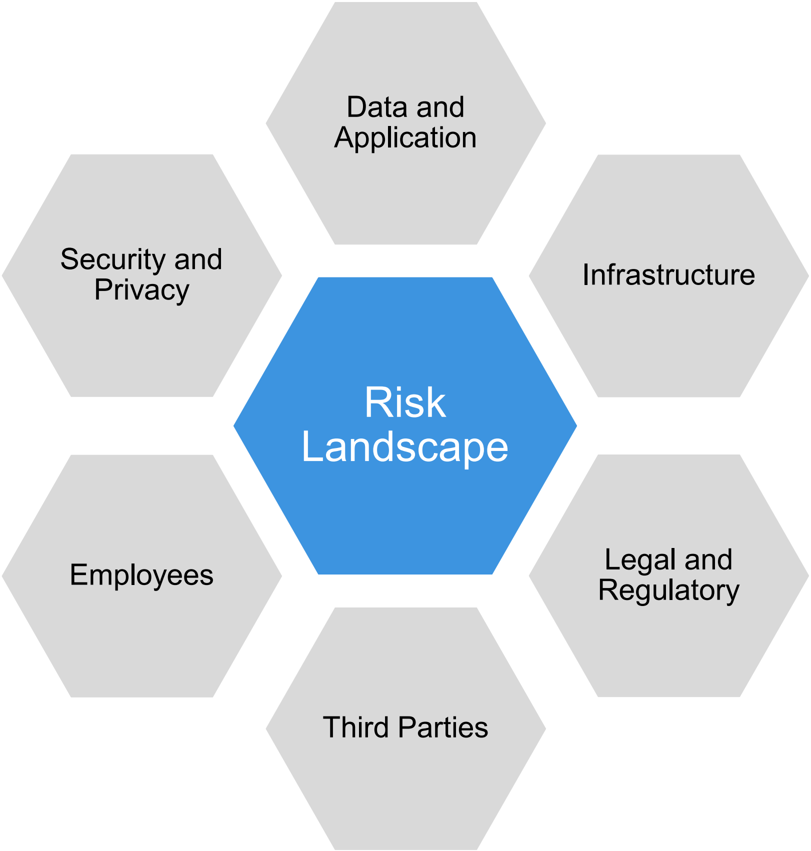
HP study - http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

56% of respondents say that its unlikely that their organization would be able to detect a sophisticated attack

EY Global Information Security Survey

- Cybersecurity is a business issue and not just a technology risk
- Mobile, IoT, Public Clouds are pushing boundaries of trust and risk monitoring
- People, Platforms, Processes, Things play a critical role in extending this trust boundary
- Governance and compliance issues are becoming complex as borders become blurred

The changing risk landscape



For an organization to effectively manage risk in an IoT ecosystem, it needs to clearly define the limits of that ecosystem

Top Cybersecurity Challenges in IoT

- Infrastructure
  - Cyber security attackers are moving out of attacking through conventional systems to attacking through power grids, transportation systems etc
- Cloud Computing
  - Cloud computing while a necessity for large volume data processing from IoT devices could be a single point of risk if their infrastructure fails to keep up the evolving cyber security landscape
- Governance and Compliance Issues
  - With changing legislation, data retention policies and expanding ecosystem, setting governance standards will become a complex affair, more so if it is cross border
- Privacy and Data Protection
  - All smart devices hold information about institutions ranging from their Trade secret, to individuals about where they work to what is their engagements. IoT presents an opportunity for aggregation of data and for behavioural targeting for commercial reasons. Where should the line be drawn?

UN/CEFACT IoT Whitepaper Project

- Cybersecurity as an issue only gets complex in the context of IoT for Trade Facilitation with the convergence of IoT (sensor data), AI (intelligence on data) and Blockchain (distributed storage of data)
- At UN/CEFACT, we have launched a Whitepaper project to focus on standards, processes and cybersecurity issues relating to IoT
- As part of our work programme, cyber security is a critical focus across our projects
- Governments, Public and Private sector organizations must stay ahead of the game with threat detection capabilities so they can respond appropriately and proactively
- We have also undertaken work on an international convention on for Trusted transboundary electronic interaction/mutual recognition mechanism

International Convention – Mutual Recognition

- Mutual recognition is an important issue in the context of electronic communication. The scope of this could extend even to IoT systems
- An intergovernmental international convention is required to facilitate cross border mutual recognition
  - Currently, efforts around mutual recognition are regional or domain specific – UN/ESCAP Paperless Trade Agreement, Bi-lateral or Multi-lateral agreements
  - UNCITRAL text addresses some of the issues
  - As a result of this, a lot of cross border trade still continues to rely on paper
- Progress so far
  - Whitepaper exploring principles of trusted transboundary electronic interaction prepared and approved by Bureau
  - Position Paper highlighting need for international convention prepared and finalized
    - Highlights benefits of cross border trade
    - Regional efforts around mutual recognition and need for framework convention
    - Assessment of Impact

International Convention – Mutual Recognition

- Next Steps
  - Study existing instruments and cooperate with other organizations, expert members to understand effectiveness of existing instruments
  - Define how UN/CEFACT's work through an international convention can facilitate progress in enabling mutual recognition
  - Prepare proposal document and project highlighting necessity for International Convention

Thank you

takhan@meity.gov.in