IoT Security Foundation (IoTSF)

Introduction

IoT: What more can be said?

- **$:** The economic impact of the Internet of Things will be measured in $trillions.
- **∑:** The number of connected devices will be measured in billions.
- **∞:** The resultant benefits of a connected society are significant, disruptive and transformational.

But we can't carry on like this

IoT Security Foundation

Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking

Latest recall designed to protect connected vehicles from remote manipulation, says automobile company

News > World > Americas

Hacker takes control of Ohio couple's baby monitor and screams 'bad things'

NEWS

Anonymous hacker claims he broke into wind turbine systems

Cyber criminals hack a REFRIGERATOR: Will the 'Internet of Things' create a new bot army for the spammers?

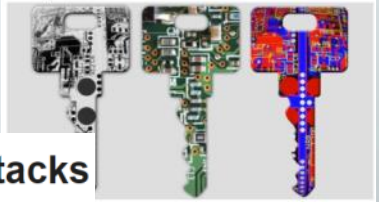
HOME › EXTREME › OUR INSECURE INTERNET OF THINGS IS BECOMING TERRIFYING

Our insecure Internet of Things is becoming terrifying

By Graham Templeton on September 8, 2015 at 8:37 am | 19 Comments

Lazy IoT, router makers reuse skeleton keys over and over in thousands of devices – new study

SSH logins, server-side HTTPS certs baked in firmware



Multiple Backdoors found in D-Link DWR-932 B LTE Router

Wednesday, September 28, 2016 Swati Khandelwal

Army of webcams used in net attacks

29 September 2016 | Technology

Hacking traffic lights with a laptop is easy

TECHNOLOGY NEWS | Tue Oct 4, 2016 | 8:58pm BST

J&J warns diabetic patients: Insulin pump vulnerable to hacking

RISK ASSESSMENT —

New, more-powerful IoT botnet infects 3,500 devices in 5 days

Discovery of Linux/IRCTelnet suggests troubling new DDoS menace could get worse.

DAN GOODIN - 11/1/2016, 9:15 PM

Introducing the Internet of Things Security Foundation

IoT Security Foundation

Beyond the horror stories: the IoT Security Foundation was launched on Sept 23rd 2015 in response to wide-ranging security concerns from IoT stakeholder groups

Purpose

Our Mission

Our mission is to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this we will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems.

Make it safe to connect

Or simply: "Drive the quality and pervasiveness…
… of IoT security"

Our Values

SECURITY FIRST *Designed in at the start*

FIT FOR PURPOSE *Right-sized for application*

RESILIENCE *Through operating life*

www.iotsecurityfoundation.org

Executive Steering Board

Prof. Paul Dorey, **CSO Confidential**

Prof. John Haine, **University of Bristol**

Prof. David Rogers, **Copper Horse Solutions**

Ken Munro, **PenTest Partners**

Prof. Ben Azvine, **BT plc.**

Majid Bemanian, **Imagination Technologies**

Dr. Stephen Pattison, **ARM**

Haydn Povey, **Secure Thingz**

Prof. Kenny Paterson, **Royal Holloway, University of London**

Dr. Steve Babbage, **Vodafone Group**

Richard Marshall, **Xitex Ltd.**

John Moor, **IoT Security Foundation**

How we are organized

Executive Steering Board

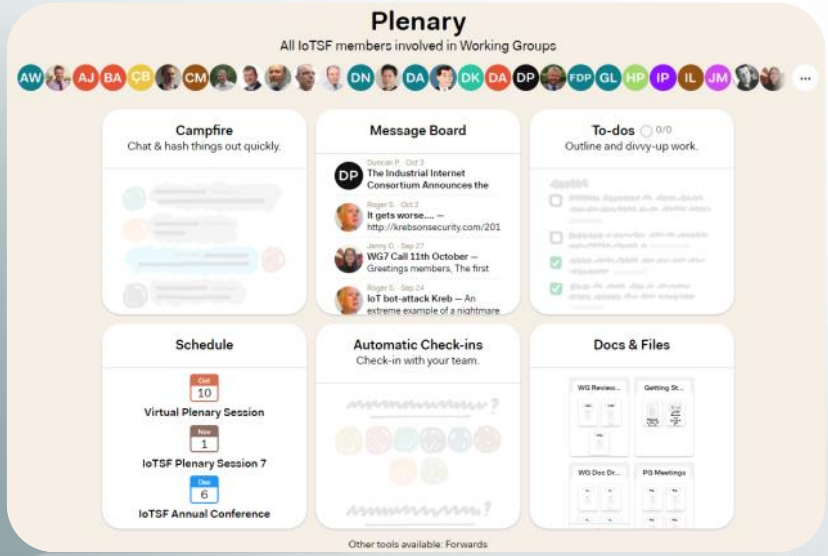
Plenary Group

Working Groups

Members

Priority Working Groups	Chaired by:
Working Group 1: Self-Certification	
Working Group 2: Connected Consumer / Home	
Working Group 3: Patching Constrained devices	
Working Group 4: Vulnerability Disclosure	
Working Group 5: IoT Security Landscape	
Working Group Formed: Trustmark / Regulatory	

Working Across Continents



Online Collaboration Platform

Physical Meetings

THE BIG IOT SECURITY CHALLENGE

Who owns security in IoT?

What can “*we*” do together?

How can “*we*” improve best practice?

How can we position ourselves ahead of regulation (it’s coming!)?

What's The Big Idea?

IoT is a ***"Highly Distributed Moral Responsibility"***

- We must all play our part
    - Producers
    - Integrators
    - Procurers
    - Retailers / Users
    - Governments and Citizens
    - …

DUTY OF CARE

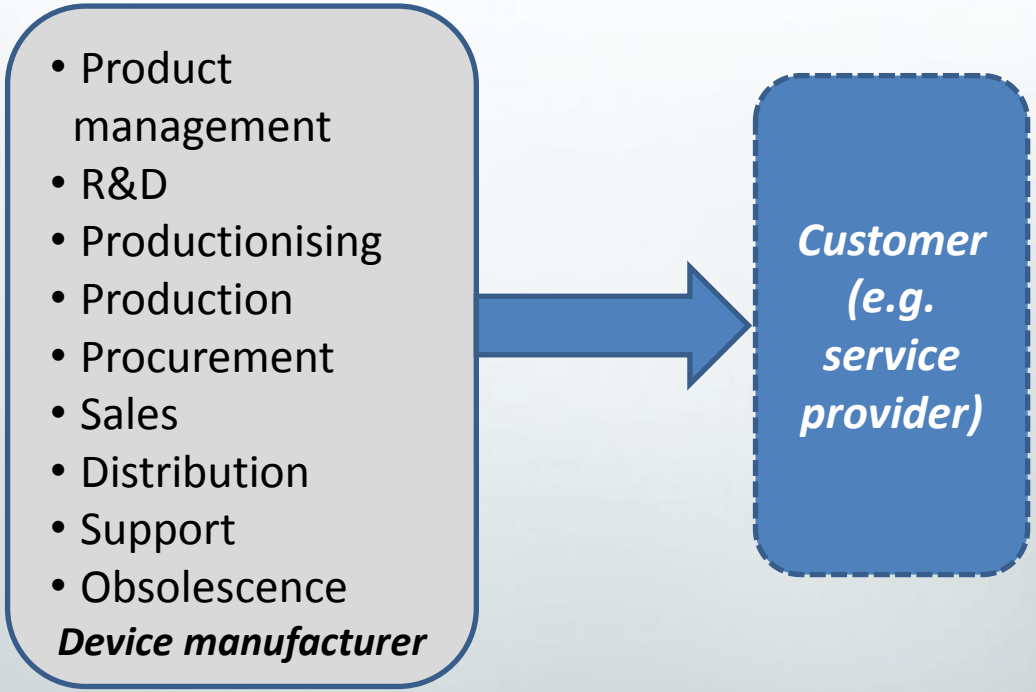
SUPPLY CHAIN OF TRUST

A link in the “supply chain of trust”

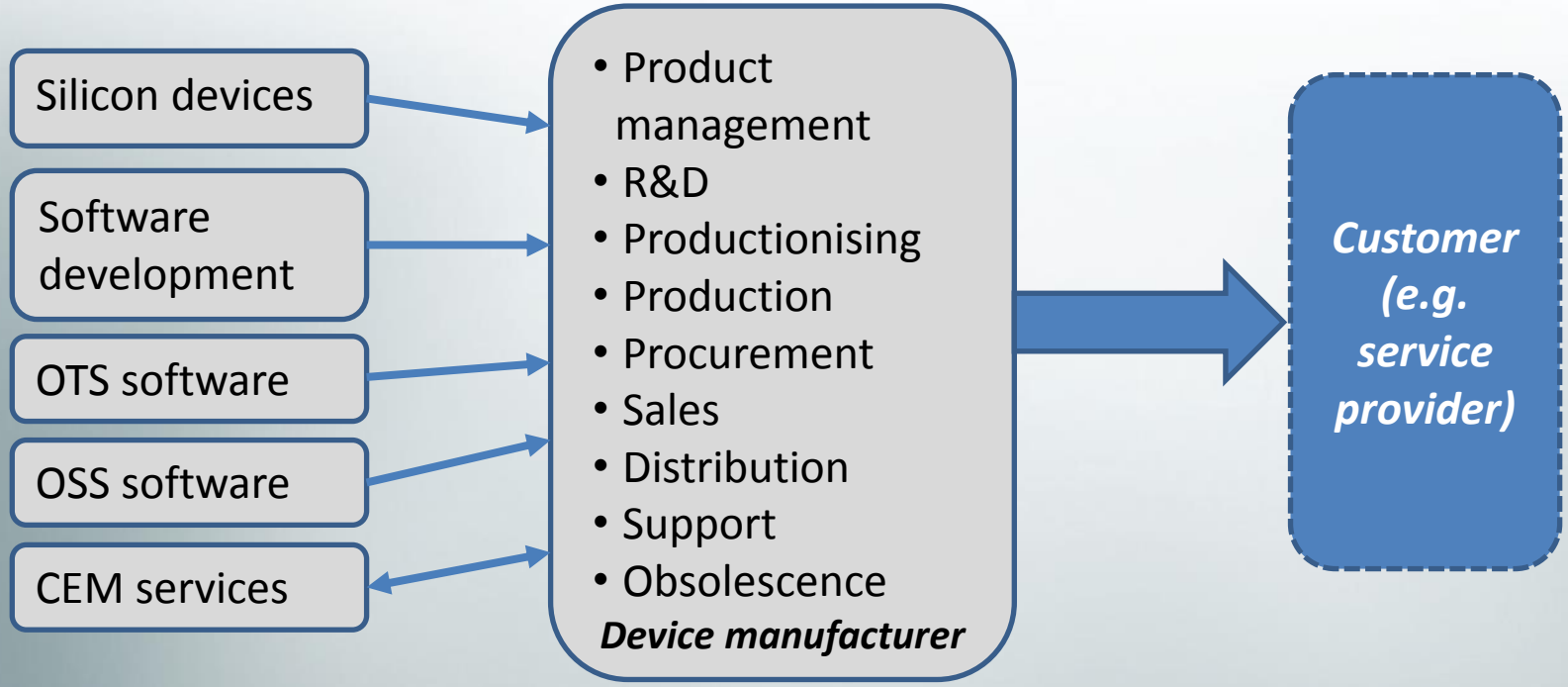
- Product management
- R&D
- Productionising
- Production
- Procurement
- Sales
- Distribution
- Support
- Obsolescence

Device manufacturer

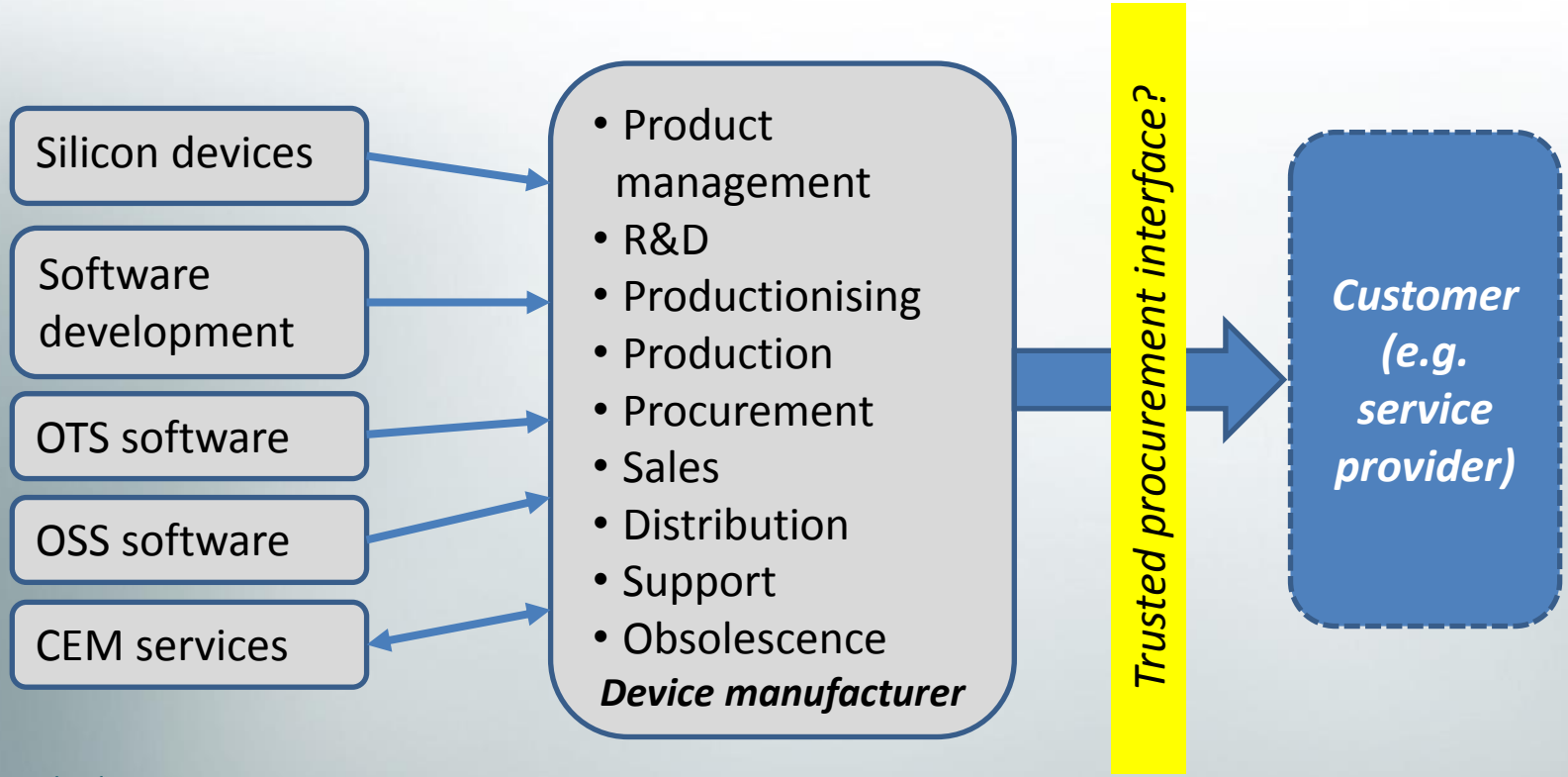
A link in the “supply chain of trust”



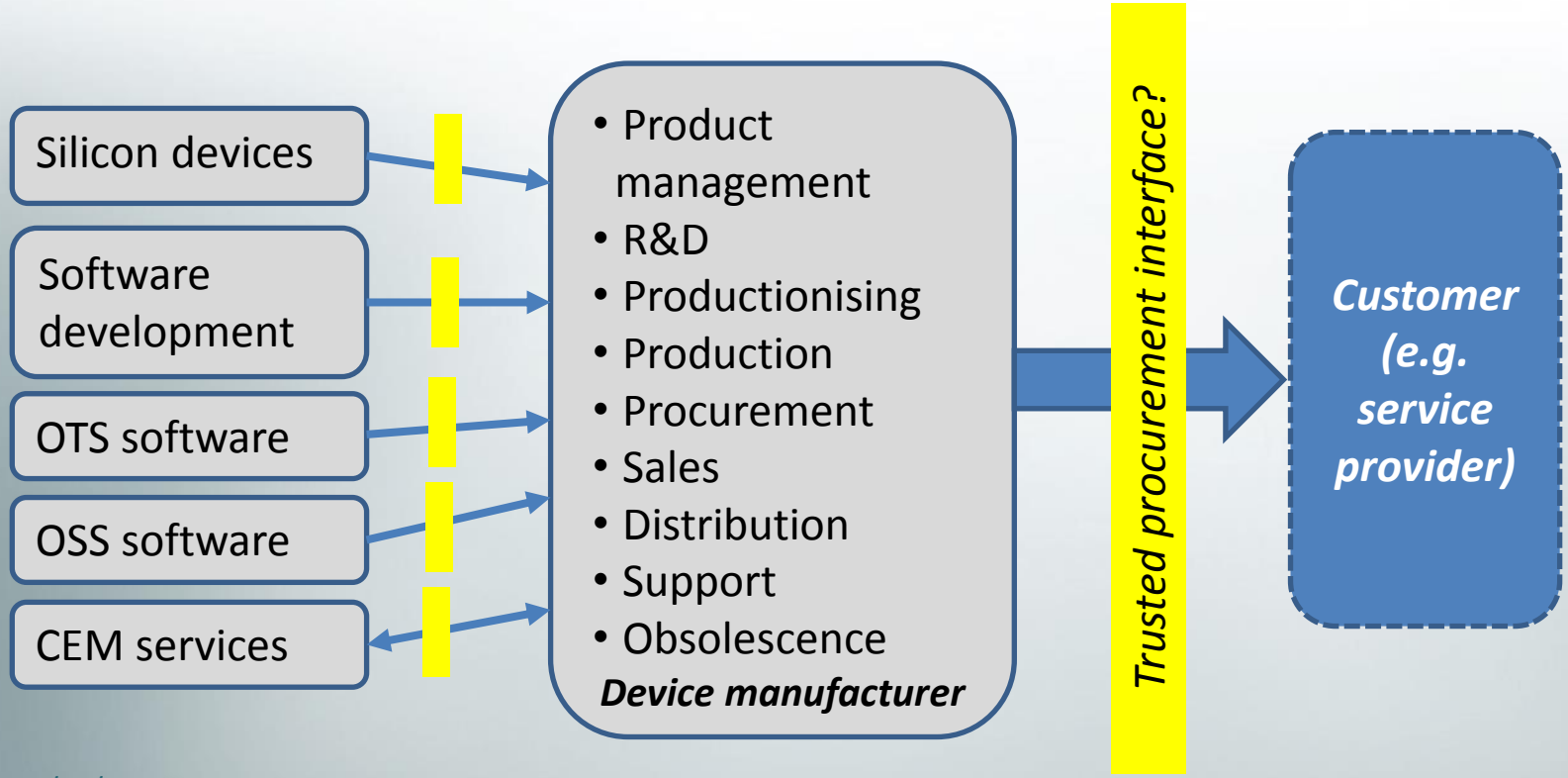
A link in the “supply chain of trust”



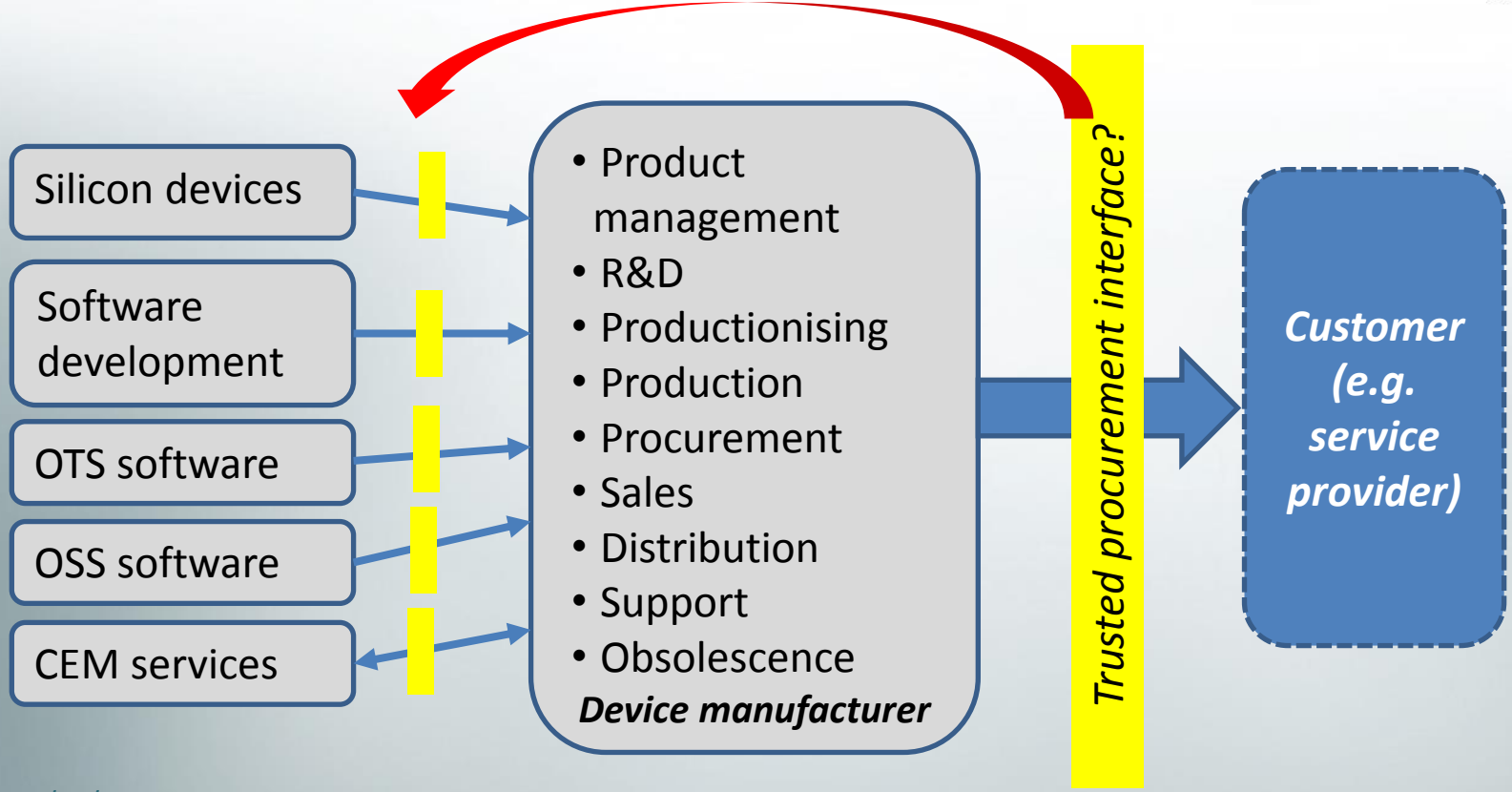
A link in the “supply chain of trust”



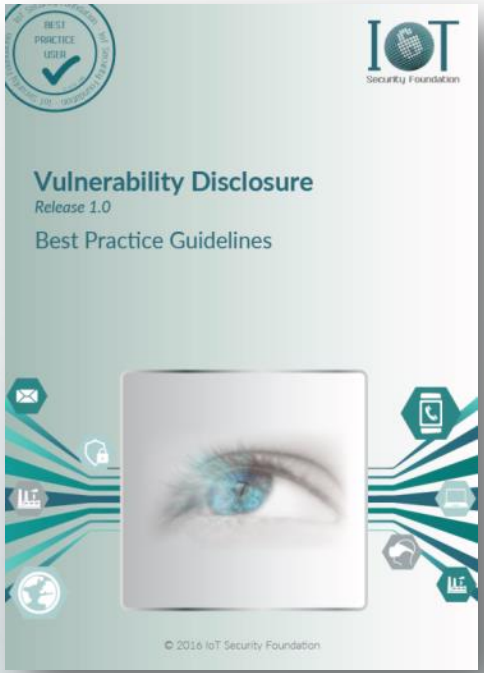
A link in the “supply chain of trust”



A link in the “supply chain of trust”



Best Practice Guides



Free to download
Free to use
More coming…

See https://iotsecurityfoundation.org/best-practice-guidelines/

IoT Security Compliance Framework

1.Compliance Applicability - Business Security Processes and Responsibility

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.1.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	1 and above	M	TBD in future release
2.3.1.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	1 and above	M	TBD in future release
2.3.1.3	There are documented business processes in place for security.	1 and above	M	TBD in future release
2.3.1.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework etc.).	2 and above	A	TBD in future release
2.3.1.5	A policy has been established for dealing with both internal and third party security research on the products or services.	1 and above	M	TBD in future release
2.3.1.6	A security policy has been established for addressing changes, such as vulnerabilities, that could impact security and affect or involve technology or components incorporated into the product or service provided.	2 and above	A	TBD in future release
2.3.1.7	Processes and plans are in place based upon the IoTSF “Vulnerability Disclosure Guidelines” or similar recognised process to deal with the identification of a security vulnerability or compromise when they occur.	1 and above	M	TBD in future release
2.3.1.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements. In particular that any public statements made in the event of a security breach, should give as full and accurate account of the facts as possible.	1 and above	M	TBD in future release
2.3.1.9	There is a secure notification process based upon the IoTSF “Vulnerability Disclosure Guidelines” or similar recognised process, for notifying partners/users of any security updates.	1 and above	M	TBD in future release
2.3.1.10	A security threat and risk assessment shall have been carried out using a standard methodology such as Octave, NIST RMF to determine the risks and evolving.	2 and above	A	TBD in future release

1. Business Security Processes and Responsibility

Please confirm and verify with evidence (to be supplied) that the business processes and responsibility supporting the product/service comply with the following requirements. Each response should be selected from the following: “Compliant” [C]; “Partially Compliant” [P]; “Non-compliant” [N]:

Req. No	Requirement	Compliance Class	Response	Evidence
3.1.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	1 and above	C/ PC/ N	<link to evidence>
3.1.2	There is be a person or role, who takes ownership for adherence to this compliance checklist process.	1 and above	C/ PC/ N	<link to evidence>
3.1.3	There are documented business processes in place for security.	1 and above	C/ PC/ N	<link to evidence>
3.1.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework etc.).	2 and above	C/ PC/ N	<link to evidence>
3.1.5	A policy has been established for dealing with both internal and third party security research on the products or services.	1 and above	C/ PC/ N	<link to evidence>
3.1.6	A security policy has been established for addressing changes, such as vulnerabilities, that could impact security and affect or involve technology or components incorporated into the product or service provided.	2 and above	C/ PC/ N	<link to evidence>
3.1.7	Processes and plans are in place based upon the IoTSF “Vulnerability Disclosure Guidelines” or similar recognised process to deal with the identification of a security vulnerability or compromise when they occur.	1 and above	C/ PC/ N	<link to evidence>
3.1.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements.	1 and above	C/ PC/ N	<link to evidence>
3.1.9	There is a secure notification process based upon the IoTSF “Vulnerability Disclosure Guidelines” or similar recognised process, for notifying partners/users of any security updates.	1 and above	C/ PC/ N	<link to evidence>

Annual Conference

- IoTSF has an annual conference
  - Addressing contemporary and forward looking themes
- 2017: Dec 5th / London

"IoT: What will security standards and certification look like ten years from now?"

"Weaponising IoT"

We invite you to join us!

Growing membership, large and small, across the IoT eco system and stakeholder groups

Low Cost Membership / High Value Activity

Join us simply online at:
https://iotsecurityfoundation.org/join/

See https://iotsecurityfoundation.org/our-members

IoTSF ::

THE GLOBAL HOME FOR IoT SECURITY

Community / best practice / next practice

https://iotsecurityfoundation.org