India – Japan Emerging Tech initiative

Cyber Technologies for Security

IoT Security – Initiatives taken in TEC/ DoT, India

March 22, 2024

Sushil Kumar

Additional Director General Telecom

Department of Telecommunications (DoT)

Government of India

M2M/ IoT – need of Cyber security

- IoT / M2M technology is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety, Surveillance, Health care, Agriculture, Smart homes, and Smart cities etc.

- World Economic Forum (WEF) in its report titled Future of Connected World released in June 2022 mentioned that

    - there was an increase in Cyber attacks by 31% in 2021 as compared to 2020.

    - IoT device attacks became double in the first half of 2022 as compared to 2021.

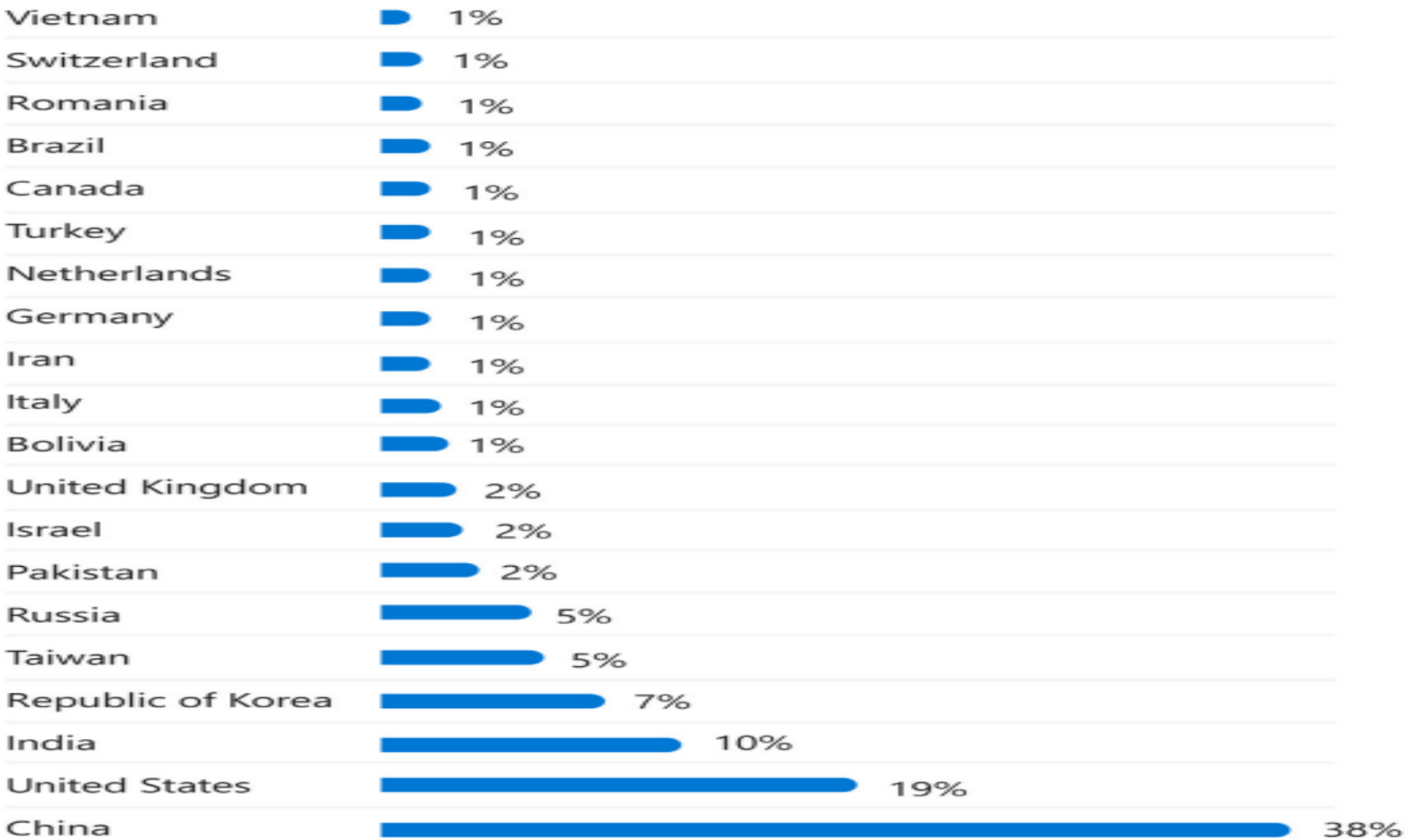
    - US $ 1.85 Million average recovery cost for mid sized companies to recover from cyber attacks

- Security of the IoT domain, from devices to the applications becomes a matter of paramount importance as hacking of the devices / network being used in daily life will harm companies, organisations, nations and more importantly people

Threats to IoT devices

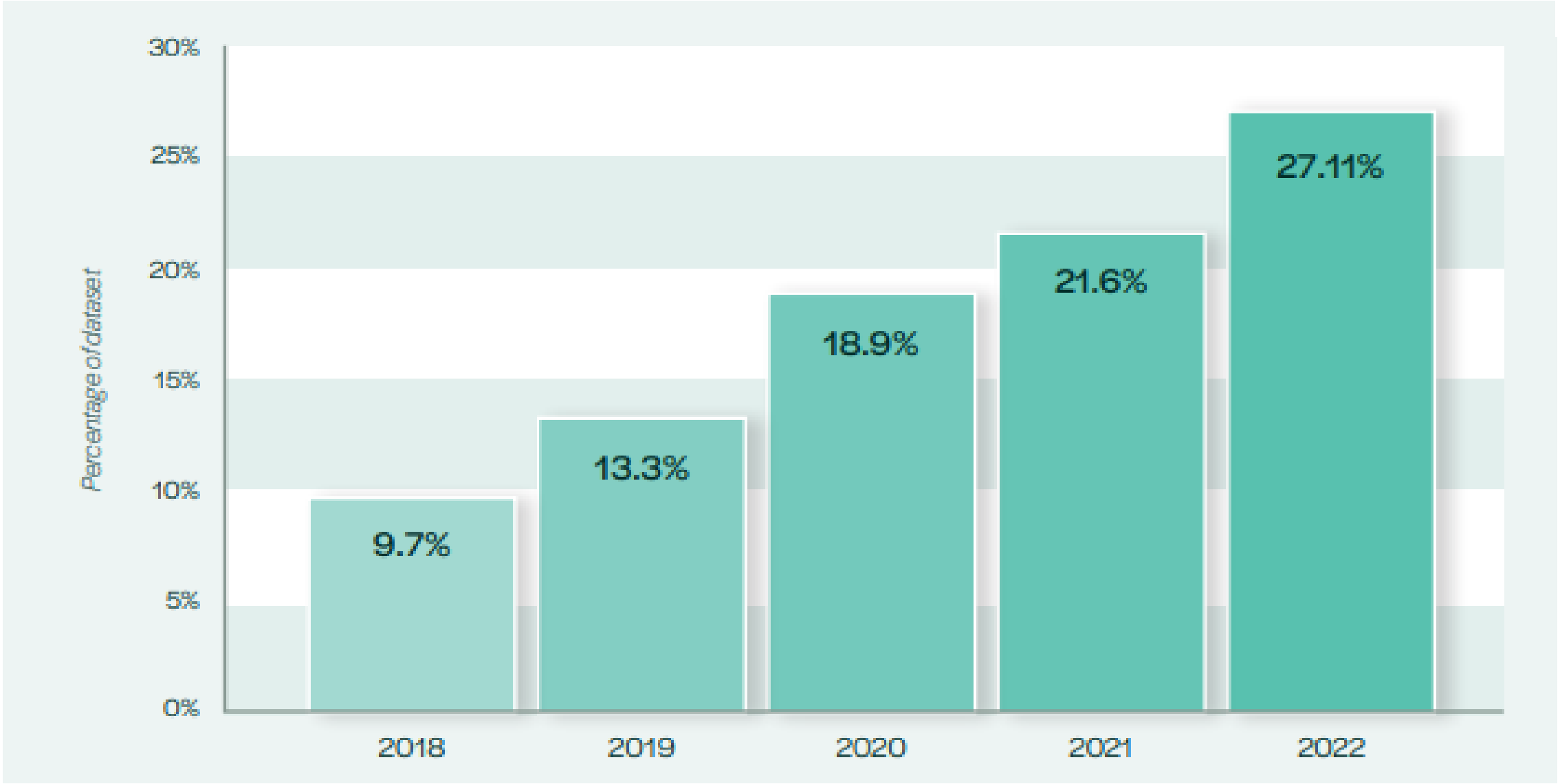
- IoT devices may become vulnerable due to various type of threats, some of them are as:
  - Weak user credentials
  - Insecure Firmware upgrade or Outdated Firmware
  - Malware
  - Use of weak encryption algorithm
  - Device modification
  - Lack of Physical Hardening

Top countries originating IoT malware infection during 2022



Source: Cyber signals, Dec 2022

Vulnerability Disclosure statistics



Source: IoTSF

DoT policy initiatives on M2M/ IoT & 5G

- **National Digital Communication Policy (NDCP)-2018** released by Department of Telecom (DoT) in 2018. Some of the salient features available in this policy are:
  - Creating a roadmap for emerging technologies and its use in the communications sector, such as **5G, Artificial Intelligence, Robotics, Internet of Things, Cloud Computing and M2M**
  - Establish a multi-stakeholder led collaborative mechanism for coordinating transition to Industry 4.0
  - Developing market for IoT/ M2M connectivity services in sectors including Agriculture, **Smart Cities, Intelligent Transport Networks, Multimodal Logistics,** Smart Electricity Meter, Consumer Durables etc. incorporating international best practices
- National Telecom M2M Roadmap released in 2015.
- M2M Service provider registration policy released in Feb 2022.
- Telecommunication Engineering Centre (TEC), technical wing of DoT is working in M2M/ IoT domain since 2013 for finalizing specifications in sync with global SDOs.

TEC / DoT initiatives on M2M/ IoT security

- While working as DDG(IoT) in TEC (2013- Oct 2023), developed & released twenty one technical reports (TRs) in multi stake holders working groups and in sync. With global SDOs. These TRs are in M2M/ IoT domain covering various verticals, communication technologies, EMF radiation from IoT devices and IoT Security. Several recommendations of these TRs have been used in the development of policies / standards and a lot in process. Available on https://tec.gov.in/M2M-IoT-technical-reports

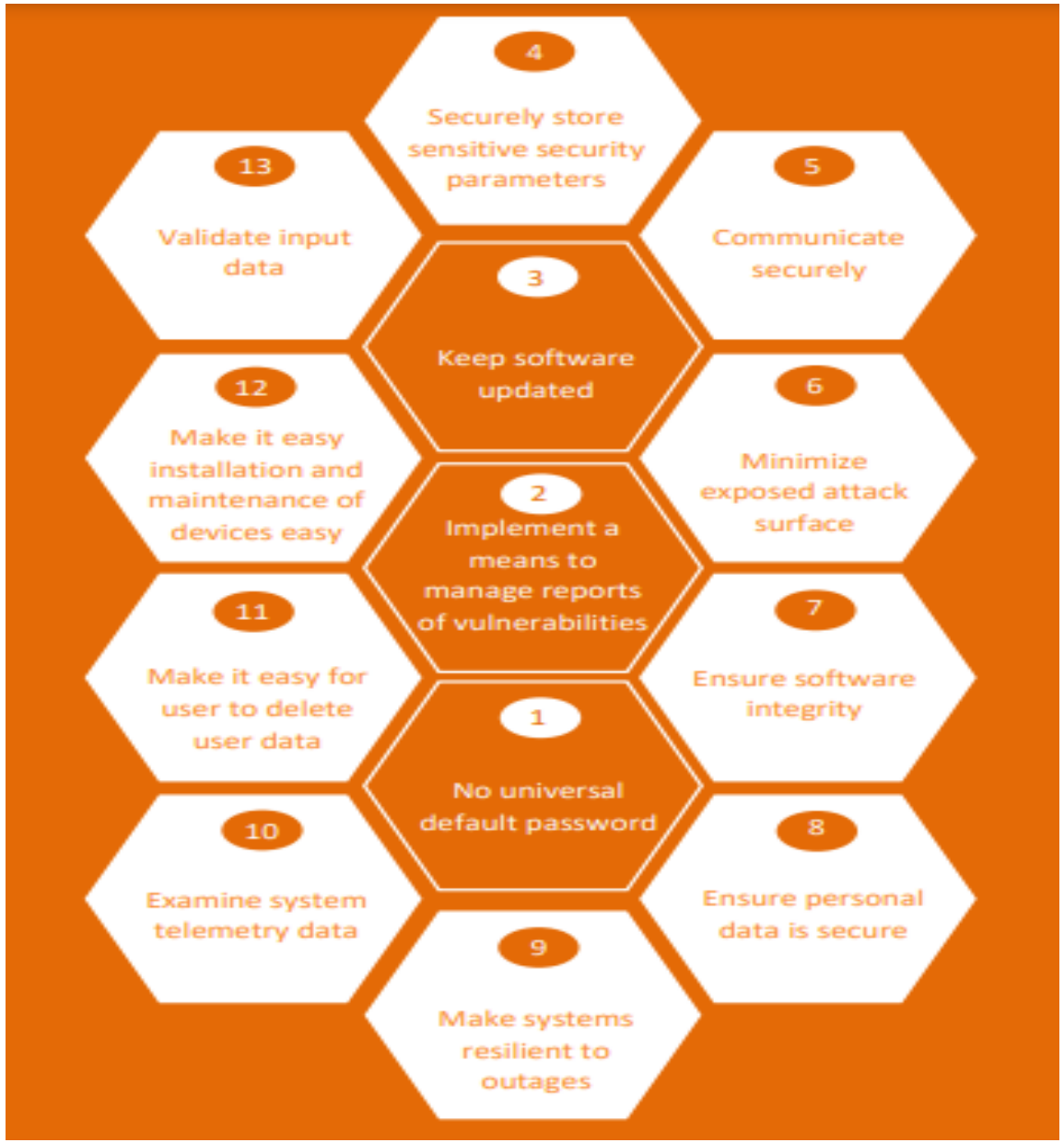
- Adopted oneM2M as well as 3GPP specifications as national standards for the development of standards based and sustainable eco system in the country.

- Out of twenty, following Technical Reports are related to IoT Security:

    1. *Security by design for IoT device manufacturers*, released in March 2023
    2. *Framework of National Trust Centre for M2M/IoT Devices and Applications*, released in March 2022
    3. *Code of Practice for Securing Consumer Internet of Things (IoT),* released in August 2021
    4. M2M/ IoT Security, released in 2019.

- Envisaging the importance of these technical reports, ITU has posted Six TEC Technical reports including the above three (1 to 3) on its global resource portal in IoT section (2023 – 2021) for the benefit of global community (https://www.itu.int/cities/dt-resource-hub/iot/) .

Code of Practice for Securing Consumer IoT, released by TEC in Aug 2021



➢ WEF Joint statement on consumer IoT Security released in Feb 2022

a. No universal default passwords
b. Implementing a vulnerabilities disclosure policy
c. Keeping software updated
d. Securely communicating
e. Ensure that personal data is secure

DoT, India has endorsed **Code of practice for securing consumer IoT** to all related stakeholders including M2M Service Providers (M2MSPs) to follow at least the first three guidelines.

TEC / DoT initiatives on M2M/ IoT security

- The technical report on ***Framework of National Trust Centre (NTC) for M2M/ IoT Devices and Applications*** released in March 2022 visualizes the implementation of national trust centre in a phased manner for managing/ addressing the vulnerability related issues of the IoT devices reported by IoT/ Smart city platforms working in the network.

  This project is being developed and expected to be implemented in near future..

- Technical Report ***Security by design for IoT Device Manufacturers*** released in March 2023, highlights various threats and challenges related to IoT device security; includes study of national/ international standards (by **ITU, ISO/ IEC, ETSI, ENISA, IoTSF, NIST, GSMA, 3GPP** etc.), best practices and guidelines (**UK DCMS, CSA Singapore, WEF, STQC** etc.) to mitigate these challenges. This report also provides recommendations for IoT device manufacturers and related stakeholders including policy makers, which will help in securing IoT ecosystem.

  Cyber Security labeling scheme is an important outcome of this technical report.

  Recommendations are being included in the security requirements being developed for testing & certification of the products.

Proposed IoT devices classification for India

Proposal for Device Classification						
Security Features	Security Requirements	Level-0	Level-1	Level-2	Level-3	Level-4
Confidentiality	Message Encryption	X	√	√	√	√
	Attack Protection	X	X	√	√	√
	Data Encryption	X	√	√	√	√
	Tamper Resistance	X	X	√	√	√
	Security Assessment Certificates	X	X	√	√	√
	Device ID Management (Physical/ Logical)	√	√	√	√	√
Integrity	Data Integrity	X	X	√	√	√
	Platform Integrity	X	X	√	√	√
	Secure Booting and Integrity Test / Self Test	X	X	X	√	√
Availability	Logging	√	√	√	√	√
	External Attack Prevention & Response	X	X	X	√	√
	Secure Monitoring	X	X	X	√	√
	Secure Firmware Update & Patch Update	X	√	√	√	√
	Software Assets Protection & Response	X	X	√	√	√
	Vulnerability Management & Response	X	√	√	√	√
	Security Policy Update & Response	X	X	X	√	√
Authentication/ Authorization	Biometrics	X	X	X	X	√
	User Authentication	X	√	√	√	√
	Data Authentication	X	X	√	√	√
	Password Management	X	√	√	√	√
	Access Control	√	√	√	√	√
	Device ID Verification	X	X	√	√	√

Security Assement and standard	Level-0	Level-1	Level-2	Level-3	Level-4
Meet Baseline Security Requirement					
Adherence to cyber security based on International Standards					
Adherence to the principles of Security by Design, and absence of known common software vulnerabilities					
Resistance against common cyber-attack and undergo for penetration testing					

Need of Cyber Security labels for IoT devices

- There are around 25 billions of IoT devices globally, which are expected to increase sharply in view of development of smart infrastructure in various verticals including smart cities.
- It is not practically possible to develop the testing requirements for every type / model of the devices as these may be in millions.
- Testing requirements may depend upon the risk associated / criticality of the application
- Proposed labelling scheme (L1 to L4) is in an increasing order of security requirements. These Labels / QR code may be printed on the device to create an awareness to the user about the security available in the device. NCCS Bangalore and IIT Hyderabad have adopted this labelling scheme in preparing IoT security specifications.
- Governments may assign/ change the security labels for particular devices as per need.
- Import / export may be linked with the security features available in the devices.

Some Recommendations on IoT Security

Recommendations available in **Security by design for IoT device manufacturers** are being considered to be the part of ITSAR/ other policy guidelines for the stake holders. These are H/W Security, S/W Security, Policy recommendation and Generic. Some of them are listed below:

1. First three guidelines of **Code of practice for Securing Consumer IoT** need to be mandated

    i. No universal default passwords
    ii. Implementing a vulnerabilities disclosure policy
    iii. Keeping software updated

2. IoT device manufacturer should test the devices against known vulnerabilities before launch in the market. To begin with critical devices and network elements such as IoT Gateway, Smart Camera, Wi-Fi routers, ONT etc. may be taken.

3. Life expired devices or the devices not getting updates may be highly vulnerable and threat to the network. Suitable policy mechanism is required to replace such type of devices.

Some Recommendations on IoT Security

4. Secure on boarding of IoT devices at the platform preferably using ITU-T X.509 standard for digital certificates

5. Platform providers are also the M2M/ IoT Service providers. All the M2M/ IoT Service providers should register with DoT. Other entities like M2M/ IoT device manufacturers, application providers, network providers etc. should also register on DoT portal.

6. Platform / NTC is expected to analyse

    - Average response time / patch release time for critical vulnerabilities by product
    - Percent/ number of products no longer receiving security updates in operation.

7. Consumer awareness regarding Vulnerabilities / security of IoT products.

8. Every consumer device should have a forced mechanism for changing the password by the user prior to its first use.

THANKS

For detail, pl. see the Technical Reports in M2M/ IoT domain, available on
www.tec.gov.in/technical-reports/

Sushil Kumar
Additional Director General Telecom,
Department of Telecommunications,
+919868131551
Sushil.kumar20@gov.in
sushil.k.123@gmail.com
in.linkedin.com/in/sushil-kumar-98895560