FED4FIRE
FEDERATION FOR FIRE PLUS

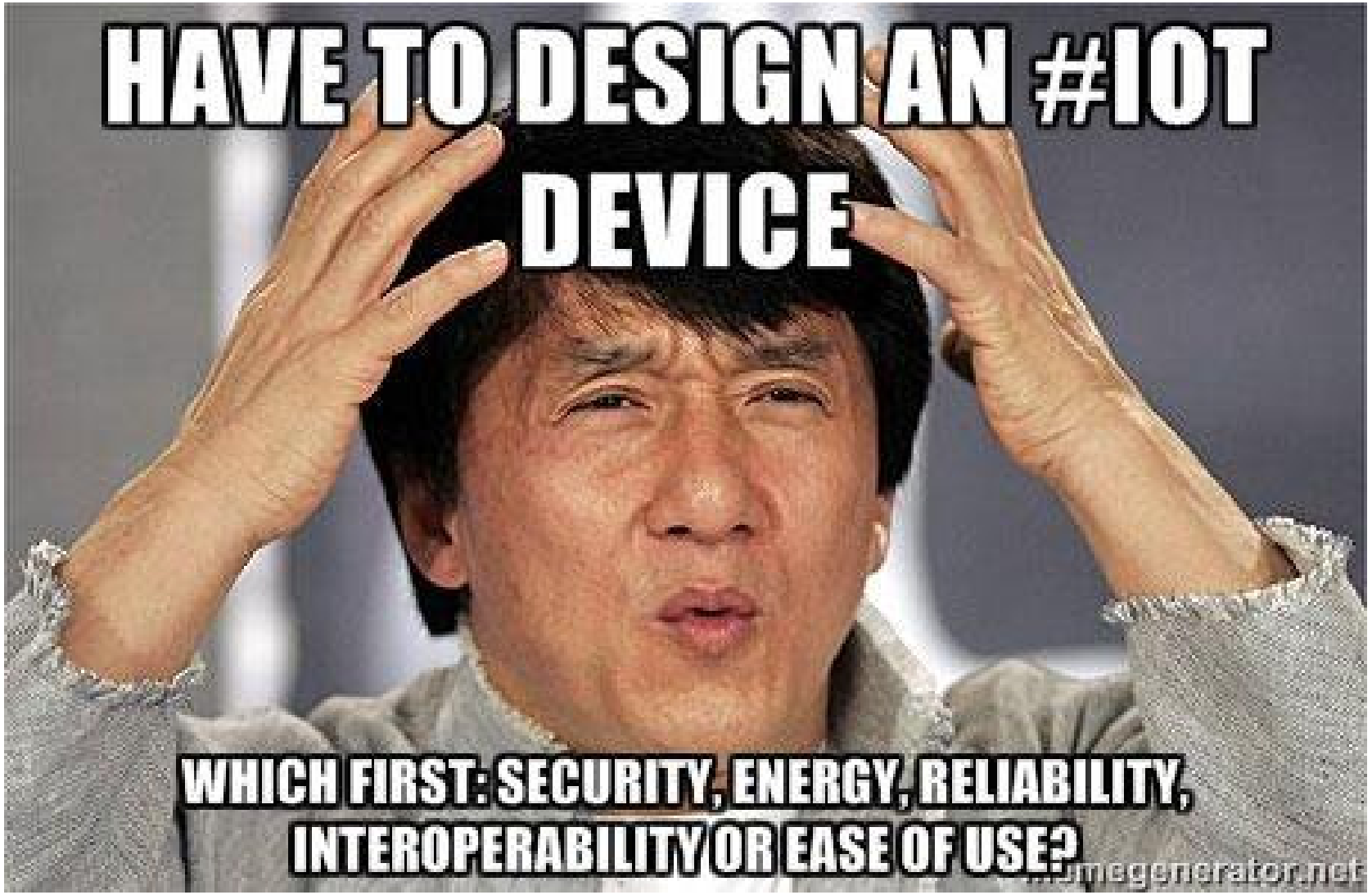
IOTWeek | Aarhus, 17-21 June 2019

CReAT – Cybersecurity Risk Assessment Framework for IoT Platforms

Session: IoT Risk Assessment & Management

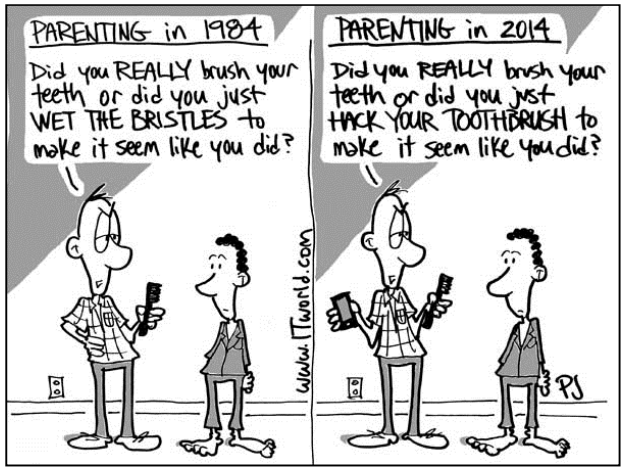
Soumya Kanti Datta
soumya@digiotouch.com

Digiotouch


HAVE TO DESIGN AN #IOT DEVICE
WHICH FIRST: SECURITY, ENERGY, RELIABILITY, INTEROPERABILITY OR EASE OF USE?
memegenerator.net

Cyberattack resilience and privacy

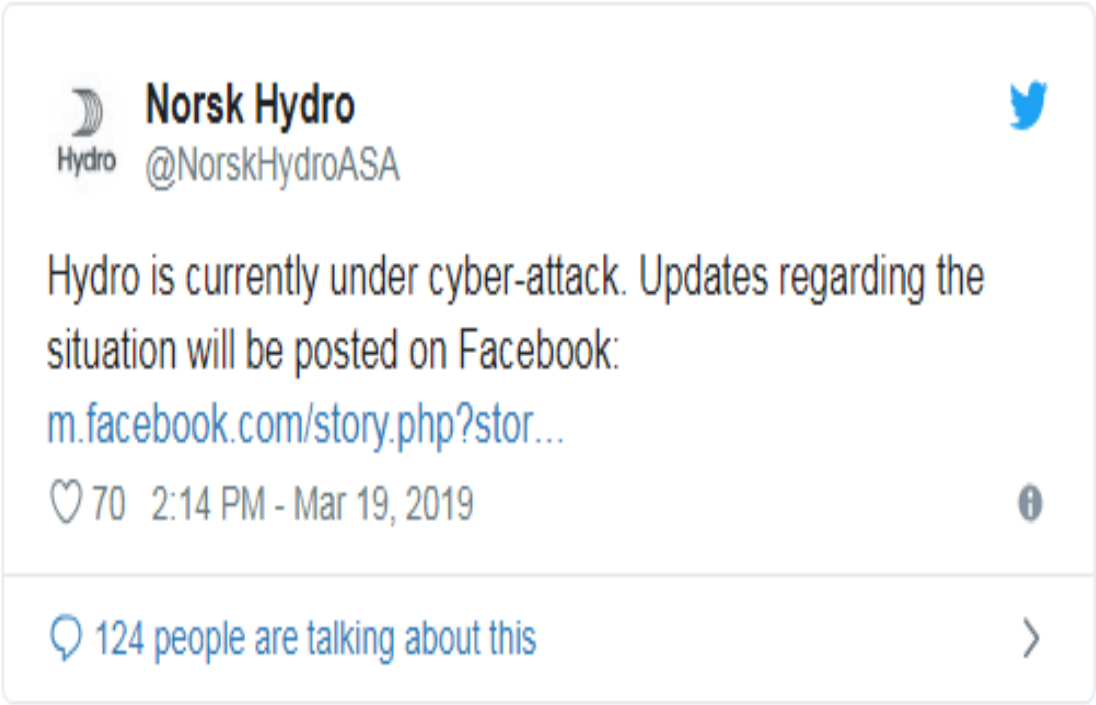
- Cyber-criminals stepping up attacks on IoT systems
- Privacy concerns in disruptive technologies
- No uniform Cyberattack resilience methodology



Source: http://www.itworld.com/

Increased attacks …

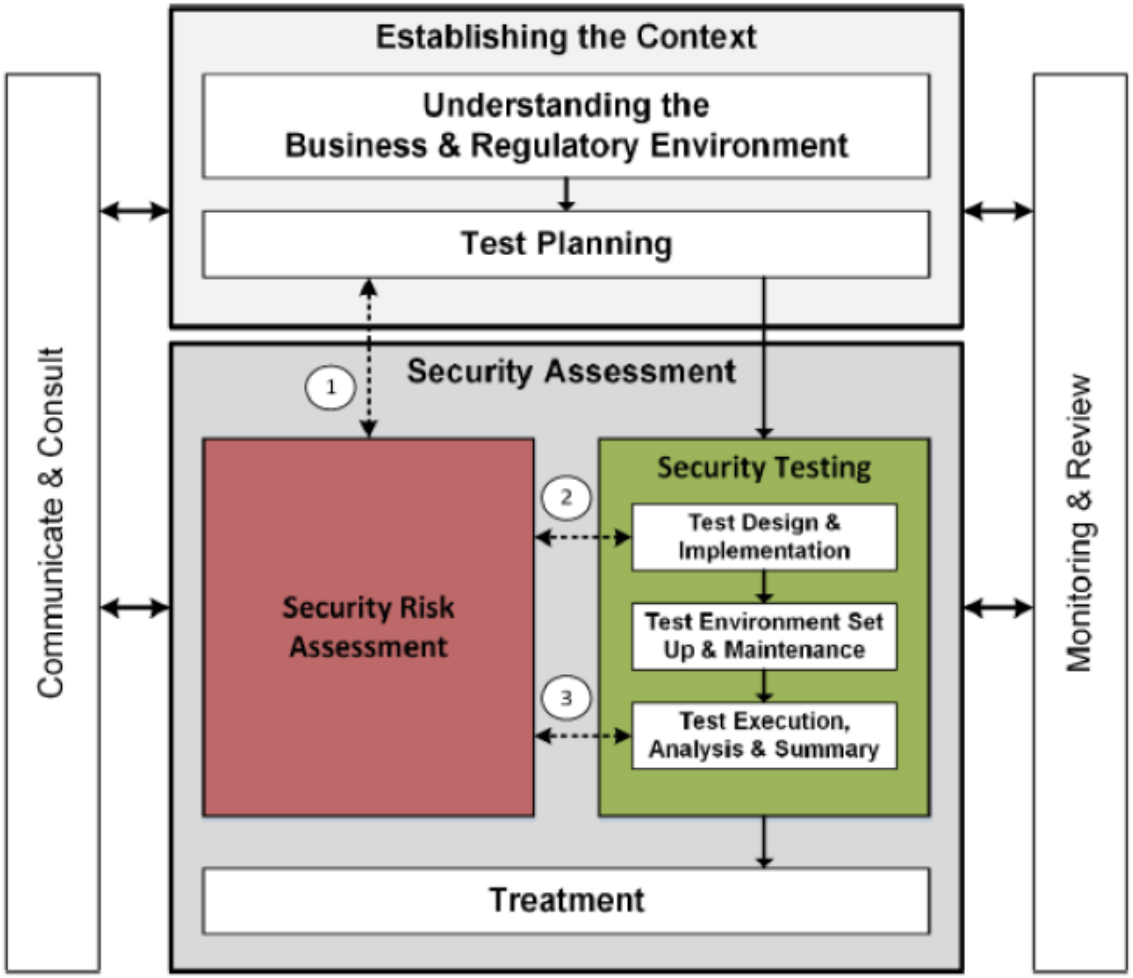
- Multiple DDoS attacks led to inaccessibility of Github, Twitter, and more in October 2016.
  - Attacks carried out by IoT devices including printers, IP cameras, and baby monitors.
- Stuxnet – malicious computer program targeting industrial computer systems around a decade ago.



Growing concerns …

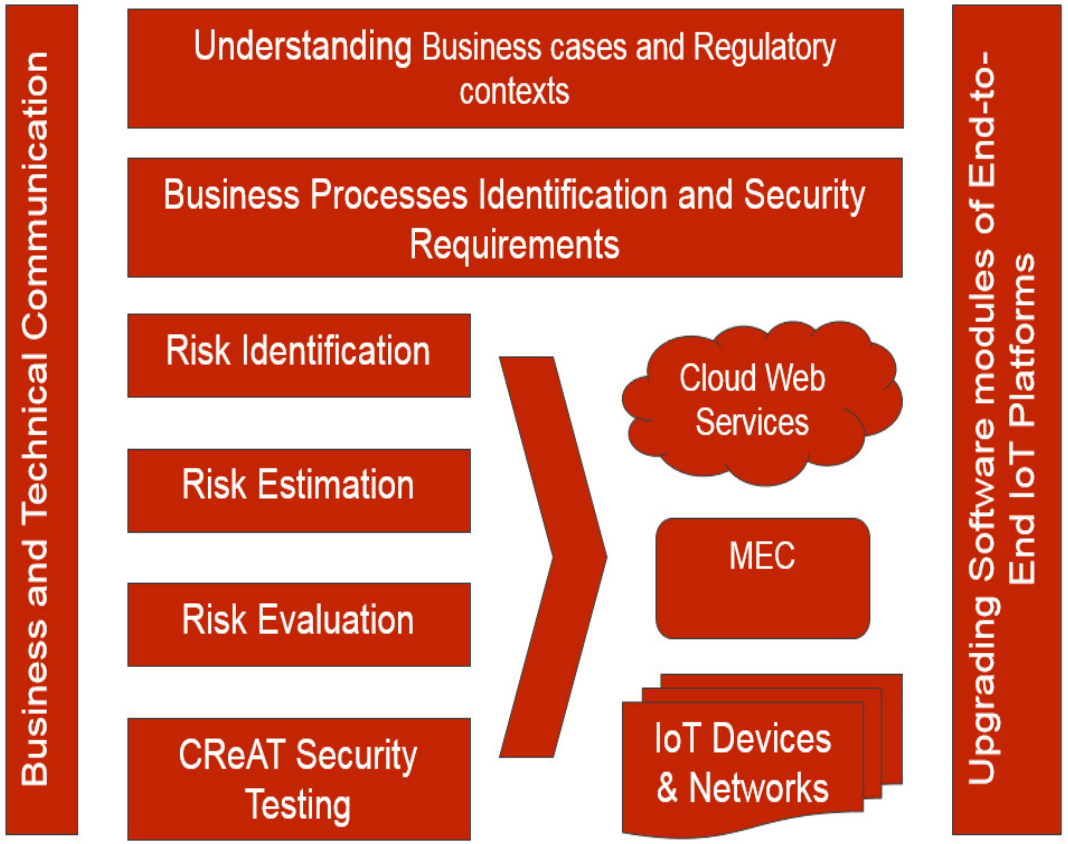
- Critical infrastructure being targeted
- Legacy systems that do not handle latest security protocols
- Lack of standards for Industrial IoT security
- Scalability
- 32% of IIoT devices connect directly to the internet, bypassing traditional IT security layers.
- Almost 40% said identifying, tracking and managing devices represented a significant security challenge.
- Only 40% reported applying and maintaining patches and updates to protect their IIoT devices and systems.
- 56% cited difficulty in patching as one of the greatest security challenges
  - More info - https://www.themanufacturer.com/articles/iiot-security-endpoints-most-vulnerable-aspect/

Cybersecurity Risk Assessment – ETSI Framework

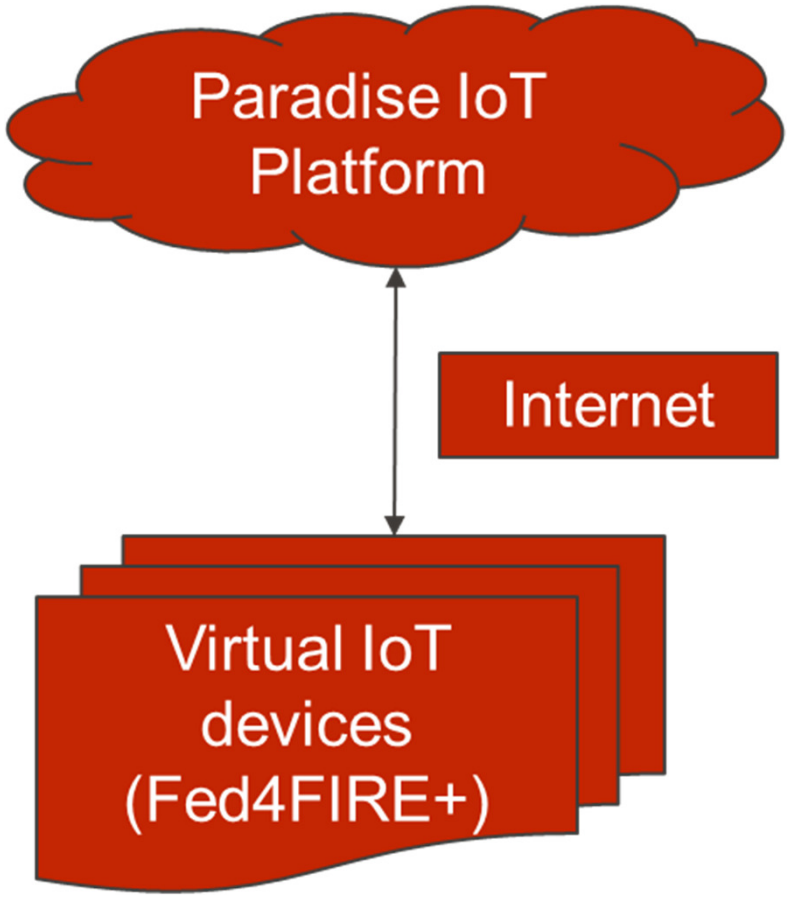


- OWASP Application Security Verification Standard Project
- Microsoft's STRIDE
- Common Vulnerability Scoring System

CReAT Framework for Cybersecurity Risk Assessment



CReAT Framework Testing in Fed4FIRE+



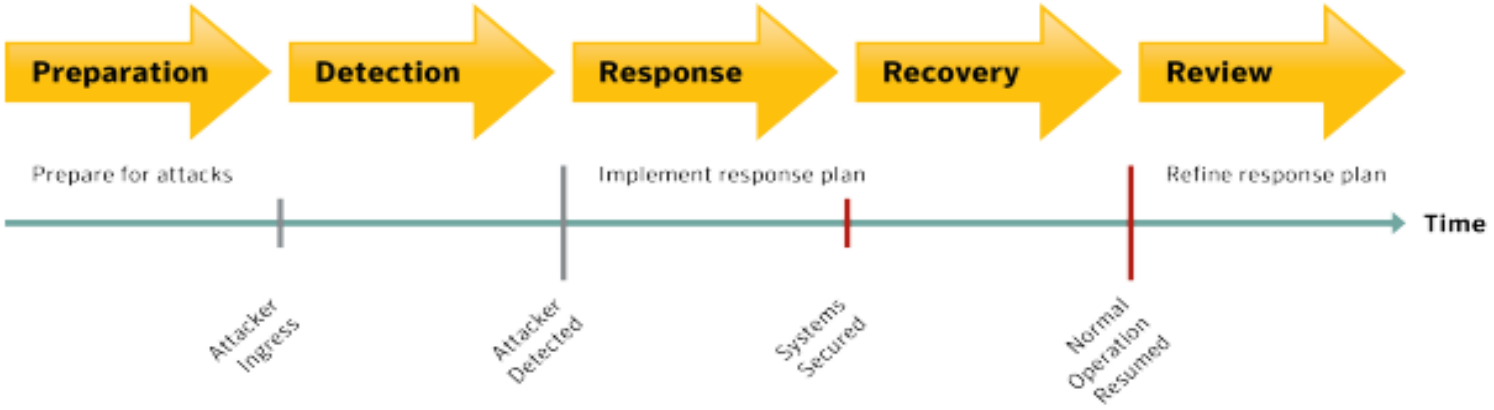
Risk assessment in terms of

- DDoS detection
- Insufficient authentication, authorization
- Insecure Cloud web services

No security breach observed

Cyber Resilience

- Ability to prepare for, respond to and recover from cyber attacks.
  - It helps an organisation protect against cyber risks, defend against and limit the severity of attacks, and ensure its continued survival despite an attack.
- Emerged over the past few years because traditional cyber security measures are no longer enough.
- It is now commonly accepted that it's no longer a matter of 'if' but 'when' an organisation will suffer a cyber attack.



Source: Symantec Whitepaper

Four Step Approach

Manage and Protect

- Malware protection
- Data security
- Identity and access control
- Encryption, network security …

Identify and detect

- Continuous monitoring of network and information systems to detect anomalies and potential cyber security incidents before they can cause any significant damage.

Respond and recover

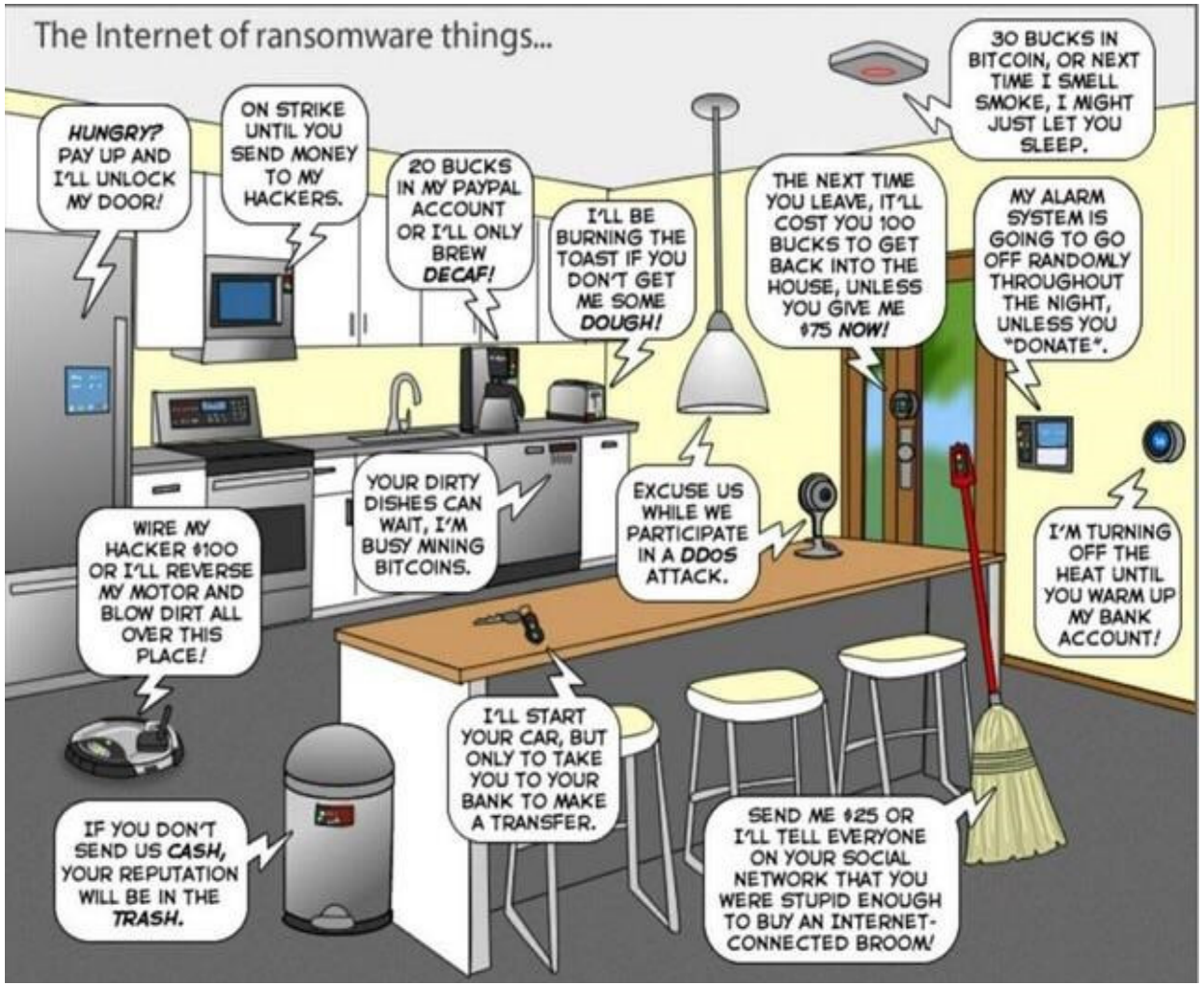
- Incident response management program
- Measures to ensure business continuity
- Restore normalcy as soon as possible

Govern and assure

- Such program and measures are a part of enterprise organization and built into business.

Conclusion

- Risk assessment must be performed at the early phases of product and service definition, development.
- Security, privacy, and trust are key aspects when designing winning UX.



Source - https://www.reddit.com/r/Iota/comments/6axglx/how_does_iota_help_with_the_huge_iot_security/

Acknowledgement

Co-funded by the European Union

Co-funded by the Swiss Confederation

FED4FIRE
FEDERATION FOR FIRE PLUS

- The work leading to this presentation is a part of CReAT experiment of Fed4FIRE+.
- Fed4FIRE+ project has received funding under grant agreement No 732638 from the Horizon 2020 Research and Innovation Programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation.

Thank You!!

감사합니다 Natick

Grazie Danke Ευχαριστίες Dalu Obrigado

Thank You Köszönöm

Tack

Спасибо Dank Gracias

谢谢 Merci Seé ありがとう

Digiotouch Core Business

- Sustainable and Secure Digital Transformation
  - Cloud based, secure, End-to-End Paradise IoT Platform