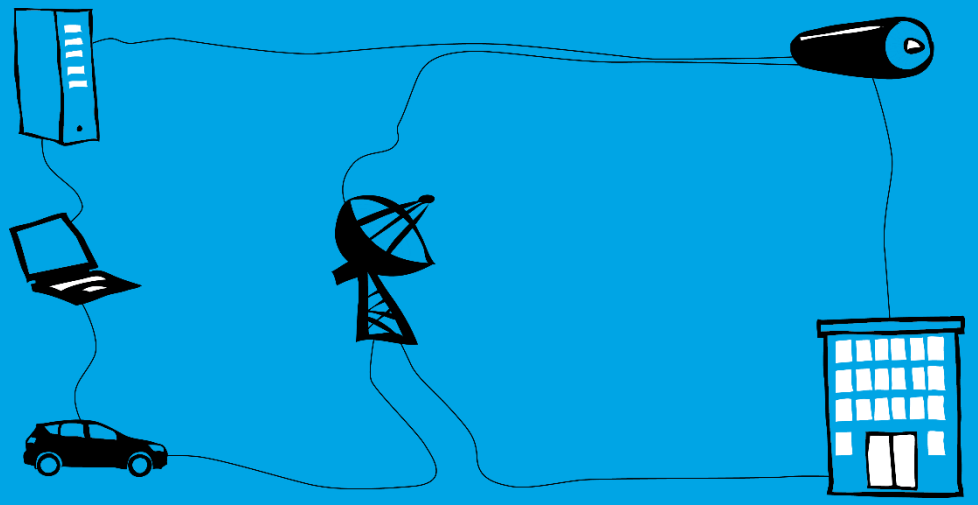
IoT device cyber security is becoming regulated - are you ready?

May 2019

Antti Tolvanen
Sales Director
Software & Embedded Solutions



Etteplan

https://www.youtube.com/watch?v=C0tpMb7I1GI

Etteplan – a growth company

Rapidly growing and developing engineering services company

Our customers are global machine and equipment manufacturers

We stand out by the high-level competence and service attitude

Founded 1983 | Nasdaq Helsinki Ltd

Etteplan

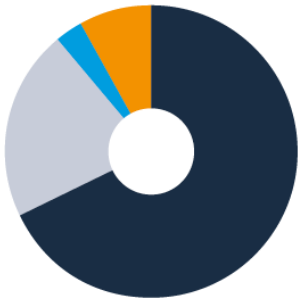
~236

REVENUE, EUR MILLION 2018

> 3,000

NUMBER OF PERSONNEL 2018

Revenue by geographical area 2017 (2016)



- Finland 68% (68%)
- Sweden 21% (23%)
- China 3% (2%)
- Central Europe 8% (7%)

Revenue by service area 2017 (2016)

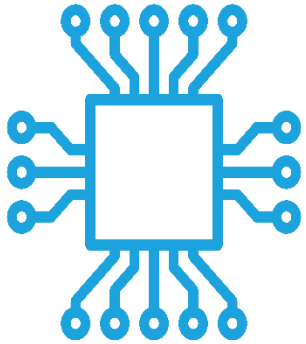
- Engineering services 56% (61%)
- Embedded systems and IoT 25% (19%)
- Technical documentation 19% (20%)

Revenue by customer segment 2017

- Forest and paper 13%
- Energy and power transmission 13%
- Industrial machinery and components 12%
- Lifting and hoisting equipment 11%
- Mining 11%
- ICT 7%
- Transportation and vehicle 6%
- Aerospace and defense 4%
- Medical technology 4%
- Metal 4%
- Consumer products 2%
- Others 13%

Software & Embedded Solutions – chip to app

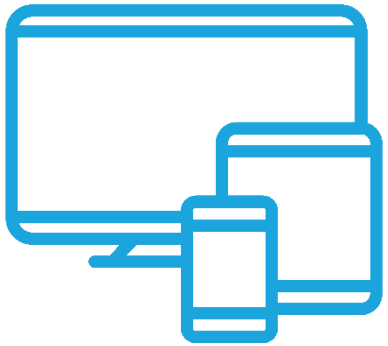
Embedded Products and Systems



Connectivity

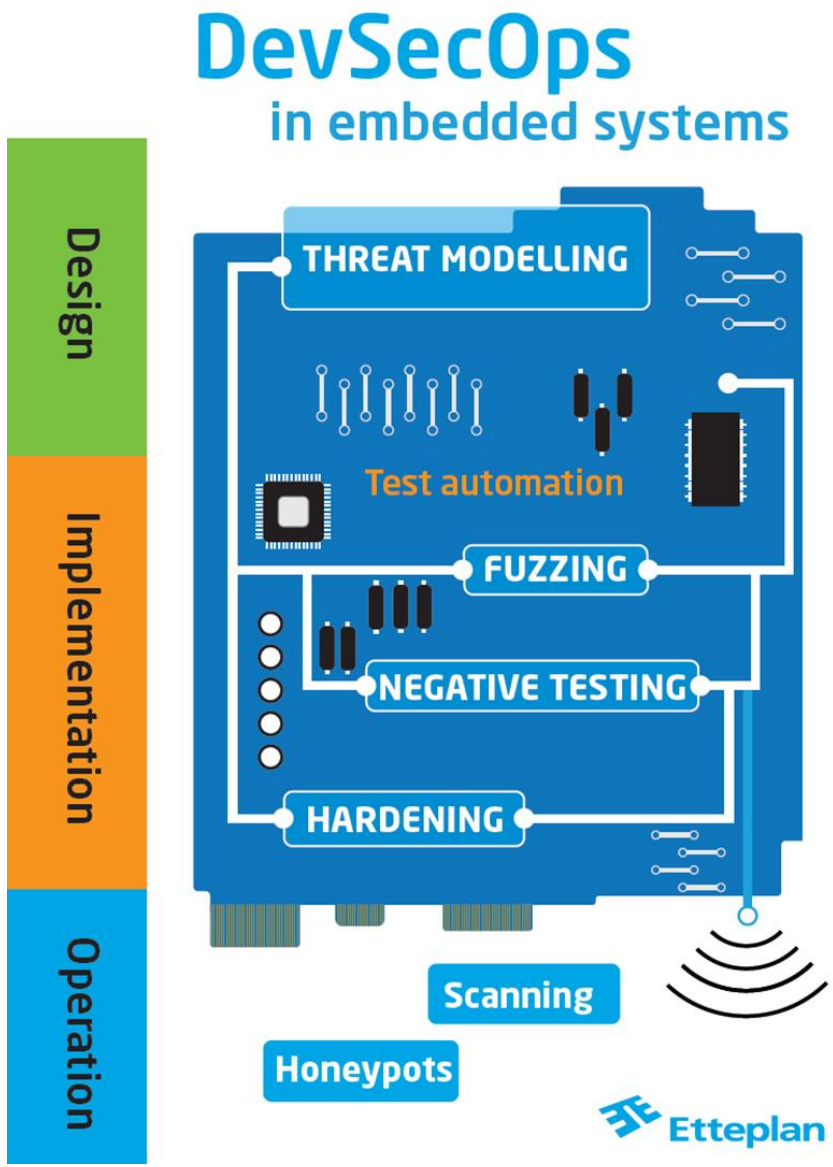
IoT Cloud Services

Value-adding Applications and User Interfaces



SW test automation
Cybersecurity consulting & testing
RF & antenna design
Accredited EMC & RF Test Lab
Production testing equipment & automation

UX, Web/Mobile, Analytics, Integrations/Backend
Digitalized business models enablement
(e.g. solution business, after-sales)
24/7 application management services
(including field service)



Embedded Cybersecurity

Security-oriented QA Specialists

- Broad knowledge and experience of embedded systems, including medical devices
- Ability to support pre- and post-market vulnerability management and product security program development

Threat Modelling (Architectual Risk Analysis)

- Discovery and assessment of weaknesses using STRIDE methods
- Workshops, trainings, and learning materials

Linux System Hardening

- Guidance on how to securely develop code and configure Linux-based embedded systems

Fuzz Testing

- With experience of a variety of tools and methods the best applicable approaches are used

Vulnerability Scanning

- F-Secure Radar and other tools for scanning IP-connected devices and systems
- Tools for scanning binaries and source code to identify known and unknown vulnerabilities

Penetration Testing

- Skills and experience of penetration testing, including cloud and web systems

Shock at the wheel: your Jeep can be hacked while driving down the road

July 23, 2015

Oops, they've done it again: after two successful breaches into the systems of Toyota Prius and Ford Escape, security researchers Charlie Miller and Chris Valasek have recently hacked a Jeep Cherokee.

WIRED
@WIRED

Hackers remotely kill a Jeep on the highway — with me in it
wrd.cm/1HNWxrL

1,053 2:44 PM - Jul 21, 2015

2,265 people are talking about this

CNN BUSINESS Markets Tech Media Success Perspectives Video

Cyber-Safe

Chrysler recalls 1.4 million hackable cars

by David Goldman @DavidGoldmanCNN

July 24, 2015: 4:29 PM ET

What a hacked Jeep looks like on the road

Chrysler is recalling 1.4 million vehicles that can be remotely hacked over the Internet.

- https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Cybersecurity regulations in EU, USA, China

Hard Law - legislation

- EU Cybersecurity Act (effective)
- EU Cybersecurity Certification schemes (under development)
- UK Consumer IoT security (proposal)
- US Cybersecurity Improvement Act (IoT devices for US government, under development)
- US Medical Devices Draft Pre-Market Cybersecurity Guidance (draft, under development)
- China Measures for the Security Review of Network Products and Services (for Trial Implementation) (effective)

Soft Law - standards

- EU Consumer IoT standard (effective)
- Voluntary Cybersecurity Certification Programs

Summary

- Additional benefits of IoT device cybersecurity regulation

EU Cybersecurity Act March 2019

- Mandates European Union Agency for Network and Information and Security, ENISA
  - Defend EU against Cyber Attacks with focus on Operators of Essential Services and Digital Services
  - Prepare for the Commission candidate cybersecurity certification schemes that are specific for different products, services and processes

- Establishes EU framework for cybersecurity certification of ICT products, services and processes
  - Develop single market for IoT devices in EU (today national certification schemes, e.g. CPA in UK)
  - Certification will be voluntary, unless explicitly mandatory by EU or member state Law

→ Let's take a look at the Cybersecurity Certification legislation from IoT device perspective

Source: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf

EU Certification – High Level Requirements

Product

- Protects data (and availablility of data) during entire life cycle
- Manages and records all access to data, services and functions
- Recovers in timely manner from hardware or software malfunction / incident / anomaly
- Provided with up-to-date SW and HW, and with mechanisms for secure updates

Design & testing process

- Secure by default and design
- Known 3rd party SW dependencies have been identified (traceability)
- It has been verified that there are no known vulnerabilities

Post-market surveillance

- Vulnerability reporting to customers or authorities (Viestintävirasto in Finland)

Labeling

- Instructions for secure configuration, installation, operation and maintenance
- Period for cybersecurity related support and updates
- Contact information for providing identified vulnerabilities to manufacturer
- Link to repository with publicly known vulnerabilities

Source: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf

Cybersecurity Certification Assurance Levels

Basic

- Evaluation vs requirements at level intended to minimise the **known basic risks of incidents and cyberattacks**.
- Review of technical documentation (at least)
- Conformity self-assessment may be possible

Substantial

- Evaluation vs requirements at a level intended to minimise the known cybersecurity risks, and the risk of incidents and **cyberattacks carried out by actors with limited skills and resources.**
- The evaluation activities to be undertaken shall include at least the following:
  - a review to demonstrate the absence of publicly known vulnerabilities and
  - testing to demonstrate that the necessary security functionalities are correctly implemented.

High

- Evaluation vs requirements at a level intended to minimise the risk of **state-of-the-art cyberattacks carried out by actors with significant skills and resources.**
- The evaluation activities to be undertaken shall include at least the following:
  - a review to demonstrate the absence of publicly known vulnerabilities;
  - testing to demonstrate that necessary security functionalities are correctly implement the at the state of the art;
  - an assessment of their resistance to skilled attackers, using penetration testing.
- Certificate will be issued by national cybersecurity certification authority, or accredited conformity assessment body to whom the task is delegated

Source: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf

Essential Services are in focus of certification

Essential Services

- Electricity
- Oil
- Electricity
- Gas
- Air transport
- Rail transport
- Water transport (incl port equipment)
- Road transport (incl infrastructure, vehicles, users)
- Banking
- Financial market infrastructure
- Health sector
- Drinking water supply and distribution
- Digital Infrastructure

Digital Services

- Online marketplace
- Online search engine
- Cloud computing service

From voluntary to mandatory certification schemes

- As next step, ENISA implements voluntary cybersecurity certification schemes with focus on ICT products, services and processes used by Essential Services Operators
- Several schemes appear to be under drafting/ development, e.g. Consumer IoT standard published, 5G risk analysis ongoing
- Medical & In Vitro Device Regulations: state-of-the-art information security required → certification scheme under development??
- Latest in 2023 European Commission assesses which certification schemes should be made mandatory through EU law to improve cybersecurity and internal market

Sources: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

5G certification scheme development ongoing

- 5G networks risk assessment by Oct 1st 2019:
  - Supply chain risks
  - Software vulnerability risks
  - Access control risks
  - 3rd country (outside EU) legal and policy framework risks

- Toolbox for 5G networks cybersecurity by Dec 31st 2019:
  - Security risks inventory (as above)
  - Mitigating measures that address each identified risk, e.g.
    - 3rd party conformity testing / certification of Products, Software, Services
    - Processes to ensure that access controls exist and are enforced
    - Identification of insecure product and services suppliers

- Voluntary certification scheme in 2020?

Source: https://ec.europa.eu/commission/news/common-eu-approach-security-5g-networks-2019-mar-26_en
https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

Consumer IoT cybersecurity standard published

ETSI TS 103 645 V1.1.1 (2019-02)

CYBER;
Cyber Security for Consumer Internet of Things

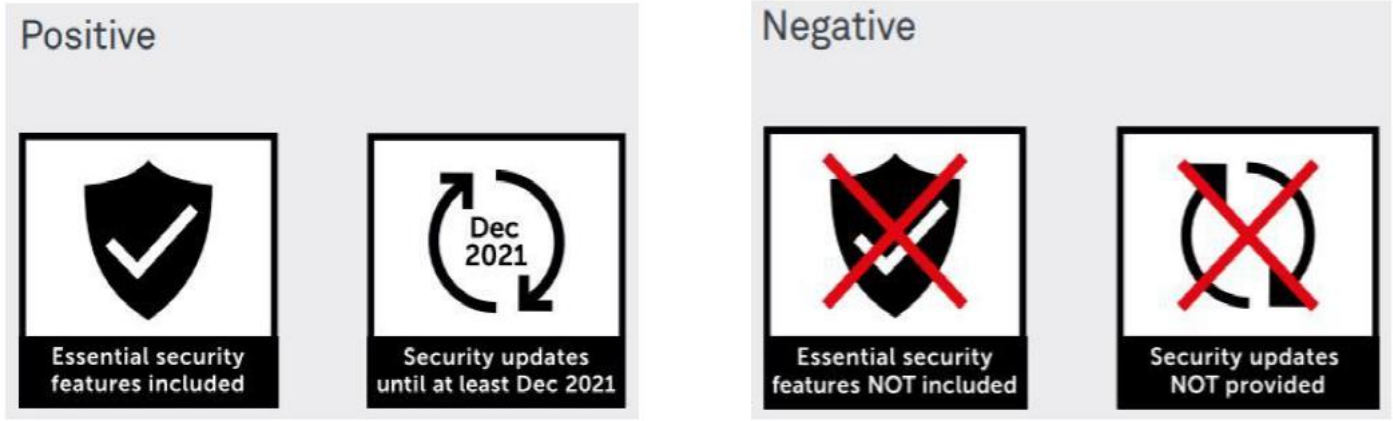
- Each section of the standard contains one or several requirements, which are either mandatory or recommended

Source: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

UK consumer IoT minimum requirements (draft)

To be decided : Retailers may sell products that

- Option A: have IoT security label (self assessment)
- Option B: have IoT security label and have been self assessed against ”top 3 guidelines”
  - Unique passwords that are not resettable to a universal factory setting
  - Public point of contact for vulnerability disclosure
  - Minimum lenght of time for security updates



- Option C: have IoT security label that shows compliance with complete ETSI TS 103 645 ”13 guidelines”

Etteplan

Source: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798721/Consultation_on_the_Government_s_regulatory_proposals_regarding_consumer_Internet_of_Things_security.pdf*

US Cybersecurity improvement act / NIST draft

→ **Cybersecurity requirements for IoT devices purchased by US government**

Core IoT device cybersecurity capabilities' baseline

1. …can be identified both logically and physically.
2. …software and firmware can be updated using a secure, controlled, and configurable mechanism.
3. Authorized users can securely change the IoT device's configuration, including restoration to a secure "default." Unauthorized changes to the IoT device's configuration can be prevented.
4. Local and remote access to the IoT device and its interfaces can be controlled.
5. …can use cryptography to secure its stored and transmitted data.
6. …can use industry-accepted, standardized protocols for all layers of the device's transmissions.
7. …can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems
8. …can be reset by authorized users so all data-at-rest on the device is securely removed from all internal data storage.

Sector-specific add-on requirements

9. Information confirming the sources of all of the IoT device's software, firmware, hardware, and services is disclosed and accessible.
10. An inventory of the IoT device's current internal software and firmware, including versions and patch status, is disclosed and accessible.
11. …can enforce the principle of least functionality through its design and configuration.
12. …is designed to allow physical access to it to be controlled.

Source: https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

China cybersecurity law

Measures for the Security Review of Network Products and Services 2017

- Mandatory Cybersecurity Review of network products and services procured by operators of Critical Information Infrastructure, which are important for national security,
  - Similar list as in EU
- Evaluation by 3rd Party Cyber Security Evaluation Centers / Agencies of
  - Product/service security risks
  - Supply chain security risks
  - Provider-related illegal use(r) data collection and installed base exploitation risks
  - National security risks

Standards

- The Chinese government has issued close to 300 new national standards related to cybersecurity of network products and services over the past several years. “TC260”
  - Product reviews may require IP and source code
  - Not necessarily compatible with international standards
  - Multiple standards will be applicable
  - Standards are not easily available via google

Source: https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_final_regulation_on_cybersecurity_review_of_network_products_and_services.pdf
https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china

Etteplan

https://youtu.be/_mkRAArj-x0

FDA cybersecurity design requirements

A. Identify and Protect Assets and Functionality
1) Prevent Unauthorized Use (Overall)
a) Limit Access to Trusted Users & Devices
i) User authentication
ii) Automated timed termination
iii) Layered authorization (privilege control)
iv) Appropriate privileged authentication and access
v) Password strength and secrecy
vi) Physical protection
b) Authentication and authorization of safety-critical commands
i) Authentication to prevent unauthorized access to and (arbitrary) execution of software or functions
ii) Authentication before update
iii) Cryptographically strong locally stored authentication and/or communication
iv) All external connections mutually authenticated
v) Firmware and software authentication. Metadata authenticated.
vi) Irrefutable evidence based authorization checks
vii) Deny by default design
viii) Least privilege principle
2) Ensure trusted content
a) Code integrity
i) Cryptographically verified firmware/software with rollback prevention
ii) Validate integrity of software (if feasible)
b) Data Integrity
i) Verify integrity of incoming data
ii) Ensure secure data transfer capabilities
iii) Integrity of safety and performance critical data
iv) Use NIST cryptography standards or equivalent for communication channels
v) Unique per device cryptographically secure communication key
c) Execution integrity - Industry accepted best practises to maintain/verify integrity of code while executed on the device.
3) Maintain Confidentiality of Data (credentials, data "at rest" and "in transit", protected health information)

B. Detect, Respond, Recover
1. Design for Cybersecurity Events Detection
a) Implement design features for detection, recognition, logging, timing and action on security compromises
b) Permit routine security and antivirus scanning on device without loss of performance
c) Ensure design enables forensic evidence capture
d) Vulnerability impact limited
e) Software configuration management and tracking electronically
f) Product life-cycle facilitates variant analysis
g) CBOM in machine readable electronic format to be consumed automatically
2. Design to Respond and Contain
a) Notification of potential breach
b) Anticipate future patches and updates for vulnerabilities
c) Facilitate rapid verification, validation, and testing of patches and updates
d) Rapid deployment of patches and updates
3. Recover impaired capabilities or services
a) Protect critical functionality
b) Methods for retention and recovery of device configuration by authenticated user
c) Specify level of autonomy of any component when its communication is disrupted
d) Resilience to cybersecurity incidents

Source: https://www.fda.gov/media/119933/download

FDA cybersecurity risk/testing documentation requirements

1. Threat model, including supply chain, design, production, deployment into use
2. All cybersecurity risks that were considered in design, with analysis of exploitability
3. List of cybersecurity controls with justifications and verifiable requirements
4. Cybersecurity test reports should include
   - Performance testing
   - Evidence of 3rd party SW security effectiveness
   - Static and dynamic code analysis incl “hardcoded” credentials testing
   - Vulnerability scanning
   - Robustness testing
   - Boundary analysis
   - Penetration testing
   - Third Party testing reports
5. Traceability matrix
6. Cybersecurity BOM cross-referenced with National Vulnerability Database
   - Cybersecurity Bill of Materials (CBOM) – a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities.

Source: https://www.fda.gov/media/119933/download

FDA Cybersecurity labeling (manual) requirements

Configure

- Secure configuration for hardening

Install

- System diagrams sufficient for end-users
- Supporting infrastructure requirements
- Description of enabled network ports and interfaces
- Recommended cybersecurity controls in use environment (firewalls etc)

Update

- Procedure for downloading SW / FW updates
- CBOM so users can manage assets, understand impact of identified vulnerabilities and deploy countermeasures
- Information when cybersecurity support ends (patches)
- Secure network (connected) deployment and servicing

Detect, Respond, Contain

- Features that protect critical functionality if cybersecurity is compromised
- How device announces anomalous conditions and security events
- How to respond upon detection of vulnerability or incident
- How device captures forensic evidence and how log files can be automatically consumed for analysis
- Backup & restore, recovery of device configurations

Source: https://www.fda.gov/media/119933/download

Some voluntary cybersecurity certifications

- **UL 2900 Software Cybersecurity of Network-Connectable Products**
  - -1 General requirements (all devices with connectivity)
  - -2-1 Healthcare and wellness systems (medical, IVD, consumer)
  - -2-2 Industrial control systems (PLC, DCS, etc)
  - -2-3 Security and life safety signaling systems (anti-theft, alarms, CCTV, fire alarm, access control etc.)
  - Certification by UL

- **Platform Security Architecture (ARM, UL, others)**
  - Common certification framework for chip makers, OS providers and device makers
  - Level 1-3 certification for silicon vendors (HW), Level 1 for OS providers and device makers

- **CTIA**
  - US Wireless communication industry Cybersecurity certification program for LTE and WIFI IoT devices
  - Very good test plan available on web site

Source: https://standardscatalog.ul.com/standards/en/standard_2900-1_1
https://www.arm.com/company/news/2019/02/arm-and-leading-test-laboratories-unveil-independent-security-certification
https://api.ctia.org/wp-content/uploads/2019/05/ctia_IoT_cybersecurity_pmd_ver-1_1.pdf

Additional benefits of IoT cybersecurity regulation

Log data should be used in threat monitoring

- ETSI Consumer IoT: If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.
  - Examining telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimizing security risk and allowing quick mitigation of problems.
- CTIA LTE & WIFI IoT: Implement design features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use.
- FDA Medical IoT: Devices should be designed to permit routine security and antivirus scanning such that the safety and essential performance of the device is not impacted.

Benefits for solution business models

- The same device log data that should be used for security evaluation also acts as foundation for solution/service business models in e.g. predictive/condition-based maintenance

→ Cybersecurity regulation might help in getting permission from end-users to gather use data for threat monitoring and for solution business models

Summary

- EU and USA intend to regulate IoT device cybersecurity via requirements, standards and certification schemes.
- Purchasers will learn about and enforce voluntary cybersecurity standards as soon as first compliant products are available
- Mandatory IoT device cybersecurity certifications are likely over next 5 years, especially related to critical infrastructure/essential services, personal data, safety critical equipment, payments.
- The cybersecurity regulation could enable new business models that are based on IoT device data, as the same data should be used for threat monitoring

Etteplan