A New Code of Practice to Improve Consumer IoT Security

David Rogers

Conference on Emerging Cyberspace Challenges and Solutions

Canterbury Christ Church University

11th January 2019

Department for Digital, Culture, Media & Sport

UK Government approach

- 2017 - 2018:
  - Cooperation with industry, academia, consumer associations and international partners
- March 2018:
  - Policy report
- October 2018:
  - Code of Practice for Consumer IoT Security
  - Mapping of the Code to existing recommendations
  - Consumer guidance
- https://www.gov.uk/government/publications/secure-by-design

BBC

News Sport More Search

NEWS

Home UK World Business Politics Tech Science Health More

Technology

UK seeks to secure smart home gadgets

15 October 2018 Share

Which?

Log in Sign up

News All news

Technology ▸ Smart homes

How new guidelines on smart devices will help protect consumers from being hacked

Tech companies HP Inc and Centrica Hive are the first to commit to making their products 'secure by design'

FINANCIAL TIMES

Cyber Security: Internet of Things

Cyber Security ✓ Added

Manufacturers face tighter rules on devices

'It's going to take collective action to get the security outcomes we're looking for'

Mail Online WIRES

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | V

Wires Home

Smart device-makers issued with code of practice to improve cyber security

By PRESS ASSOCIATION
PUBLISHED: 13:19, 15 October 2018 | **UPDATED:** 13:19, 15 October 2018

Share

Unique passwords, timely software updates and secure storage of personal data are among Government guidelines set out in a new code of practice for smart home

The Telegraph ALL SECTIONS

Technology Intelligence More

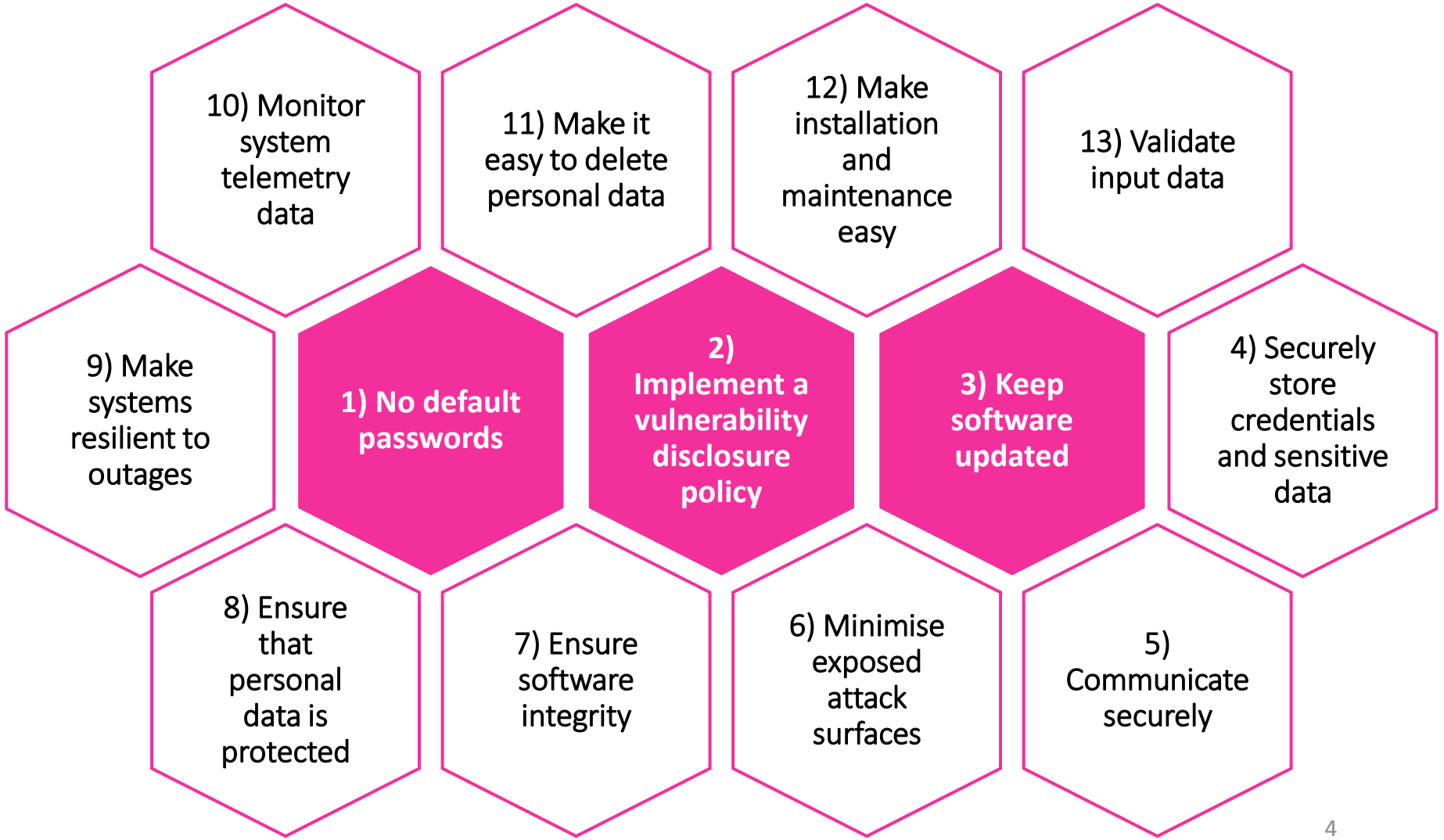
Technology Intelligence

Tech giants to sign up to new code of conduct to reduce risk of cyber attacks

share Save 1

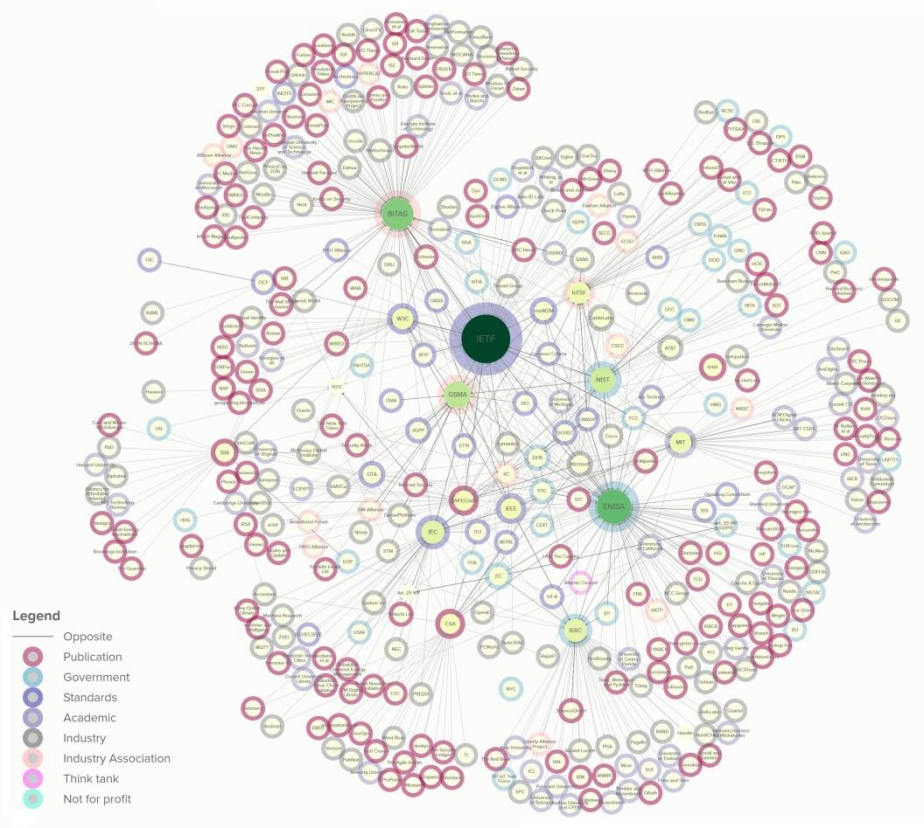
Code of Practice for Consumer IoT Security

- 13 outcome-focused, high-level guidelines. Top 3 are prioritised.
- Brings together what is widely considered good practice.
- Focuses on what matters most. Not a silver bullet to all problems.
- Primary audience: device manufacturers.
- Helps ensure GDPR compliance.



CoP mapped against existing standards and recommendations

- Analysed 100+ sources from 50+ organisations
- Mapping for each CoP guideline
  - Guideline 1 - No default passwords: 39 recommendations mapped from 13 organisations
  - Guideline 5 – Communicate securely:
  - 144 recommendations mapped from 26 organisations
- Published as report and open data on https://www.iotsecuritymapping.uk



Pledges to implement the Code of Practice

- IoT manufacturers that have made a public commitment to implement the Code of Practice:

Development of an ETSI TS on consumer IoT security

- Initial draft based on Code of Practice
- DTS/CYBER-0039

June 2018:
- Work Item approved

3-5 October 2018:
- Discussion at TC Cyber#14

Present:
- Comments are being implemented

January 2019:
- Target date for adoption

Resources

- Programme website
  https://www.gov.uk/government/publications/secure-by-design
- IoT Security Mapping
  https://iotsecuritymapping.uk
- ETSI TS Cyber Security for Consumer Internet of Things (DTS/CYBER-0039)
  https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?wki_id=54761
- Secure by Design blog on detail and context
  https://dcmsblog.uk/category/digital/

Consumer Guidance for Smart Devices in the Home

Smart or internet-connected devices, such as smart TVs, music speakers, connected toys or smart kitchen appliances can bring great benefits to your daily life. However, without taking steps to secure all of your internet-connected products, you and your data could be at risk from someone getting unauthorised access to your device or account. Developed by the UK government and industry experts, this guidance will help you manage the security of your devices and help protect your privacy.

SETTING-UP YOUR DEVICE

- **Read and follow the set-up instructions** for the device. These are often found in an app downloaded onto your smartphone, tablet or from a paper manual and guide that comes with the product.
- **Check device instructions to see if you need to** create an account on the manufacturer's website, or download any other recommended apps.
- If you are prompted to enter a password during the set-up process that is easy to guess, (such as 'admin' or '00000'), **you should change it**. Guidance on creating a strong password can be found on the **Cyber Aware** website.

MANAGING YOUR ACCOUNT

- To **set-up and manage your device**, you may need to create or use an existing account on the manufacturer's website. This account may allow you to add a new device or link your smartphone to your devices. You should ensure that your account has a **strong password**.
- For added security, if the device or app offers **Two Factor Authentication** which provides a second layer of security, (such as a text message to your phone) you should enable it. This is particularly important if the account contains your **personal data** or **sensitive information** or is linked to something that may impact your or another persons physical safety.
- **Some products allow you to access or control them** when you are away from your home's Wi-Fi network; such as, to view security camera footage. Consider whether you need to make use of this feature, as products may allow you to disable it either in the app settings or within your account.

KEEP UPDATING YOUR SOFTWARE AND APPS

Much like your laptop and smartphone, software and app updates help keep your devices secure. You should:

- **Check whether you can set-up and enable automatic updates** (on the app or on your online account).
- **Install the latest software and app updates**. These updates should download and install automatically on your device. If not, then you should install them straight away so you have the latest security protections. You should be prompted when a new update is ready to install, usually via a pop-up message or in the settings menu in the app or device menu.

IF YOU BECOME AWARE OF AN INCIDENT AND THINK IT AFFECTS YOUR DEVICE

- **Visit the manufacturer's website** to see if there is information available on what you should do next.
- Check the **National Cyber Security Centre** and the **Information Commissioner's Office** websites to see any published guidance.
- Further advice on your consumer rights can be found on the **Which?** and **Citizens Advice** websites.

HM Government CYBER AWARE **www.cyberaware.gov.uk**