FUJITSU

shaping tomorrow with you

IoT Week 2018

IoT Security & Data Protection at a Crossroad

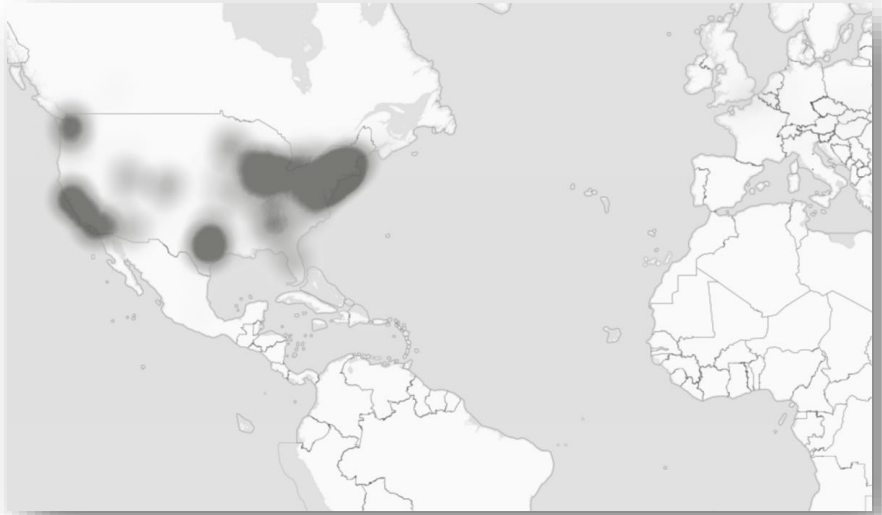
IoT Week Bilbao 2018
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Dr. Jürgen Neises
Enterprise & Cyber Security CE

© 2018 FUJITSU

Challenges of the Global Value Chain

- Industrial security, without cyber security-by-design, security by default is no longer acceptable
  - Otherwise there is a mutual "danger from attacks"
- There is also a fundamental need for trustworthy, secure communication
  - Establishing in Europe and globally the same **scheme of trustworthiness and identity** (e.g. to foster M2M contracting)
- Long investment periods, traditionally slow technological change cycles in industry and the associated inertia
- Core requirement for “Interconnectivity’ of Industry participants :
  - Secure cross-fields, -companies, -countries, -continents, and -sectors communication
- Convergence of autonomous systems



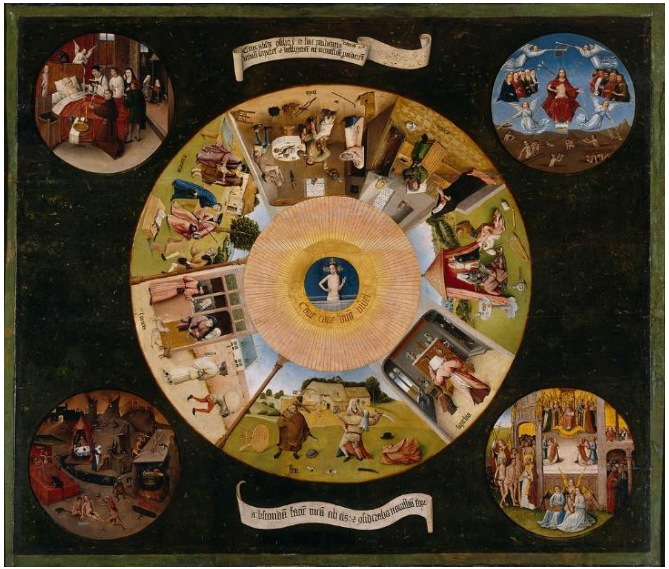
Source: https://commons.wikimedia.org/wiki/File:Level3_Outage_Map_(US)_-_21_October_2016.png

© 2018 FUJITSU

The seven deadly Sins of IoT

FUJITSU

Observations
By Hieronymus Bosch



Source: https://de.wikipedia.org/wiki/Bilder_von_Hieronymus_Bosch#/media/File:Hieronymus_Bosch-The_Seven_Deadly_Sins_and_the_Four_Last_Things.JPG

Sins
that cannot be forgiven easily

- **Pride:** totally easy
- **Greed:** too little time
- **Sloth:** lack of tests, agile “planning”, inconsistent management
- **Lust:** quick satisfaction without sustainability
- **Wrath:** cancel the user from the project equation
- **Envy:** the "soft" factor is underestimated in many places
- **Gluttony:** all in one go

© 2018 FUJITSU

How to improve the situation?

- Day-to-day security monitoring and risk mitigation
  - Holistic threat management and Cyber Threat Intelligence using data collection and data analytics for predictive IoT Security.
- Interoperability in the value chain
  - Measures to evaluate Trustworthiness.
- Risk assessment and compliance auditing
  - Flexibility in implementing different rules
  - Risk and vulnerability management.
- Refocus development to Security, Privacy and Trust to by-Design/by-Default and support developers implementing the best means for that.

Sóurce https://journal.jp.fujitsu.com/en/2016/03/17/01/

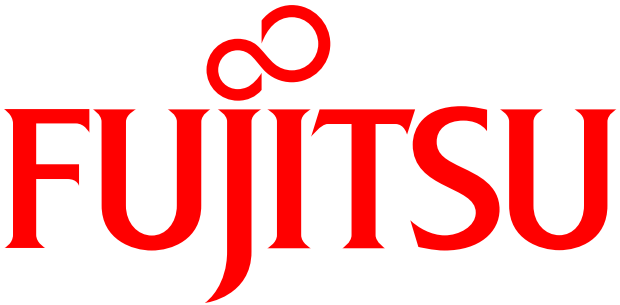
© 2018 FUJITSU

Need to reconcile the Stakeholders‘ Interests

FUJITSU

- The industry should properly implement and update what can be secure.
  - Industrial security, without cyber security-by-design, security by defaults is no longer acceptable
  - The integrity of the value chain is necessary, such that end users can have confidence in its security.
- Often ill-considered implementation of IoT solutions may endanger business success and the daily life of everyone.
  - For these reasons the market will offer a wide range of business opportunities for Security services.
- Holistic IoT-Security may contrast with data protection.
  - Collect and analyse electronic communications metadata for network and information Security purposes.
  - Access the capabilities of devices to manage vulnerabilities.

© 2018 FUJITSU



shaping tomorrow with you