RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: AIR-F02

Vulnerabilities – What Is the Future?

John Forte

Founder & Co-Director
Johns Hopkins University Institute for Assured Autonomy

Bobbie Stempfley

Director
CERT Division, Software Engineering Institute at Carnegie Mellon University

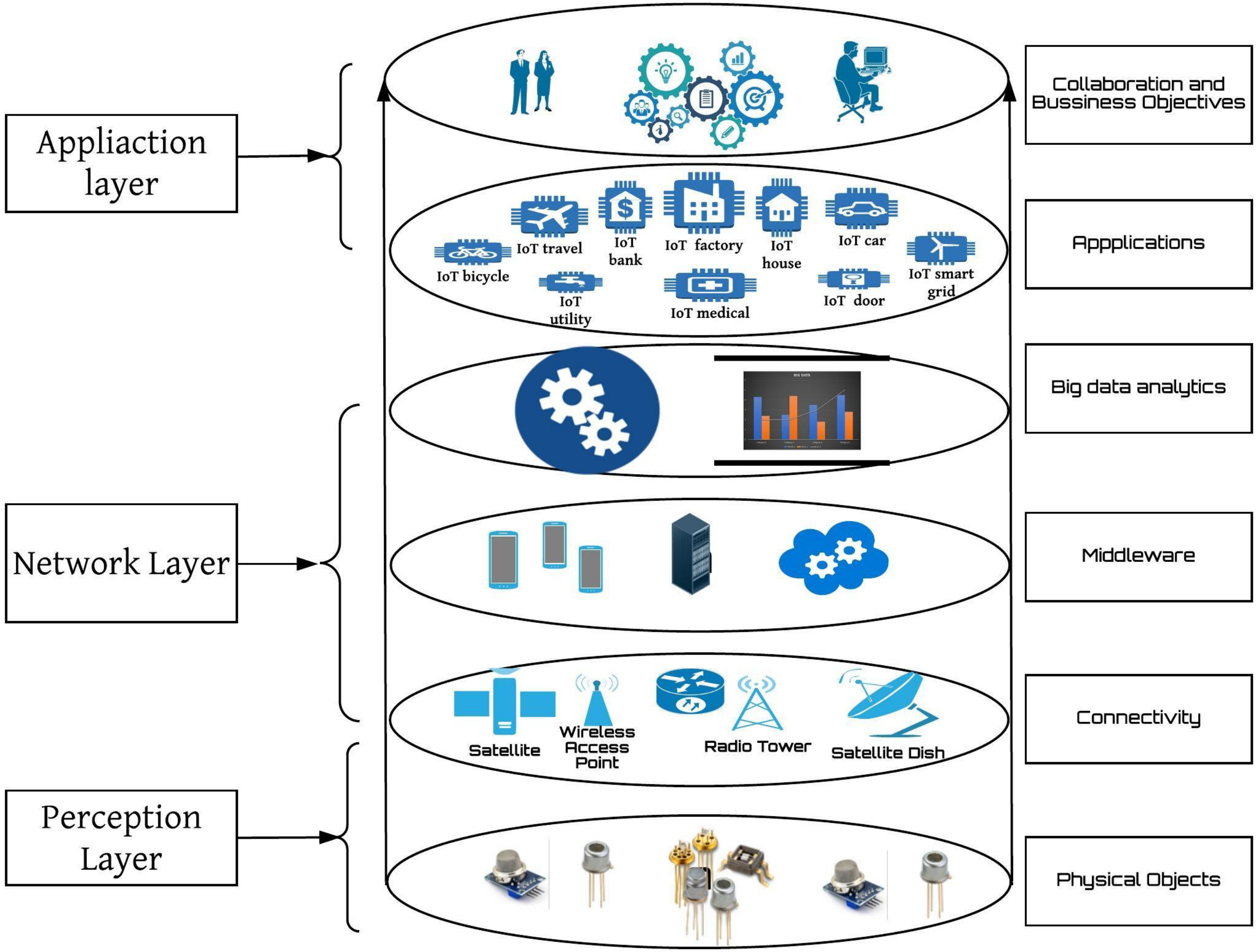
HEALTH &
MEDICINE
TRANSPORTATION
MEDICAL CENTER
BUILDINGS
& CITIES
PUBLIC SAFETY
& SECURITY
POWER GRID
& ENERGY
UNIVERSITIES
& EDUCATION
INDUSTRY
CONSUMERS &
ENTERTAINMENT

Tomorrow's highly connected, autonomous world is full of promise

Use Case: Future Remote Health Care

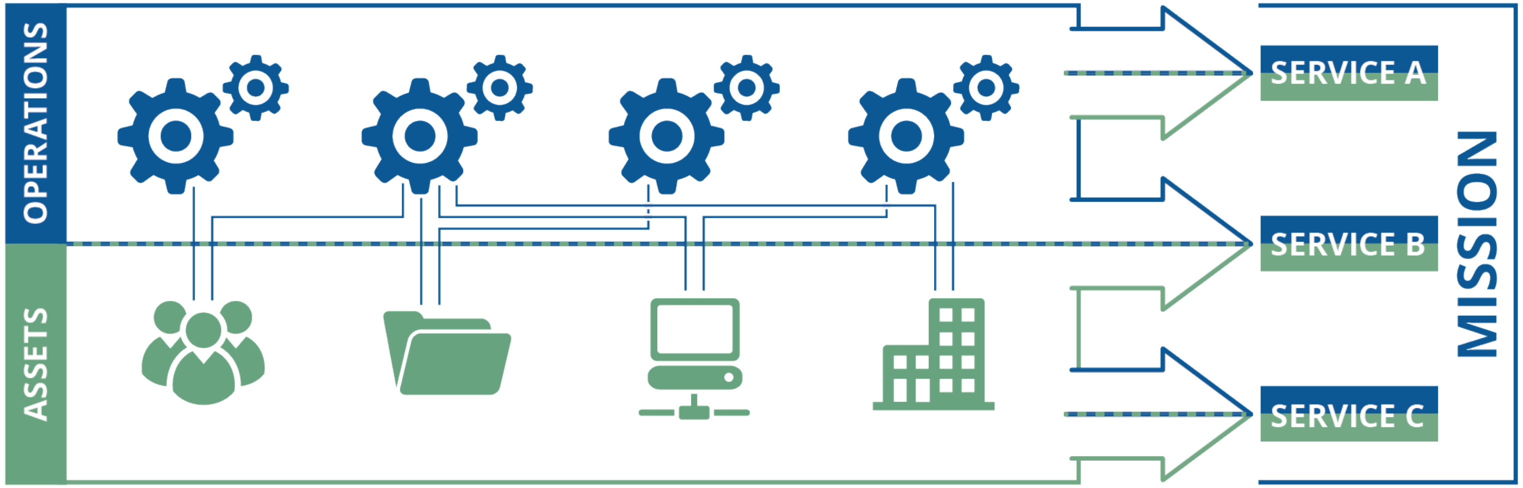
- Innovative home health care enabled by advancements in:
  - Health monitoring and therapeutic technologies
  - Remote and Telemedicine
  - Autonomy and Artificial Intelligence
  - Communications, 5G… ***IoT***
  - Other Tech (e.g. healthcare avatars)
- Teleoperated Robotics
- AI-enabled diagnostics & surgery
- Vertical Takeoff and Landing (VTOL) Emergency Vehicles

Architectural considerations – The Internet of Things (IoT)



https://arxiv.org/ftp/arxiv/papers/1807/1807.11023.pdf

Traditional CISO considerations – aligning risk to mission

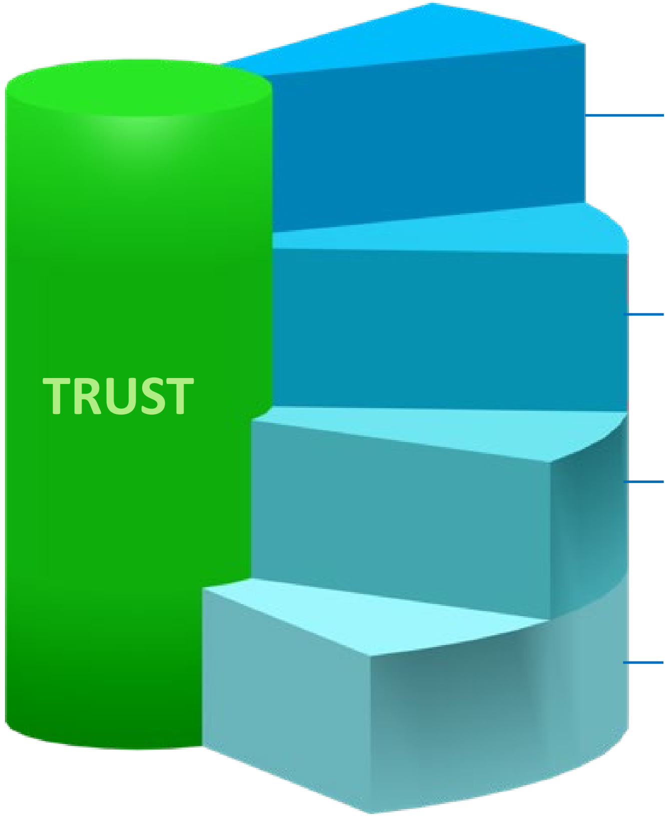


- **People**: those who operate and monitor the service
- **Information**: data associated with the service
- **Technology**: tools and equipment that automate and support the service
- **Facilities**: where the service is performed

! **Assets derive their value from their importance in meeting the service mission.**

AI-enabled capabilities, including machine reasoning, is also an asset to be managed

Perceive • Decide • Act • Team



Creativity & Innovation

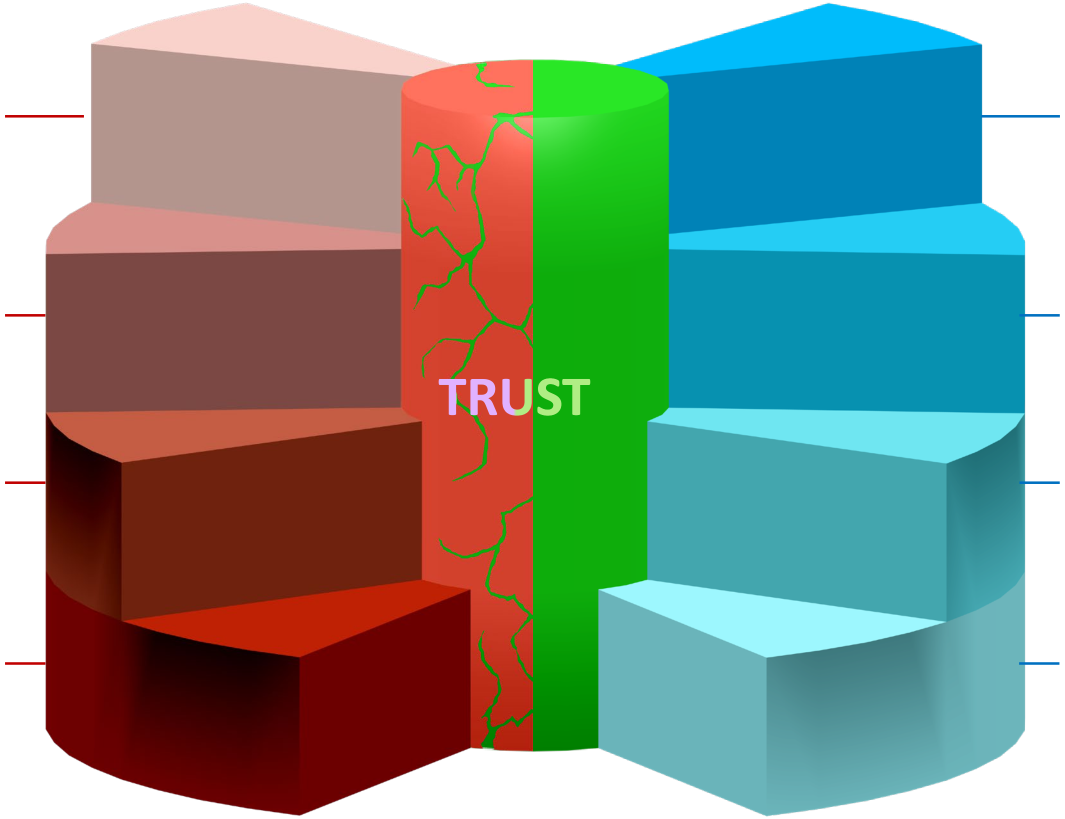
Self-Evaluation & Self-Guided Learning

Knowledge Representation & Reasoning

Pattern Recognition

AI-enabled capabilities are also going to be used by adversaries to do harm… and disrupt *trust*

Perceive • Decide • Act • Team



Adversarial – Creativity & Innovation

Adversarial – Self-Evaluation & Self-Guided Learning

Adversarial – Knowledge Representation & Reasoning

Adversarial – Pattern Recognition

Creativity & Innovation

Self-Evaluation & Self-Guided Learning

Knowledge Representation & Reasoning

Pattern Recognition

Use case – so what will be vulnerable?

Increased connections & access

Autonomous system monitoring & control

Remote execution and control

Closer IT/OT coupling

Machine Learning data & corruptible data stores

Composable tech

Network enabled equipment, remote management

Identity management & access controls

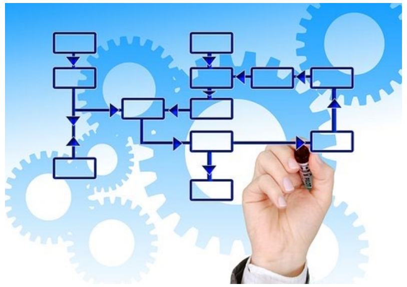
Safety of life – connections, data analytics, explainable AI

Attacks on emergency response

Data protection for Privacy and integrity

What things can we start doing today?

As a CISO:



Design Open, Resilient & Zero Trust Architectures

Master the Supply Chain

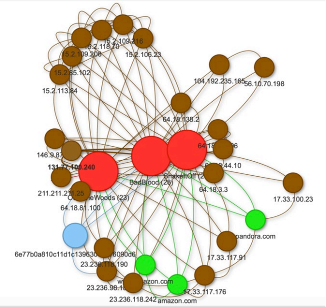
Embrace Automation & AI-enabled capabilities

! **The CISO will need to become more than just security technologists… they will also need to become *business strategists***

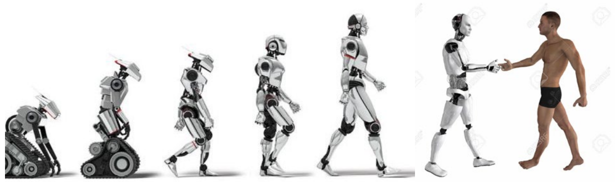
What things can we start doing today?

For the SOC:

Increase Response Speed



Become more data driven



Balance the Silicon-Carbon Ratio

By Frits Ahlefeldt

Harness the power of community

! **The SOC will need to become more data driven and machine reliant in order to keep pace with threats**

The future – what we don’t know yet and factors that we need to watch for

Environmental Evolution

Intelligent Ecosystem

Policy & Governance

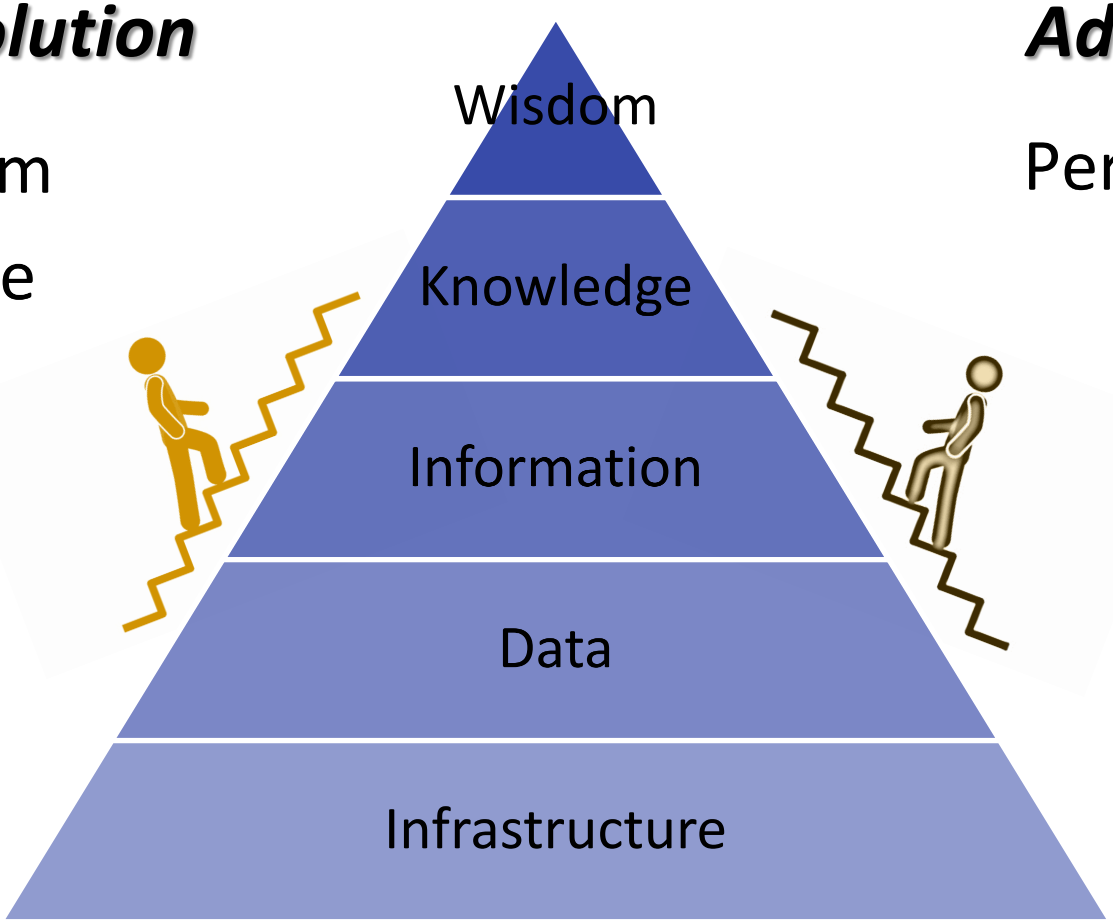
Technologies

Ethics

.

.

.



Adversarial Evolution

Perception Corruption

AI-Enabled Exploits

Data Corruption

Influence

.

.

.

I’m convinced, now what?

- Next week you should:
  - Take your Chief Data Officer to coffee – Focus on data stores, where, what, how used…
  - Recognize resilience as a necessary element of lines of business – SOC and CISO alignment
  - Shift your supply chain thinking to be focused on external dependencies
- In the first three to six months following this presentation you should:
  - Develop a security model for the technology that supports your DevSecOps efforts
  - Begin to catalog your external dependencies
- A year from now:
  - Have a catalog of your data stores
  - Know how you are automating reasoning