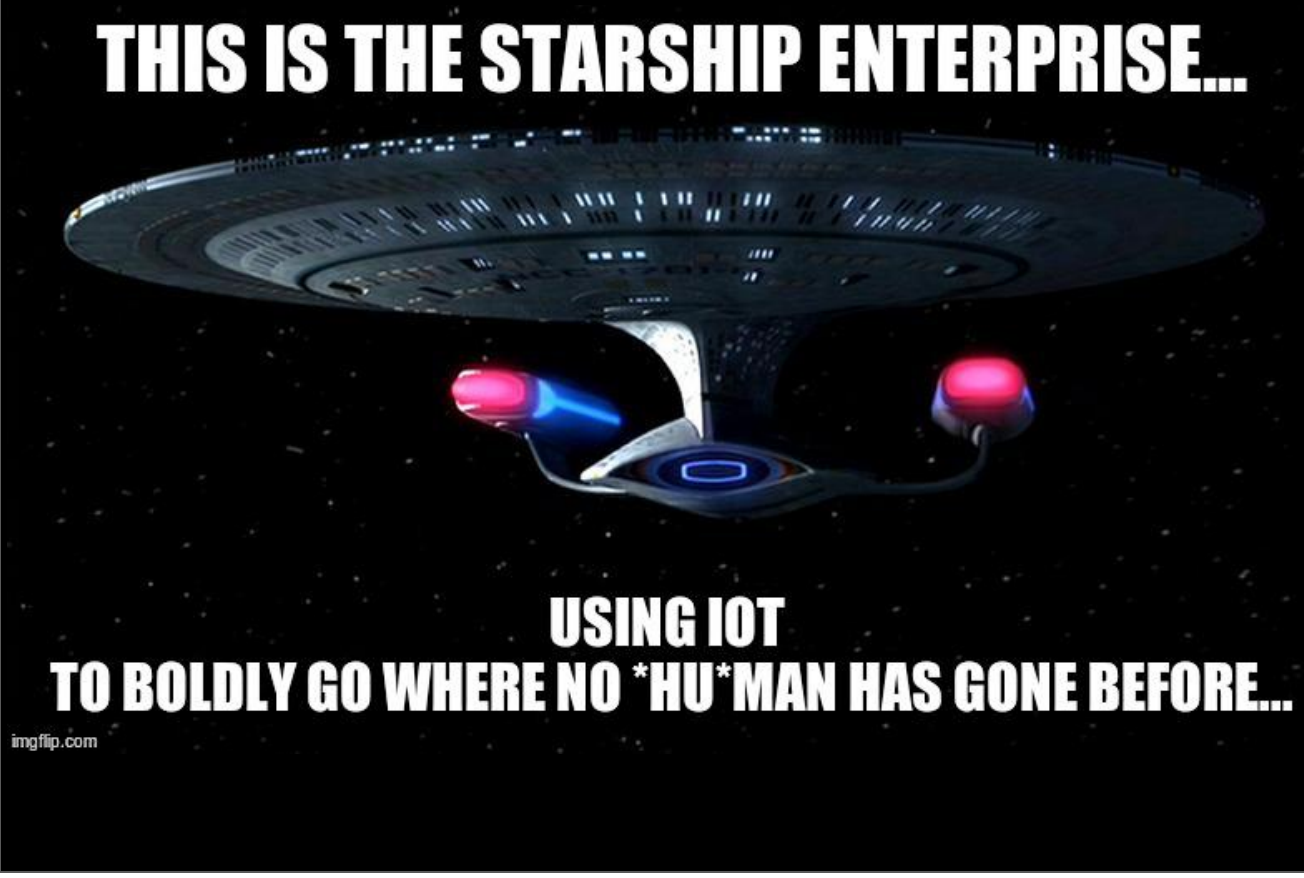
# FACE-PALM AND CARRY ON

---

## A Tale of I's, O's and T's

Sig-C, April 9, 2020

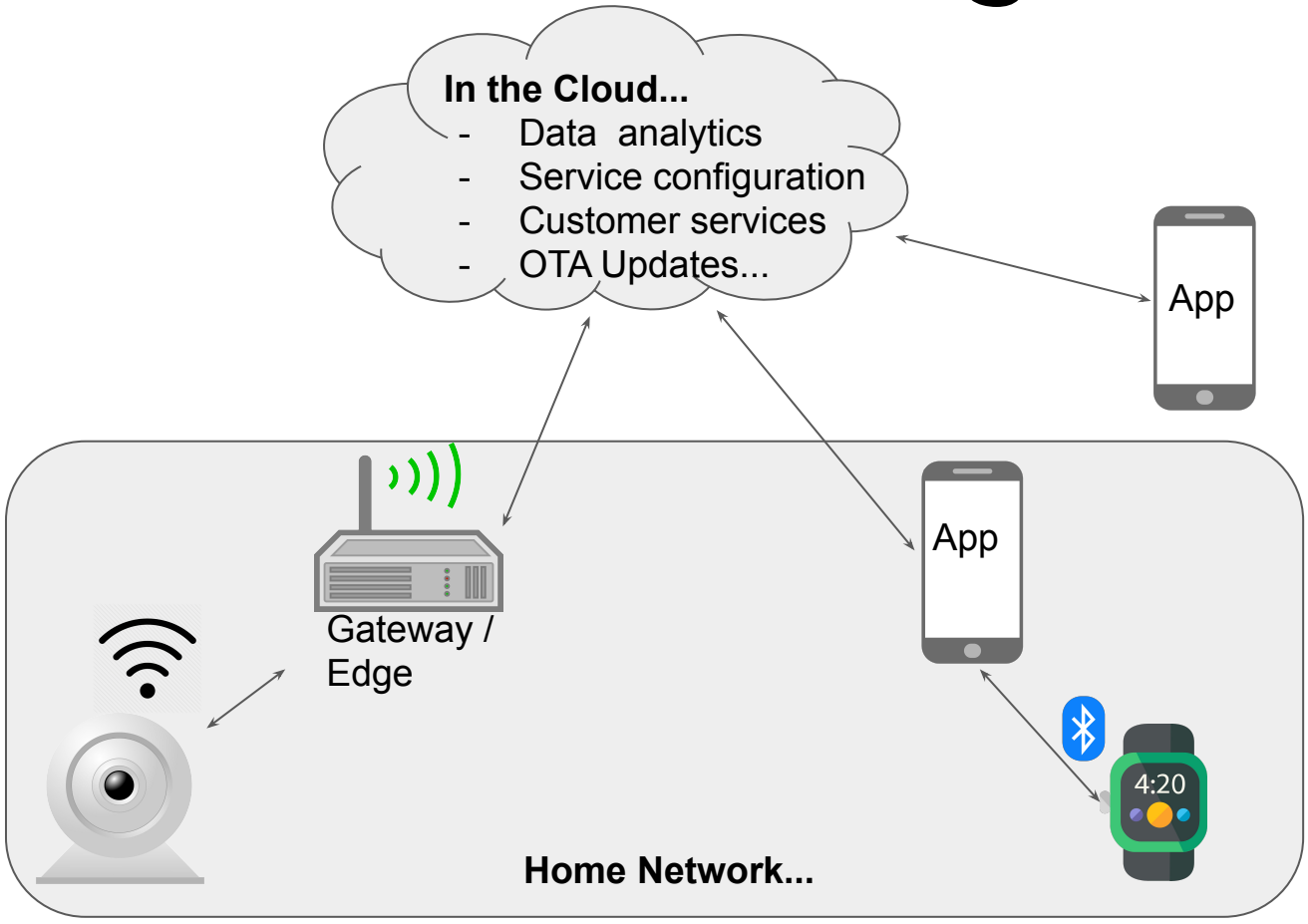
@jennjanesko



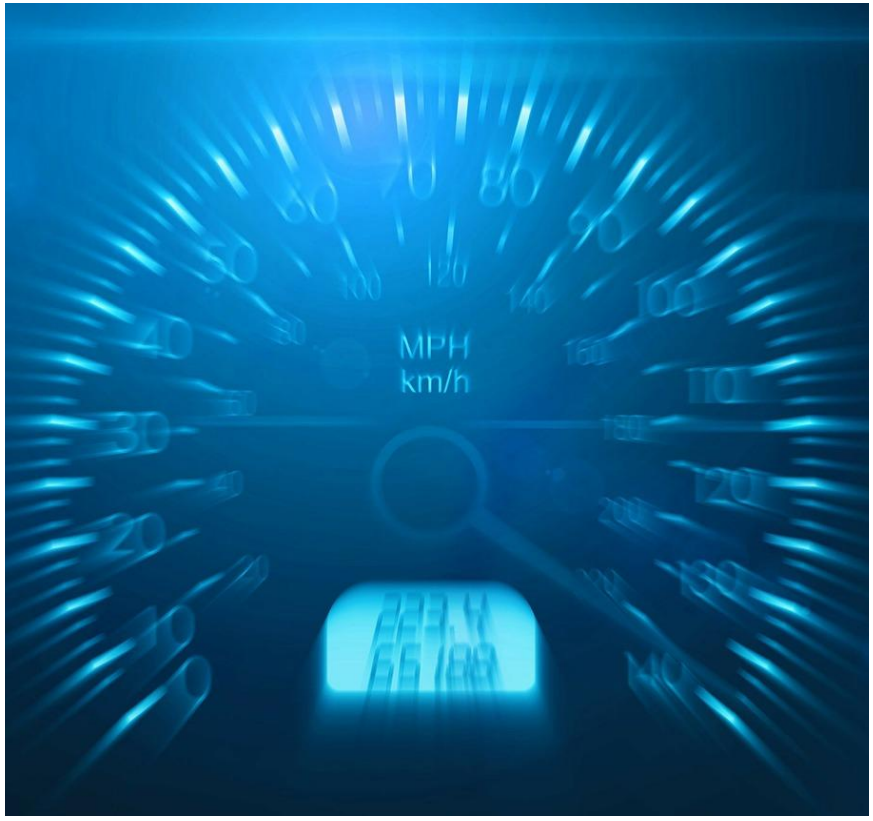

**Star Trek:**
**The Next Generation**

- Replicator
- Warp Drive
- “Computer...”
- Transporter
- Holodeck
- Cloaking Devices
- Medical Bay
- The Borg
- Data...

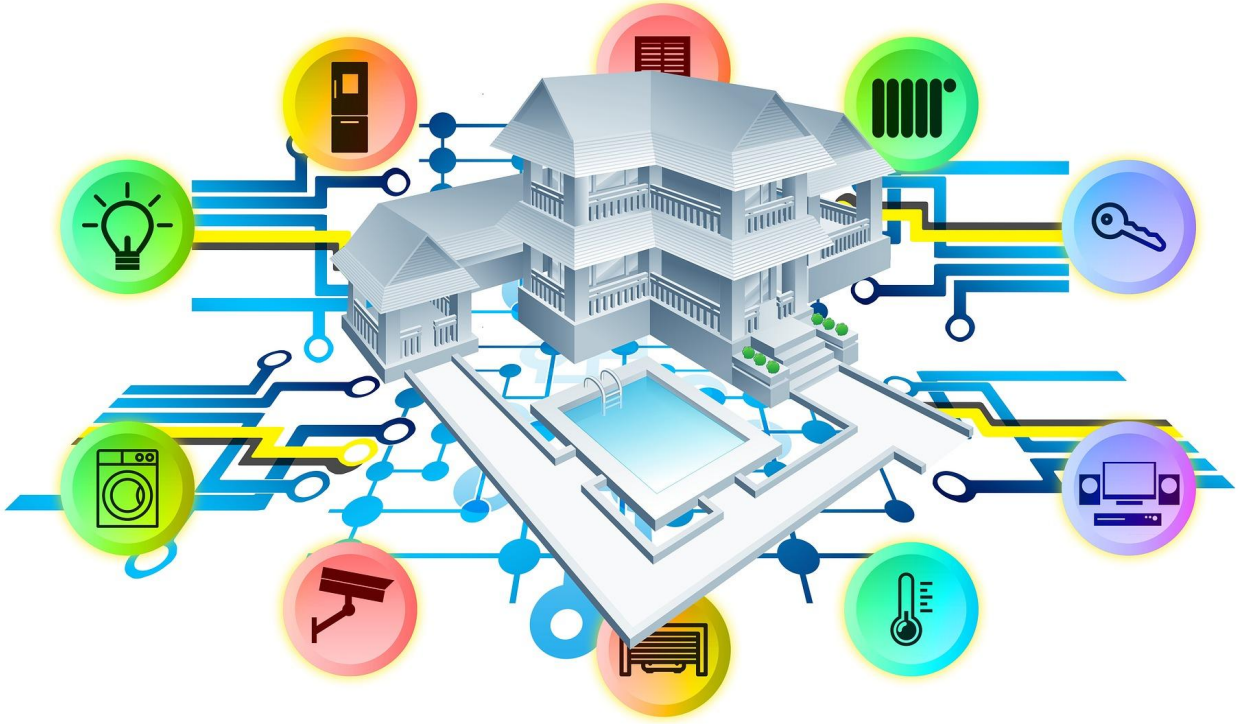
# Internet of Things



“Tea. Earl Grey. Hot.”




”Warp …“

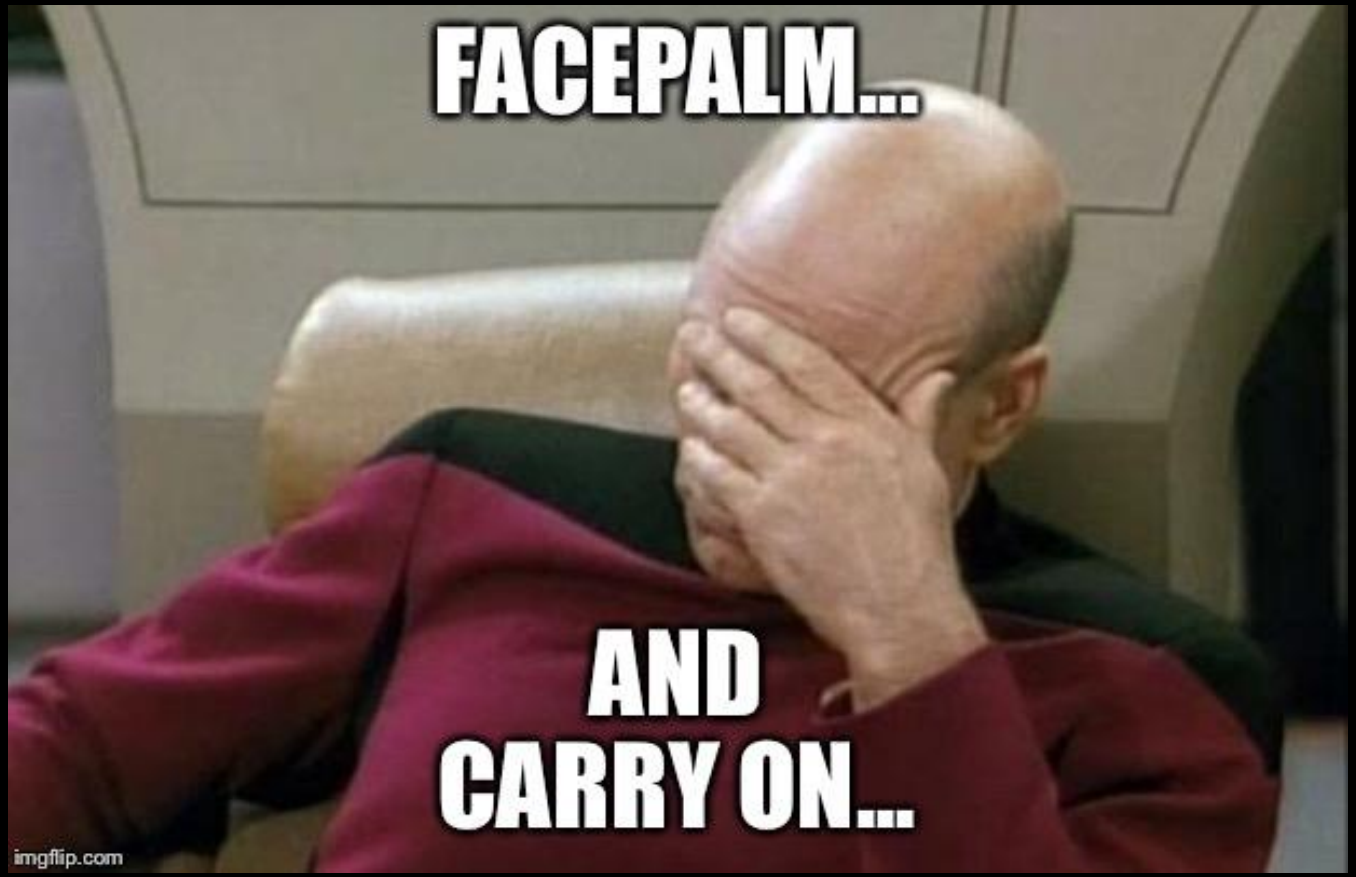


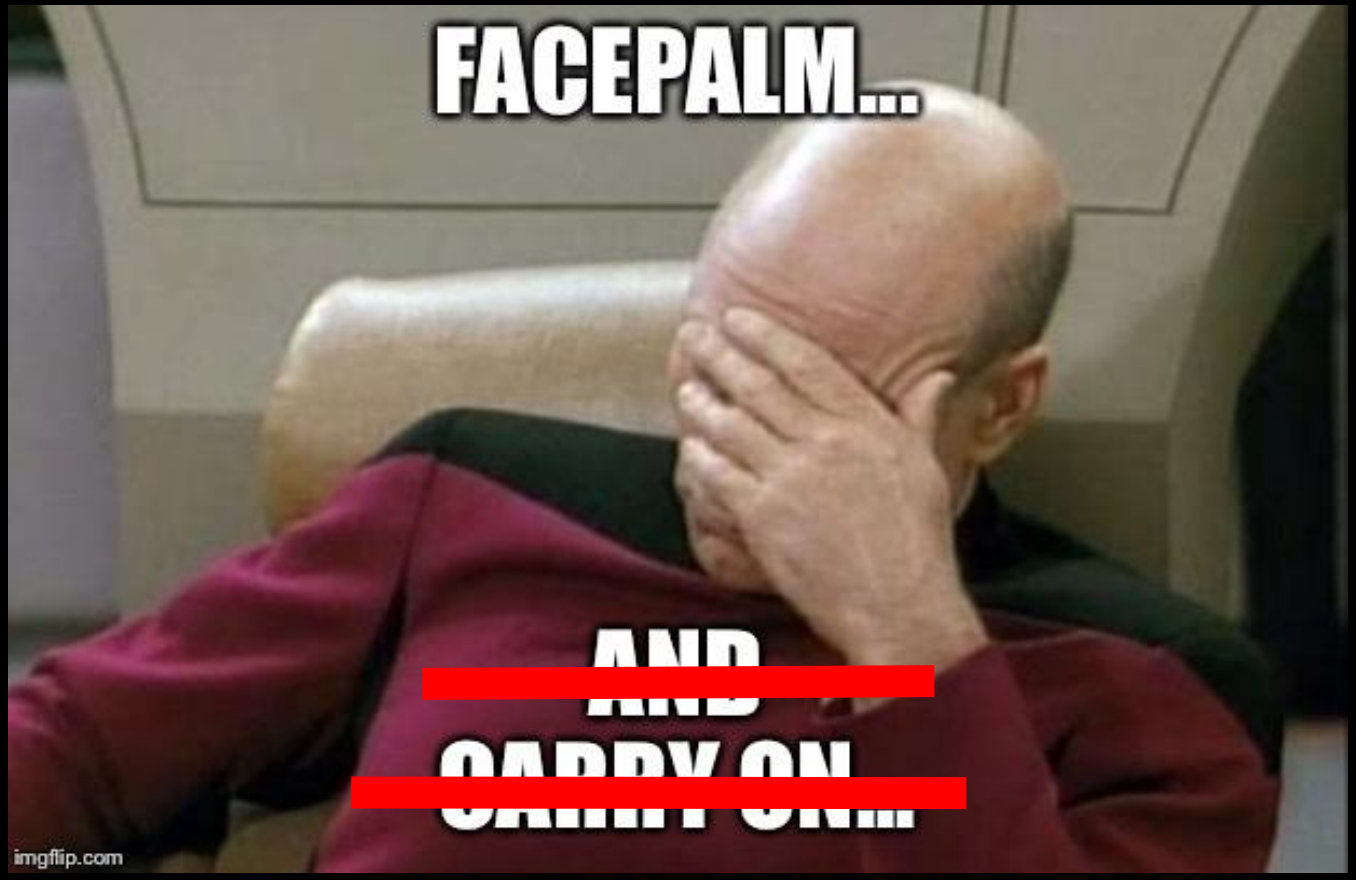
”Computer . . .”

# Software Security in IoT Improving?

- Scope:
  - 4000+ Firmware
  - 22 Vendors
  - 15 years
- General Result:
  - No positive trends

- *Data from analysis available*


FACEPALM...
AND
CARRY ON...
imgflip.com

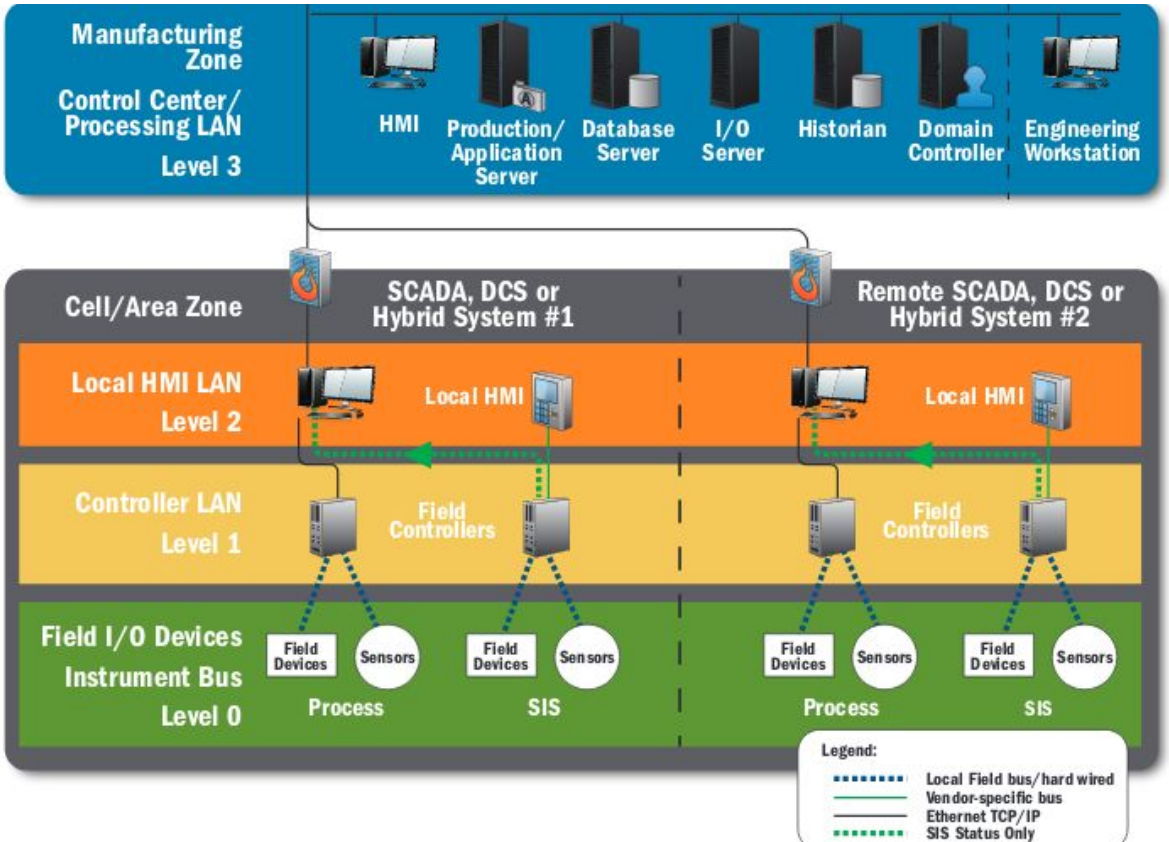

FACEPALM...
AND
CARRY ON...
imgflip.com

# Operational Technology (OT) → IIoT

- Airgapped → Connected

- Solutions:
  - Remote
  - Mobile/ web apps
  - Cloud

- Breach impacts:
  - Environmental
  - Death / Injury
  - Damage



# OT: Legislation and Legal Directives

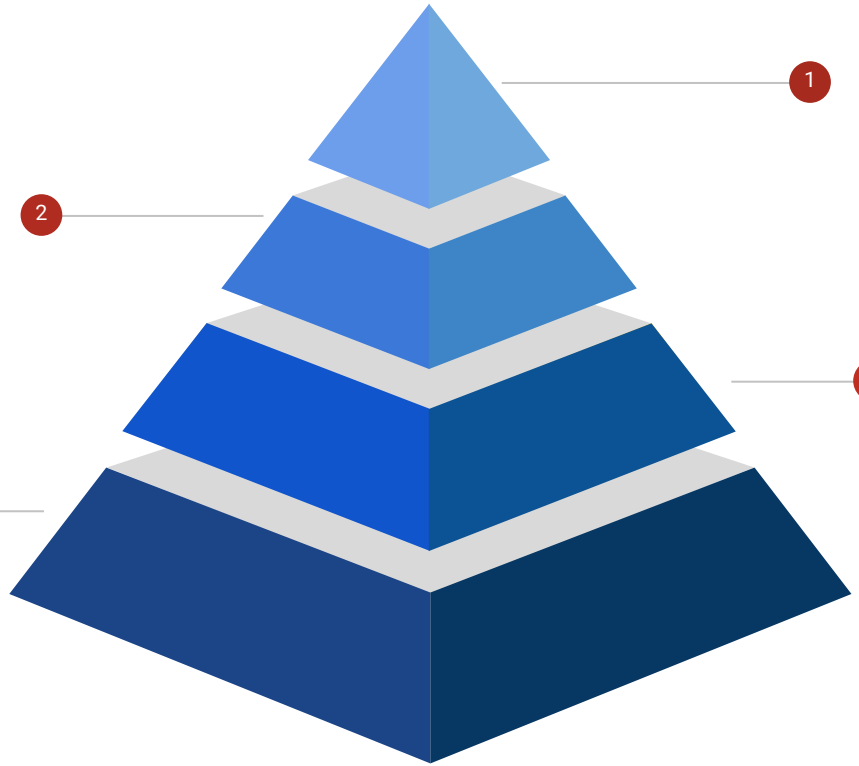
| USA | Europe | Singapore |
| --- | --- | --- |
| - Energy Policy Act of 2005<br><br>- NERC-CIP Standards | - European Programme for Critical Infrastructure Protection (EPCIP) - 2004<br><br>- Germany: 2015 Amendment to Energiewirtschafts-gesetz | - Singapore's Operational Technology Cybersecurity Masterplan (2019) |

# OT Roles

Asset Owner | System Integrator | Product Supplier


IEC 62443

# Responsibility for OT Security: Asset Owners



## Security Audits

1

Site Assessments
Vulnerability Analysis (!)
Penetration Testing (!)

## Monitoring

2

IDS
Canaries
Threat Hunting

## Access Control

3

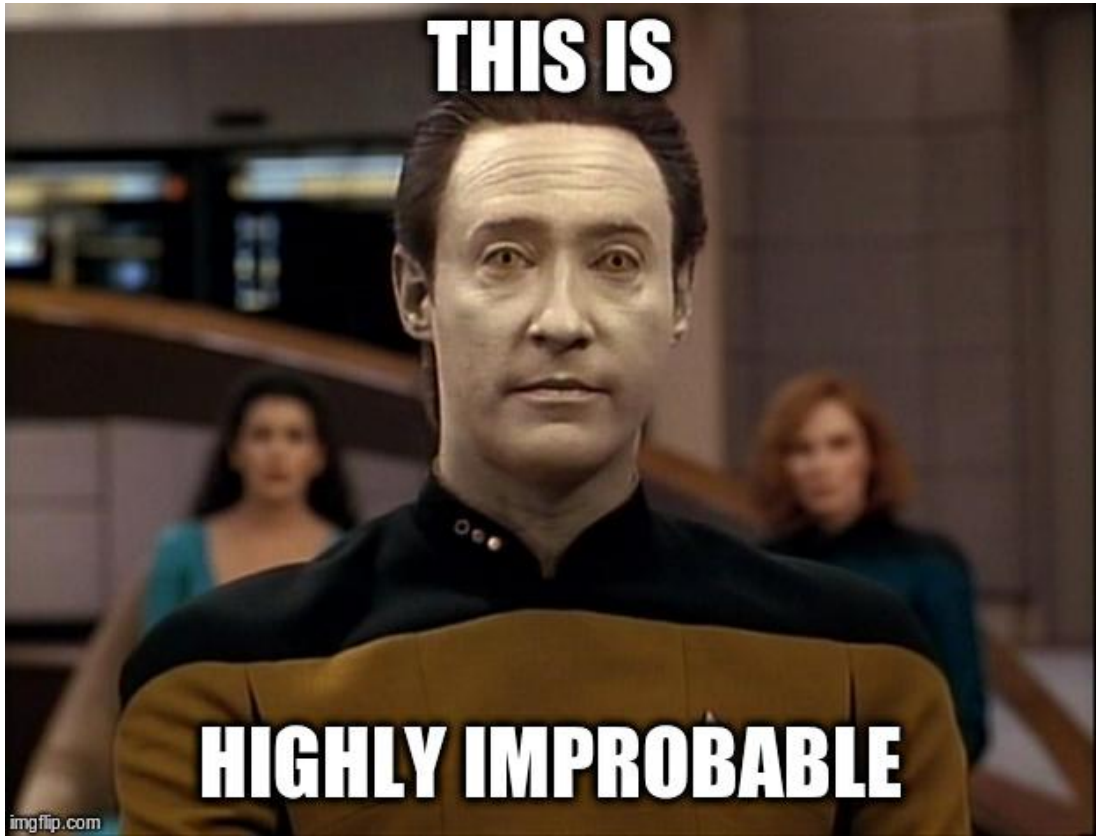
Firewalls
DMZs
Diodes
Jump Hosts
Segmentation

## Process

4

ISMS
Concepts
Procedures
Documentation!

# OT Legislation: Is it perfect?



# OT Roles in IoT

| | Asset Owner | System Integrator | Product Supplier |
|---|---|---|---|
| **Medical (IoMT)** | | | |
| **Connected Vehicle (V2X)** | | | |
| **Consumer IoT** | | | |

# OT Roles in IoT: Medical

| | Asset Owner | System Integrator | Product Supplier |
|---|---|---|---|
| **Medical (IoMT)** | Humans | Hospital, Doctor‘s Office, Medical Center | Medical device supplier, component supplier |

- USA → Food and Drug Administration
- EU → Medical Devices Regulation

# OT Roles in IoT: Automotive

| | Asset Owner | System Integrator | Product Supplier |
|---|---|---|---|
| **Connected Vehicle (V2X)** | Humans | Auto Dealer<br>Service Stations<br>Relatives/Friends with Skills | OEM, ECU Supplier |

- ISO 21434
  - “Road vehicles – Cybersecurity engineering”
- Related standards
  - ISO 26262 (safety)
  - SAE J3061 (cybersecurity)

# OT Roles in IoT: Consumer

| | Asset Owner | System Integrator | Product Supplier |
|---|---|---|---|
| **Consumer IoT** | Humans | Package Instructions, Youtube, Quora, StackOverflow... | IoT device maker, component supplier |

# Legislation for Asset Owners?

# Legislation for Product Suppliers?

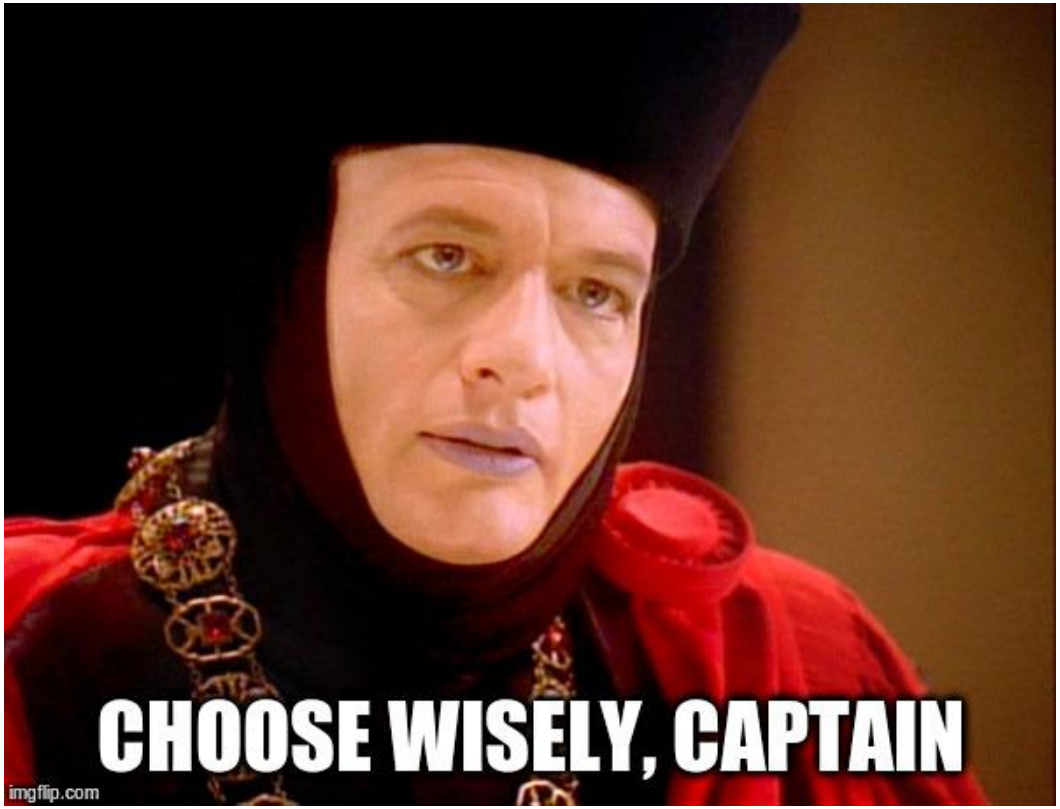
**Legislative Examples**

- Existing:
  - California: SB-327
- Proposed:
  - USA:
    House Bill 1668
  - UK:
    CoP for Consumer IoT Security
  - Germany:
    BSI TR-03148 - Router Security

**Legislative Inhibitors**

- Lack of perceived criticality (changing)
- Lack of expertise (partial)
- Impact on business (especially small and micro)
- Monitoring costs

# Standards? (YAS?)




-OWASP Internet of Things Security Recommendations

-UK Code of Practice for Consumer IoT Security

-Enisa Good Practices for the Security of IoT

-CSA Future Proofing the Connected World

-IoT Security Foundation Publications

-GSMA IoT Assessment IoT Security Guidelines

-CIS Controls: IoT Companion Guide

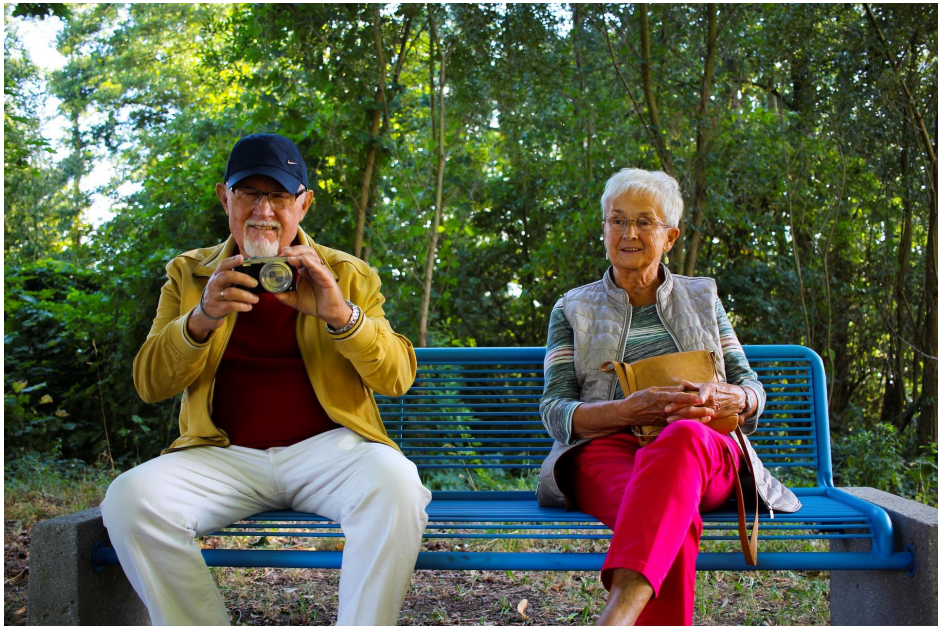
-ETSI TS 103 645: Cyber Security for Consumer IoT

-NIST IR 8228, 8259, 8267

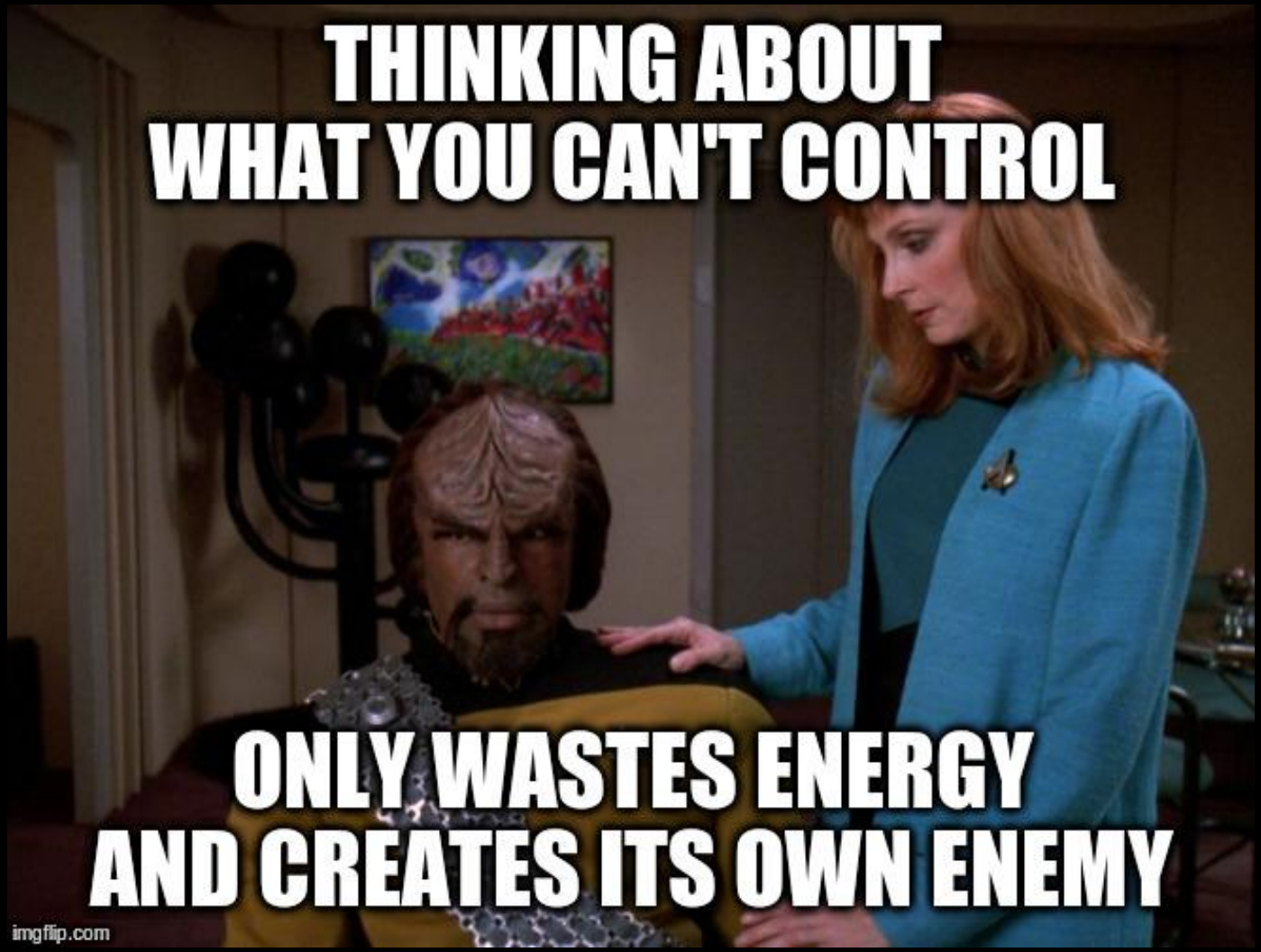
# Security - Can we sell it?

- ~ ⅓ some concern about “unauthorized access”
- > 50% default password
- < 50% look for security
- Setup time….

- Example: Norton Core - Secure Gateway



ESET & National Cyber Security Alliance (October 2019)


THINKING ABOUT
WHAT YOU CAN'T CONTROL
ONLY WASTES ENERGY
AND CREATES ITS OWN ENEMY
imgflip.com

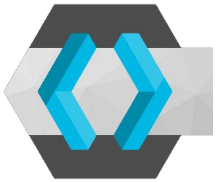
# Non-regulated improvements in web applications...











# Opportunities: Frameworks & IoT Application Stack

- **Cloud**
  - AWS, Azure, GCP, Bosch…
- **Software**
  - CoreOS, Ubuntu for IoT, Amazon FreeRTOS, BalenaOS, Windows 10 IoT Core…
- **Wireless Protocols**
  - BLE, Bluetooth, Zigbee, Sigfox, LTE, 5G...
- **Hardware**
  - … looking for ideas

Threat Model & Blog

Secure & Git
- Infrastructure as code
- Secure code snippets

Test & Report (or Patch)

# Opportunities: Secure Development in SDLC

**Design & Code (best):** Secure Frameworks, Secure Code Snippets, Linters
**Commit & Build (fine):** Code Review, SAST, SCA
**Integration & Test (usually, too late):** Fuzzing, DAST, Penetration Testing

> “There are a large number of duplicate binaries across multiple vendors, indicating a common build system or toolchain.”
>
> - Cyber ITL

IDE’s

- Platform IO
- Eclipse IoT (Kura)
- Node-Red

Build environments?...

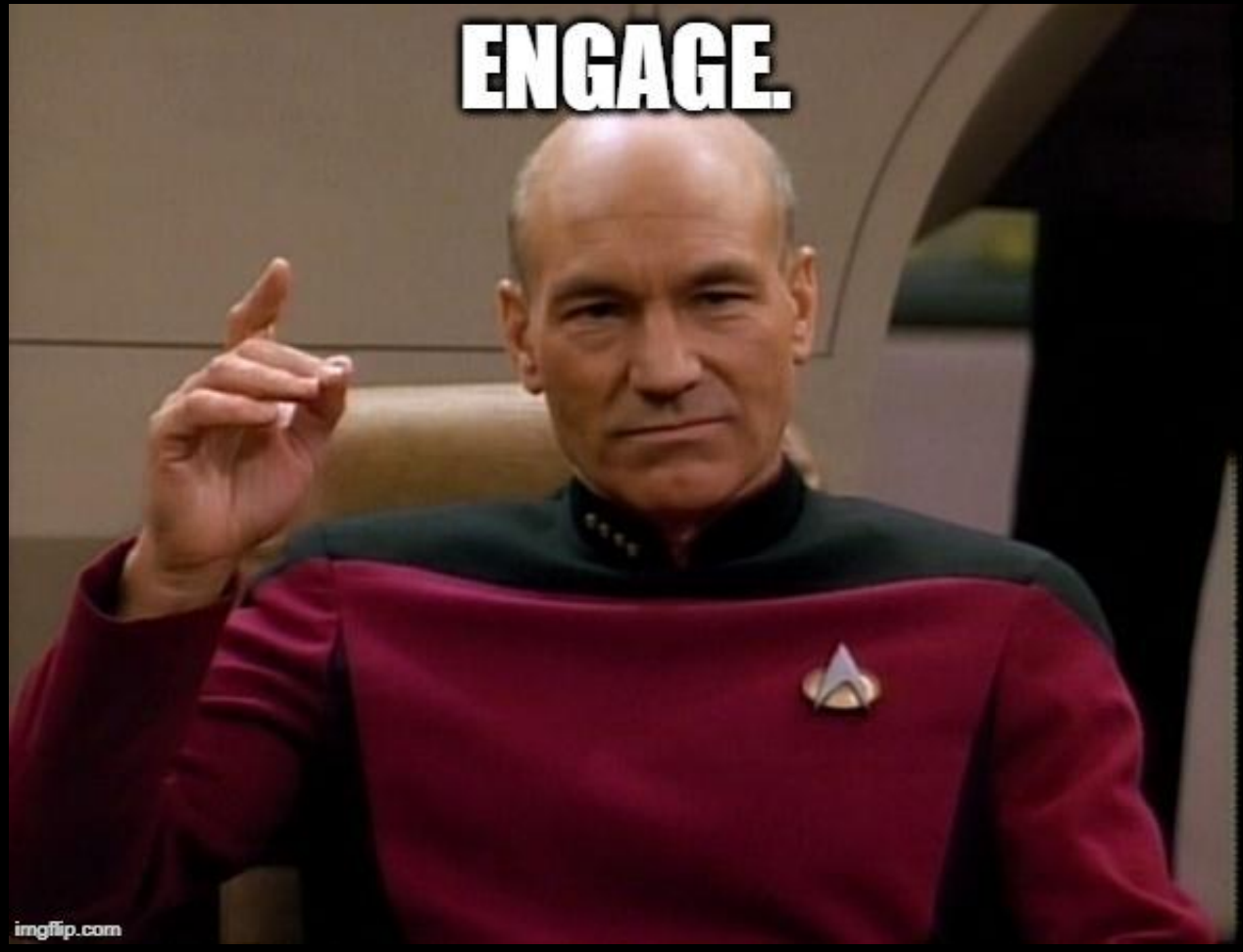
# Opportunities: Be the System Integrators


- YouTube→ SecureMeTube
- Consumer Security Review Site
  Ex. Internet of Shitdex
- Security Tools For Humans?
  Ex. Princeton IoT Inspector
- Authentication solution

# Opportunities: EU Research Funding


- https://ec.europa.eu/digital-single-market/en/newsroom-agenda/funding-opportunity/all/19/10/2019
- https://iot-epi.eu/
- https://www.eu-startups.com/startup-sourcing-research-service-for-investors-corporates/

# Opportunities: Ignore the Prime Directive


ENGAGE.
imgflip.com

# References:


The ‘S’ in ‘IoT’ stands for Security -Viktor Petersson (Screenly) and Andrew Martin (Control Plane) https://www.youtube.com/watch?v=PmWYTjr_Xso
Strava released their global heatmap… https://twitter.com/nrg8000/status/957318498102865920?lang=en
Coffee vs Tea Hackoff https://www.packetlabs.net/hackable-podcast-kettle/
Nest camera hacker threatens to kidnap baby, spooks parents https://www.nbcnews.com/news/us-news/nest-camera-hacker-threatens-kidnap-baby-spooks-parents-n949251
Hacker talks to baby through Nest security cam, jacks up thermostat https://nakedsecurity.sophos.com/2019/02/01/hacker-talks-to-baby-through-nest-security-cam-jacks-up-thermostat/
Thermostats, Locks and Lights: Digital Tools of Domestic Abuse https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
Lojack’d: Pwning Smart Vehicle Trackers https://www.pentestpartners.com/security-blog/lojackd-pwning-smart-vehicle-trackers/
http://smartlockpicking.com
Binary Hardening in IoT Products https://cyber-itl.org/2019/08/26/iot-data-writeup.html
Singapore’s Operational Technology Cybersecurity Masterplan https://www.csa.gov.sg/~/media/csa/documents/publications/ot_masterplan/otcybersecuritymasterplan.pdf
NERC-CIP Standards https://www.nerc.com/pa/Stand/Pages/Default.aspx
NIS Directive https://www.enisa.europa.eu/topics/nis-directive
Management of Security in Cyber Devices https://www.fda.gov/media/119933/download
EU Medical Devices Regulation https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices

# References (Continued):


Energiewirtschaftsgesetz -EnWG http://www.gesetze-im-internet.de/enwg_2005/__11.html
BSI TR-03148 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03148/index_htm.html
Senate Bill No. 327 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
Secure by Design https://www.gov.uk/government/collections/secure-by-design
MANDATING SECURITY REQUIREMENTS FOR CONSUMER 'IoT' PRODUCTS, Consultation Stage Impact Assessement
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf
Code of Practice for Consumer IoT Security
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
Inside consumer perceptions of security and privacy in the connected home
https://www.welivesecurity.com/2019/10/08/consumer-perceptions-security-privacy-connected-home/
Norton Core - Discontinued Product https://www.nortonsecurityonline.com/ns-us/norton-core.html
Princeton IoT Inspector https://iot-inspector.princeton.edu/
Cisco Survey Reveals Close to ¾ of IoT Projects are Failing
https://newsroom.cisco.com/press-release-content?articleId=1847422

# Media:

OpenClipart-Vectors https://pixabay.com/de/vectors/computer-netzwerk-router-server-159828/
ElsaRiva https://pixabay.com/de/illustrations/mobile-telefon-smartphone-handy-2468068/
OpenClipart-Vectors https://pixabay.com/de/vectors/kamera-hal-hal-9000-auge-159400/
OpenClipart-Vectors https://pixabay.com/vectors/ashamed-sad-silhouette-face-hand-154418/
Gio1135 https://pixabay.com/vectors/watch-wristwatch-time-clock-2649380/
Lumapoche https://pixabay.com/illustrations/the-cup-tea-png-2360104/
Kreatikar https://pixabay.com/illustrations/mobile-security-privacy-protected-3469818/
Public Domain Pictures https://pixabay.com/de/photos/geschwindigkeit-auto-limit-gefahr-164063/
OpenClipart-Vectors https://pixabay.com/de/vectors/tee-pokal-glas-untertasse-152609/
Geralt https://pixabay.com/de/illustrations/smart-home-haus-technik-multimedia-2769210/
Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, page 17 https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
WikiMichi https://commons.wikimedia.org/wiki/File:BMA_Automation_Allen_Bradley_PLC_3.JPG
Evan Emos https://commons.wikimedia.org/wiki/File:Duct-tape.jpg
Dietmar Rabich https://commons.wikimedia.org/wiki/File:D%C3%BClmen,_Umspannstation_--_2014_--_0005.jpg
FernaCM https://commons.wikimedia.org/wiki/File:Remote_Terminal_Unit_Modular.jpg
Un-perfect https://pixabay.com/de/photos/oma-opa-gro%C3%9Feltern-senioren-alt-3655814/
Clker-Free-Vector-Images https://pixabay.com/de/vectors/ma%C3%9Fstab-gerechtigkeit-richter-40635/
On a similar vein... https://twitter.com/synackpse/status/1177667702095335424

# Memes:

ImgFlip MemeGenerator https://imgflip.com/memegenerator
Action Movie FX https://apps.apple.com/us/app/action-movie-fx/id489321253


Checking your vitals...

**Nathan Ruser**
@Nrg8000

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee... ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

19:24 · 27.01.18 · Twitter Web Client

”Shields up, Mr. LaForge!“

# OT: System Integrators


- Must implement according to asset owner requirements
- Integrators in security training

# OT: Product Supplier


- **The Good**
  - Technical Controls
    - MAC & IP Whitelisting
    - VPN
    - SSH & SFTP
    - HTTPS
  - Procedural controls
    - CERT

- **The Bad**
  - Unencrypted protocols
  - Updates limited
  - Aging devices in the field

# Opportunities: Vulnerability Management


- Don’t Panic Package:
  - ISO 29147: Vulnerability Disclosure
  - ISO 30111: Vulnerability Handling Processes

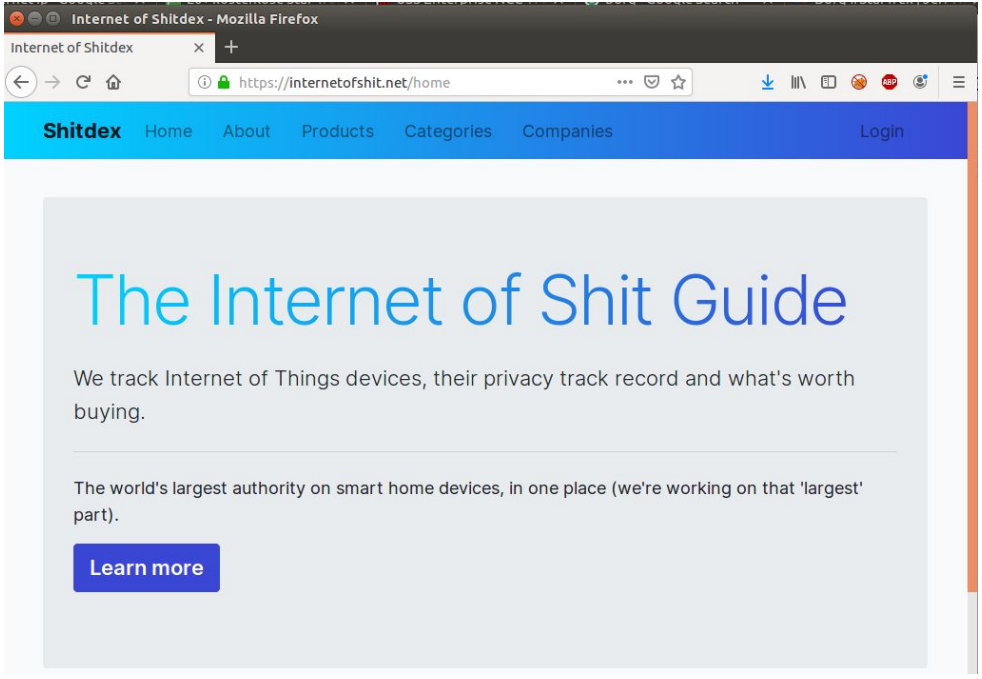
- Process for vendor that no longer exists?
  - 30% of IoT projects fail (Cisco, 2018)

# What about **consumer** IoT?

- **Legislation?**
  - Asset owners
  - Product suppliers
- **Standards?**

# Internet of “Shit”

Victor Petersson & Andrew Martin
The “S” in IoT Stands for Security (2018)



”Engage.”