IoT Security and Consumer Trust

Dr. Hosein F. Badran

Digital Transformation and Innovation Consultant

hbadran@badranconsult.com

UN-ESCWA IoT Security , Beirut **Dec. 6th, 2018**

Key Points

- Rising usage of IoT Devices
- Trends in IoT Device Security and Privacy
- Canadian Multistakeholder IoT Security Initiative
- Recommendations

ISOC Consumer Survey

7 out of 10

own an IoT device

3 out of 4

plan to purchase an IoT device in the next 12 months

Consumers want to own IoT devices, but they are deeply concerned about their security and privacy

81% concerned about personal information being leaked

73% concerned about hackers taking control of device and using it to commit crime

72% concerned about hackers gaining access to personal information

71% concerned about being monitored without their knowledge or consent

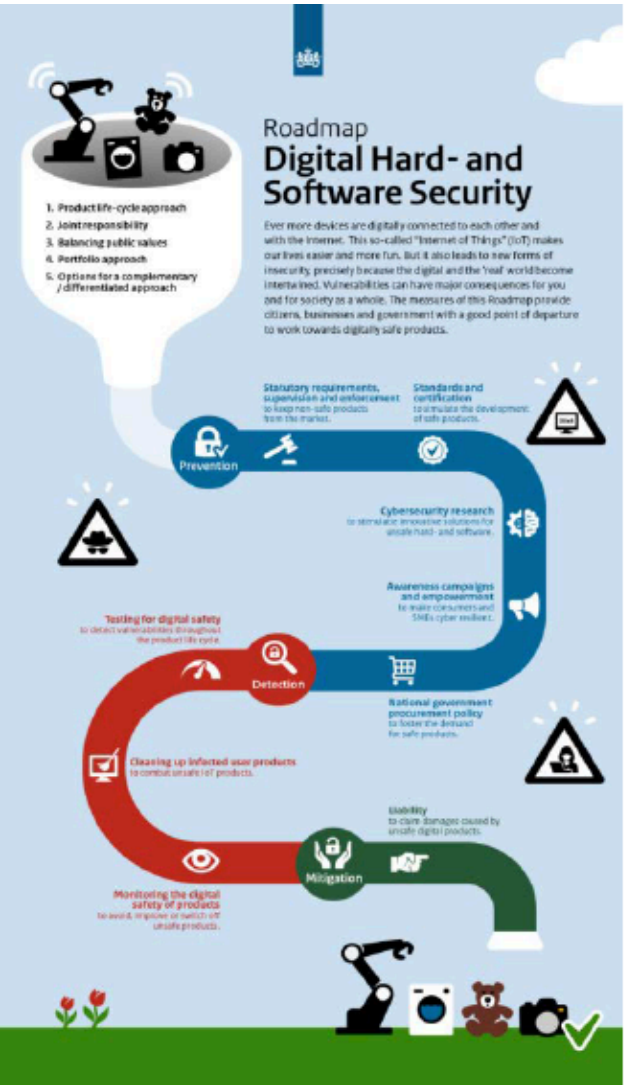
ISOC: 2018 Survey on Policy in Asia-Pacific:
We need to do Something about IoT Security

Clear Risks

• Consumer security, privacy and safety is being undermined by the vulnerability of individual devices; and

• The wider economy faces an increasing threat of large scale cyber attacks launched from large volumes of insecure IoT devices.

Netherland: Roadmap for h/w and s/w Security



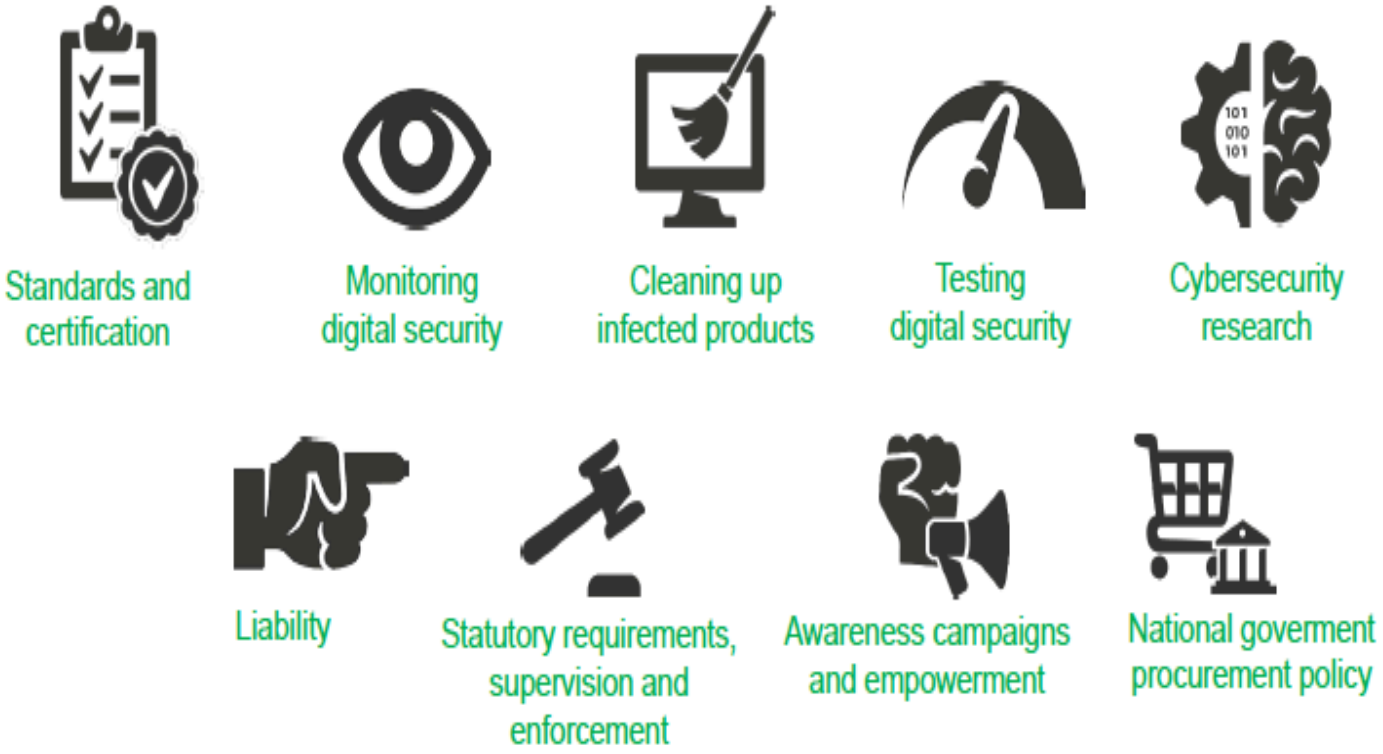
Product life cycle approach

Balancing public interest

Joint responsibility

Portfolio approach

Dutch Roadmap for h/w and s/w Security



EU – Certification

• European Cybersecurity Certification Framework Act (CSA)

• Certification covers availability, authenticity, integrity, and reliability of data or of functionality and services offered.

• Aim to start mandatory on specific high-risk products and services.

• Long term, mandatory certification with CE marking for all products with internet connectivity.

UK Government

• 2017-2018: Cooperation with industry, academia, consumer associations and international partners.

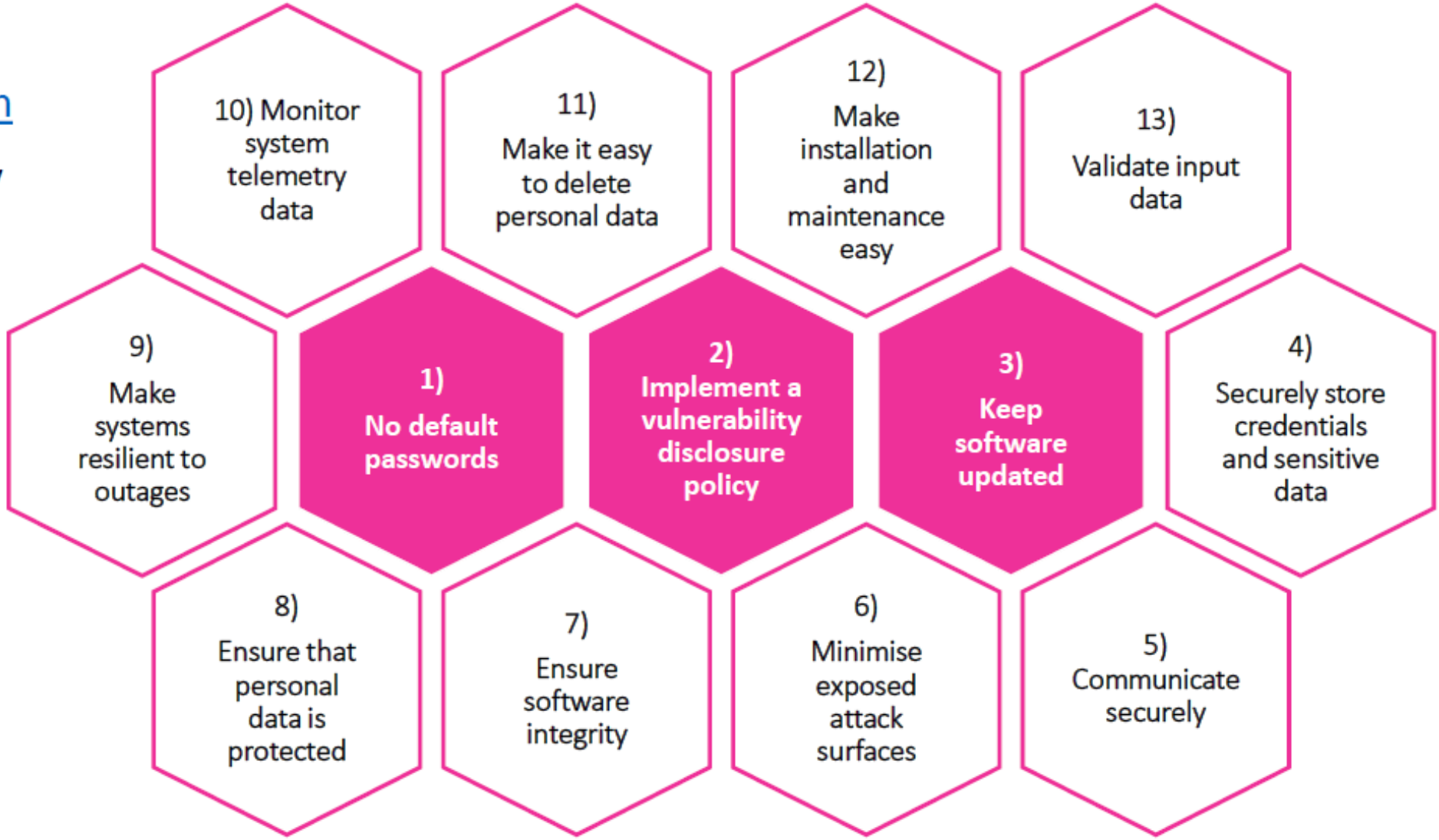
• Lead by Department of Digital, Culture, Media and Sports (DCMS).

• March 2018: “Secure By Design report”. Policy report
• October 2018:
  - “Code of Practice for Consumer IoT Security”
  - Mapping of the Code to existing recommendations and standards

UK: Code of Practice for Consumer IoT Security

gn

cy



UK – Certifications

- BSI Kitemark for IoT devices
  - Rigorous independent assessment
  - Three types of BSI Kitemarks for IoT devices
    - Residential
    - Commercial
    - Enhanced, for high value or high risk applications
  - Manufacturer assessed against ISO 9001
  - Product assessed on functionality and interoperability, and
  - Penetration testing scanning for vulnerabilities and security flaws
  - Regular monitoring and audit post award
  - Voluntary certification

Australia – Certification

- Trust framework based on
  - ***IoT Security Foundation,***
  - ***Open Web App Security Project (OWASP), and***
  - ***Online Trust Alliance (OTA)***
- IoT Product Testing to be done by labs accredited by National Association of Testing Authority (NATA)
- Award of test certificate
- Currently not mandatory
- IoTAA will release security test procedures based on OTA Framework
- Recommend to issue an IoTAA Security and Privacy Trustmark

Sponsored by: ISOC, ISED (Innovation, Science and Economic Development Canada), CIRA (Canadian Internet Registry Authority).

Three Pillars (Working Groups)

- Consumer Awareness and Education
- IoT Device Label Specification
- Network Resiliency
  - Protect network from end-user device, and protect device from network
  - IETF: Manufacturer Usage Description Protocol (draft)
    - Extension for Home Gateway
  - Promoting current best practices

IoT Device Label WG: *Objective*

• Identify the requirements of an IoT device label, aiming to:

- Provide consumers with information to help them make informed decisions at time of purchase on the security compliance and privacy measures of IoT devices

- Provide manufacturers* with a clear and concise way to display security features and related standards compliance of IoT products or devices

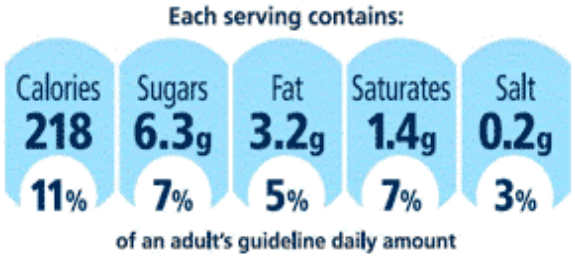
- Allow market oversight authorities to assess compliance to IoT security in a consistent and transparent approach.

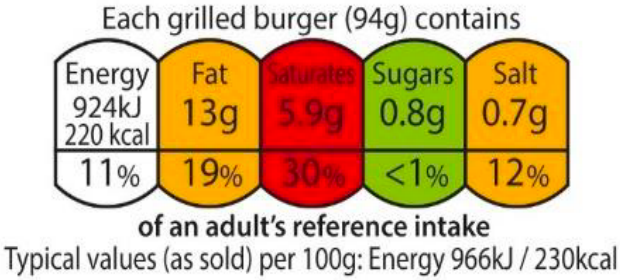
Key Considerations

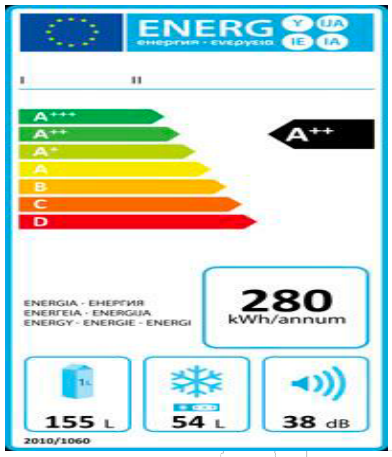
- Label formats
- Standards
- Certification
- Enforcement
- Example label requirements and structure
- H. Badran: “ ***Secure IoT: Labels to Build trust and Empower Consumers***” report, Nov. 2018.

Label Formats

- Graded Scheme







Refrigerating appliances, as EEI									
A+++	A++	A+	A	B	C	D	E	F	G
<22	<33	<42/44	<55	<75	<95	<110	<125	<150	>150

Label Formats - 2

- Binary or “Seal of Approval” Scheme

- Descriptive Information Scheme
  - Details security related information

Possible IoT Device Security Labels

- Colored graded scheme would attract attention for consumers
  - Need to be mandatory to be effective

- Binary “seal of approval” format is typically preferred by consumers
  - Could lead to false sense of security or that no further action from consumer is needed

- Descriptive information label format highlights critical information to consumers
  - Limit to most relevant information only
  - Good for voluntary label introduction

- Mandatory vs voluntary labels
  - Voluntary initially to become mandatory after a grace period

Canada: CSA Cyber Verification Program (CVP)

• CVP is a program and standard for *product* and *organization* security aspects.

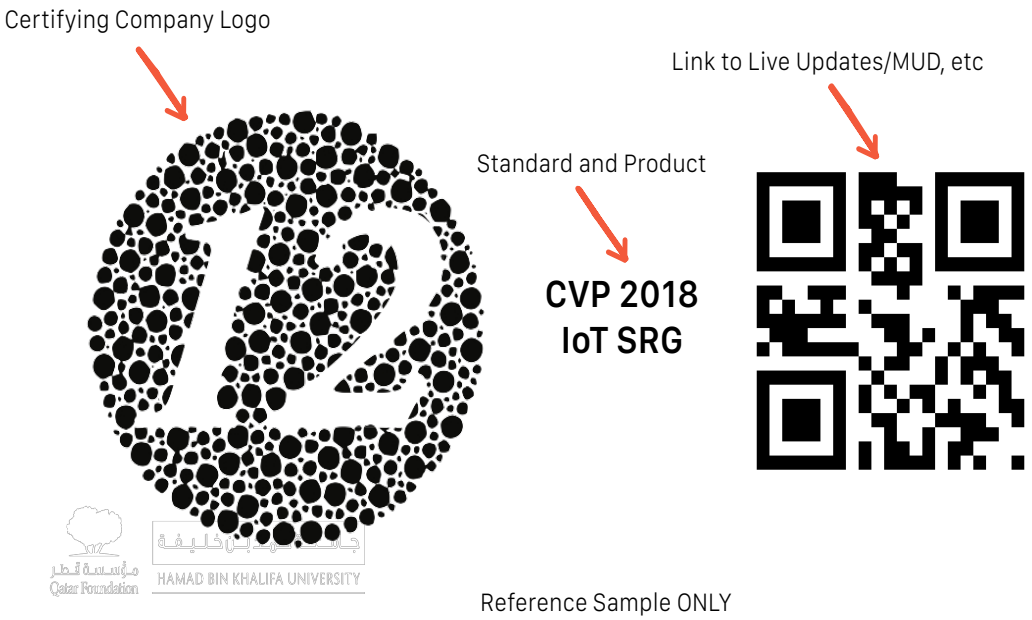
• CVP consists of:
  - Self assessment questionnaire: 198 binary questions covering 6 domains and 18 practices
  - An audit
  - Answers and audit will provide a maturity raring for the organization

• Program has been field tested

• Notice of Intent (NOI) for a Canadian standard is being filed.

Example IoT Device Label

- Label needs to identify
  - Organization who performed formal testing and assessment
  - Standard and product being tested
  - Means to prevent counterfeiting (e.g. holographic, embedded RFID, etc.)
  - Machine readable code to provide up-to-date/live product information (e.g. QR code)



Recommendations

1. Invite Arab States to establish the role of a "**Privacy Commissioner**" reporting to parliament.
   - As an example of PC mandate:
   - " The Privacy Commissioner of Canada is an Agent of Parliament whose mission is to protect and promote privacy rights".
2. Strengthen the roles of Consumer Protection agencies
   - Introduce consumer education and awareness functions for IoT consumer devices
   - Develop and publish "Code of Best Practice for Consumer IoT Security".
3. Develop national and pan-arab capabilities for IoT device testing and certification, benefiting from on-going international efforts (EU, UK, Canada, Australia).

ITU-T Focus Group on Vehicle Multimedia (FGVM)

- Newly formed group

- As a specific IoT domain,
  - identify gaps in the standardization landscape and
  - drafting technical reports and specifications
  - covering, among others,
    - vehicular multimedia use cases,
    - requirements,
    - applications,
    - interfaces,
    - protocols,
    - architectures and
    - security
- First meeting was in Ottawa, Oct. 2018

THANK YOU !!