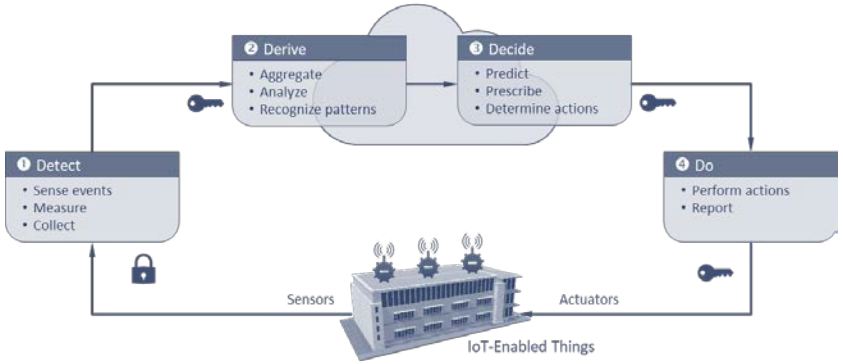
Governing IoT Records in an IG World

Records Knowledge Conference
Sacramento, California
May 23rd, 2019

By Bassam Zarkout

Contents



Session: Governing IoT Records in an IG World

- IoT systems (smart cities, smart factories, smart healthcare, smart grids, etc.) are starting to produce massive amounts of data that dwarf the amounts produced by business systems:
  - IG professionals might tell you that this IoT data is corporate data that must be governed per se
  - IoT professionals will tell you… not so fast
- IoT Trustworthiness is a critical property of IoT systems that encompasses the convergence of:
  - IT issues like Security and Privacy with
  - Physical OT (Operational Technology) issues like Reliability, Resilience and Safety
- Important to look at the governance of IoT data through the prism of IoT Trustworthiness
- Session will describe the concept of IoT Trustworthiness and will cover how developers and operators of IoT solutions can:
  - Align IoT Trustworthiness objectives with the Information Governance objectives
  - Define levels of trustworthiness mandated by various laws and regulations
  - Establish levels of trustworthiness in their systems
  - Sustain them throughout the lifecycle journey of their IoT systems

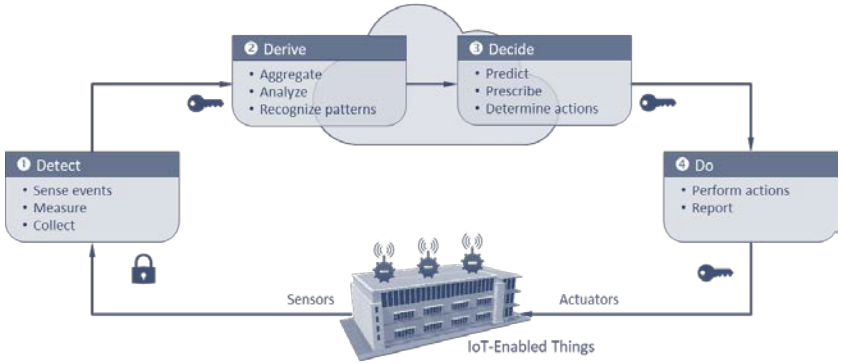
About Bassam Zarkout

- Technology tech executive (25+ years of experience in Canada, US, Europe)
  - Focus on IoT, Information Governance (IG) and Data Governance:
  - Public speaking, panelist, thought leadership, servant leadership, Twitter
  - IG, IoT, Privacy, AI, DL, etc.
- Held executive C-positions at RSD Switzerland (8 years)
  - CTO (technology), CSO (strategy)
  - Design/build RSD's Information Governance Platform
- Founded IGnPower in 2016
  - IoT consulting practice
    - Focused on IoT Trustworthiness related topics: Assessment, Journey, Program
  - IIC member since 2016
    - IoT Trustworthiness, Data Governance, Data Privacy, Data Residency, Data Protection
    - Industrial Digital Transformation and IT-OT convergence
    - Other areas: Industrial AI, Industrial DL

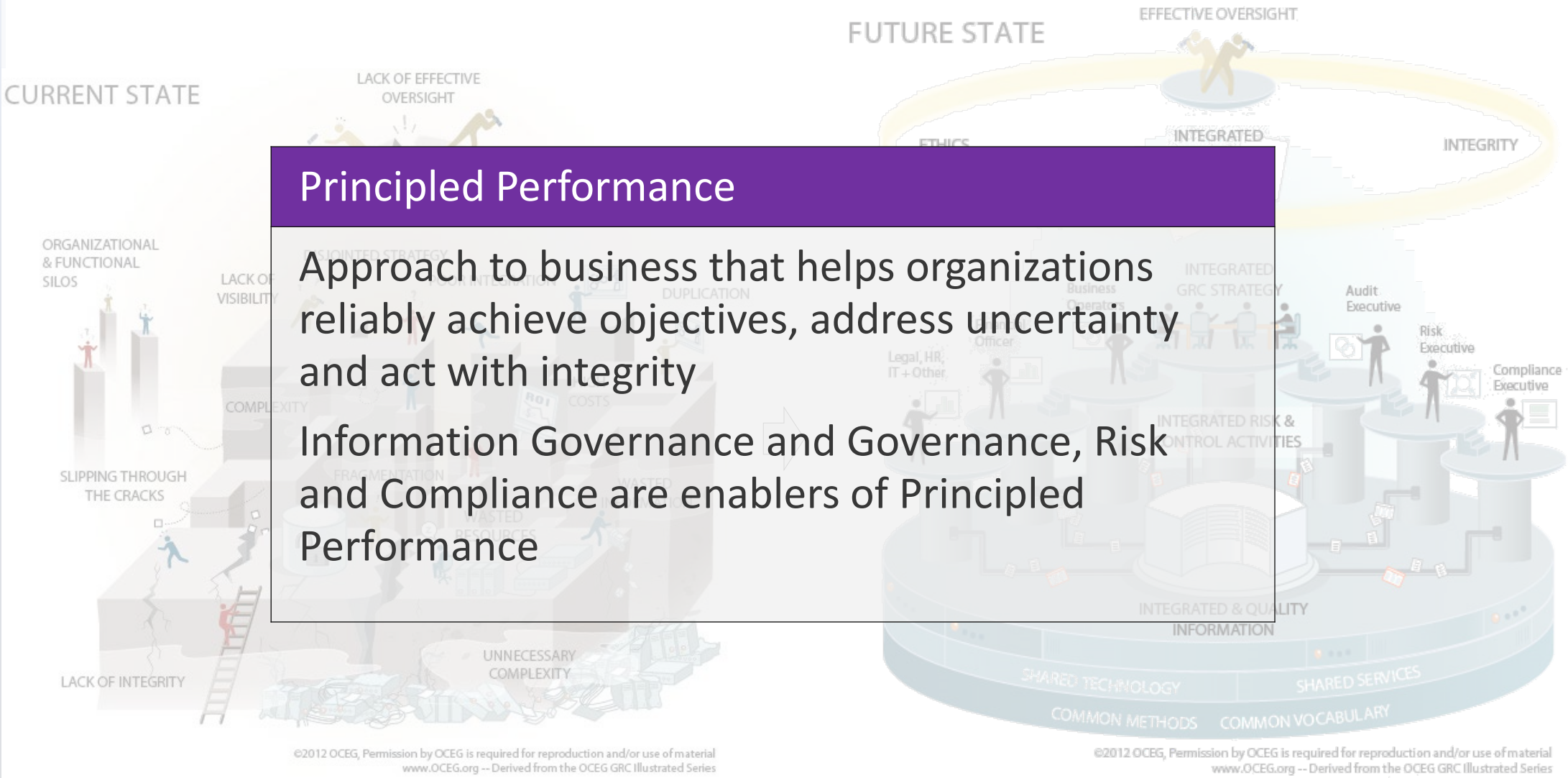
industrial internet CONSORTIUM

bzarkout@ignpower.com
@bzarkout
+1.613.7913033

Contents



Principled Performance ⇔ GRC ⇔ IG



Principled Performance

Approach to business that helps organizations reliably achieve objectives, address uncertainty and act with integrity

Information Governance and Governance, Risk and Compliance are enablers of Principled Performance

Source Open Compliance and Ethics Group (www.oceg.org)

Digitization vs Digitalization vs Digital Transformation

Digitization

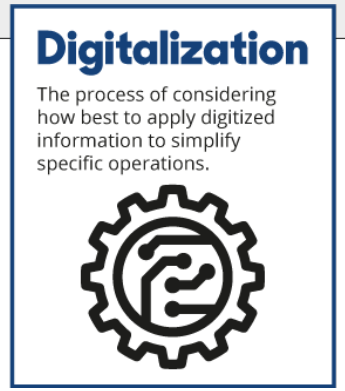
- Transition from analog to digital
- Make information available and accessible in digital format
- It all began here
- Still going on today

Digitalization

- Make digitized information work for you
- Once analog data has been digitized, there is enormous potential for applications that facilitate standard work practices

Digital Transformation

- Build on digitalization to create completely new business concepts
- Data is easily accessible for use across various platforms, devices, interfaces
- Process of devising new business applications that integrate digitized data and digitalized applications



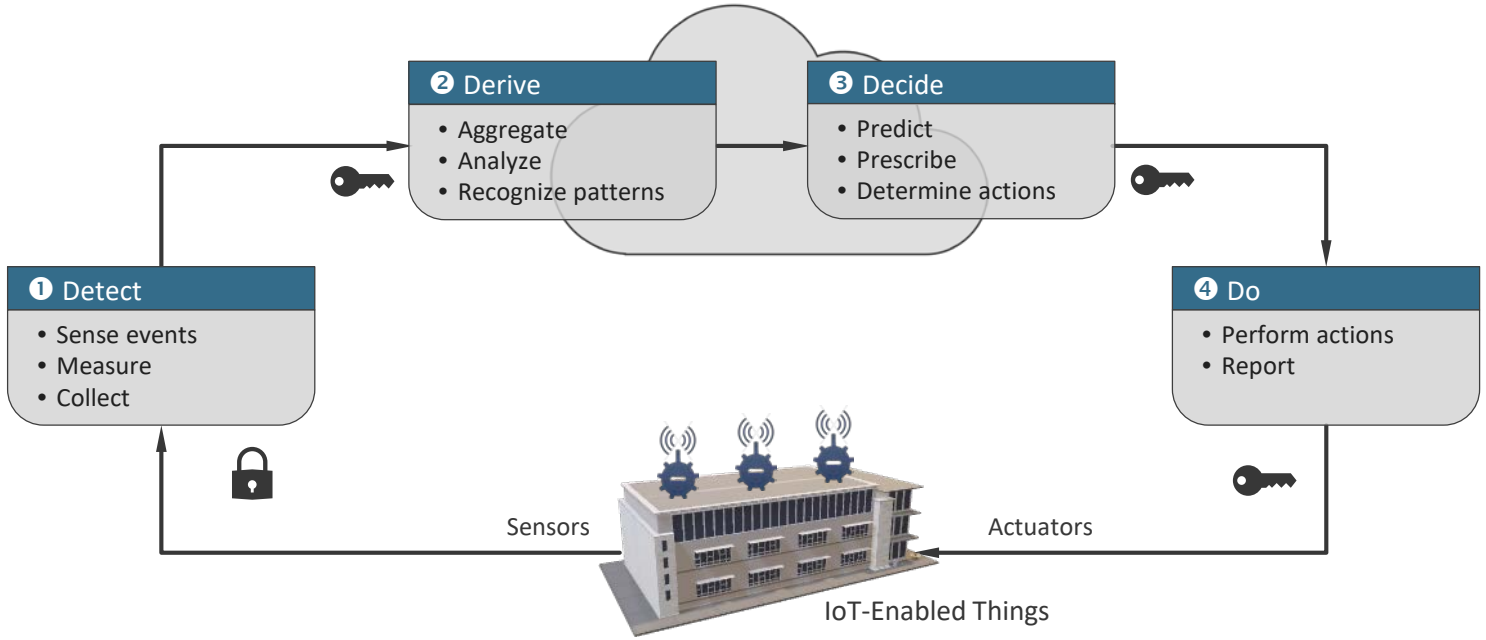
Source of information: SAP

Internet of Things is more than IT for Things

Key enabler for Digital Transformation

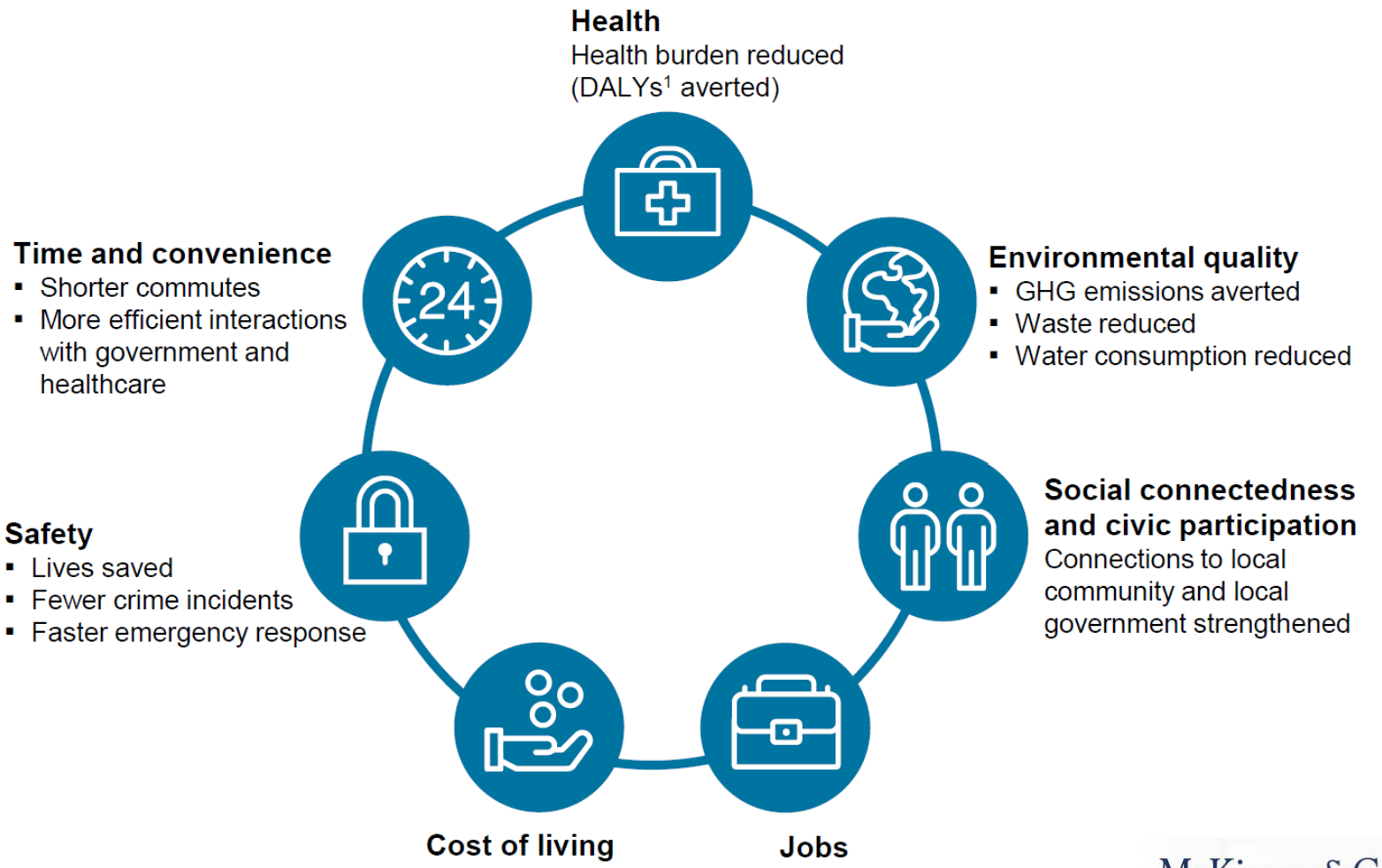
- Capture operational data
- Analyze and exploit that data
- Gain insight about the operation of things
- Control them and alter their behavior

Produce Better Outcomes



Principle of operation of IoT systems is straight forward

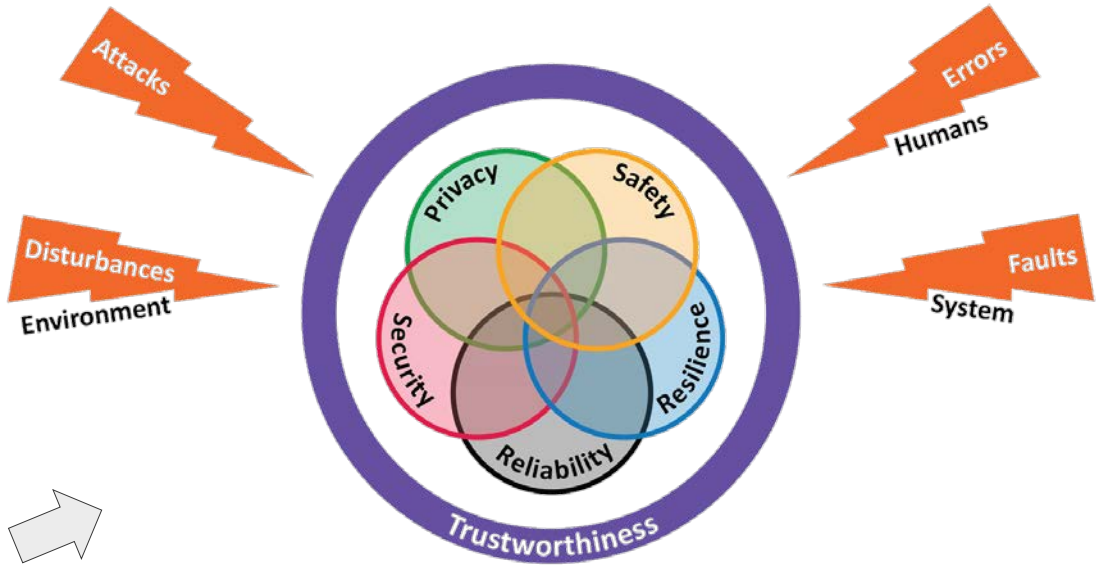
Example Benefits of IoT Solutions: Smart Cities

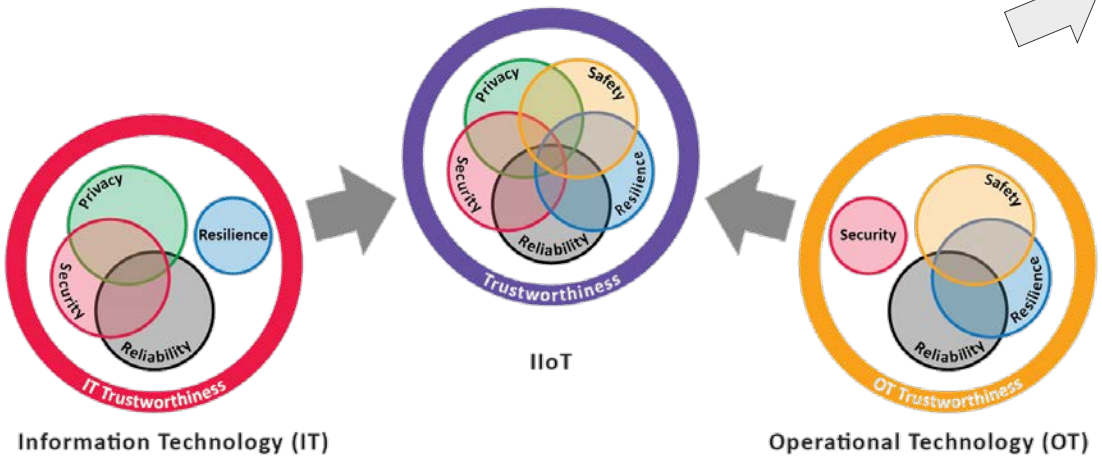


McKinsey&Company

IoT Trustworthiness

- Convergence of IT and OT
  - IT: Security and Privacy
  - Physical OT (Operational Technology): Reliability, Resilience and Safety
- Distinct and Cross-functional
  - Multiple well-established domains
  - Interdependence between them*

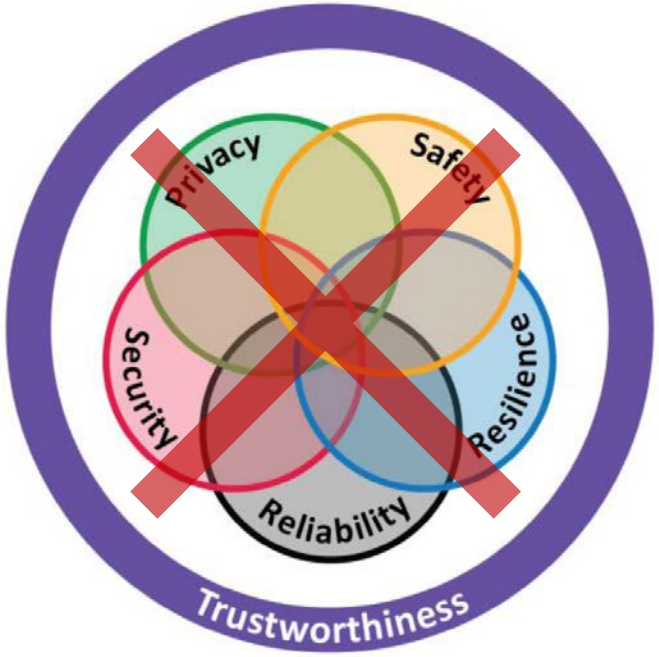




industrial internet CONSORTIUM

* Example: Delaying Security updates to maintain Reliability levels can negatively affect Safety.

Acting badly leads to negative consequences



Inaction, poor awareness, and lack of visibility and planning → low levels of IoT Trustworthiness → negative consequences

Risks to human life
Long term negative impact on environment
Interruption of critical infrastructure
Unauthorized disclosure of sensitive data
Destruction of equipment
Economic loss
Damage to reputation
Non-compliance with regulations
Liability and litigation

States of IoT Trustworthiness

Current State

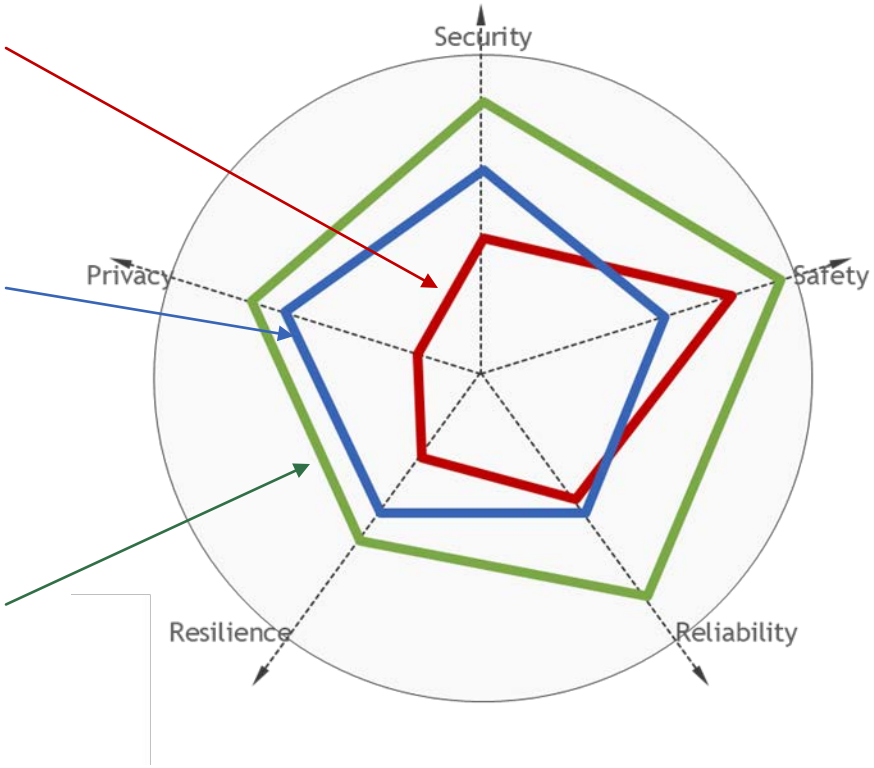
- Actual state as it exists now
- Progresses over time

Minimum State (external drivers*)

- Min non-negotiable and mandated level
- Laws, regulations, standards, best practices, etc.
- Jurisdictional variations

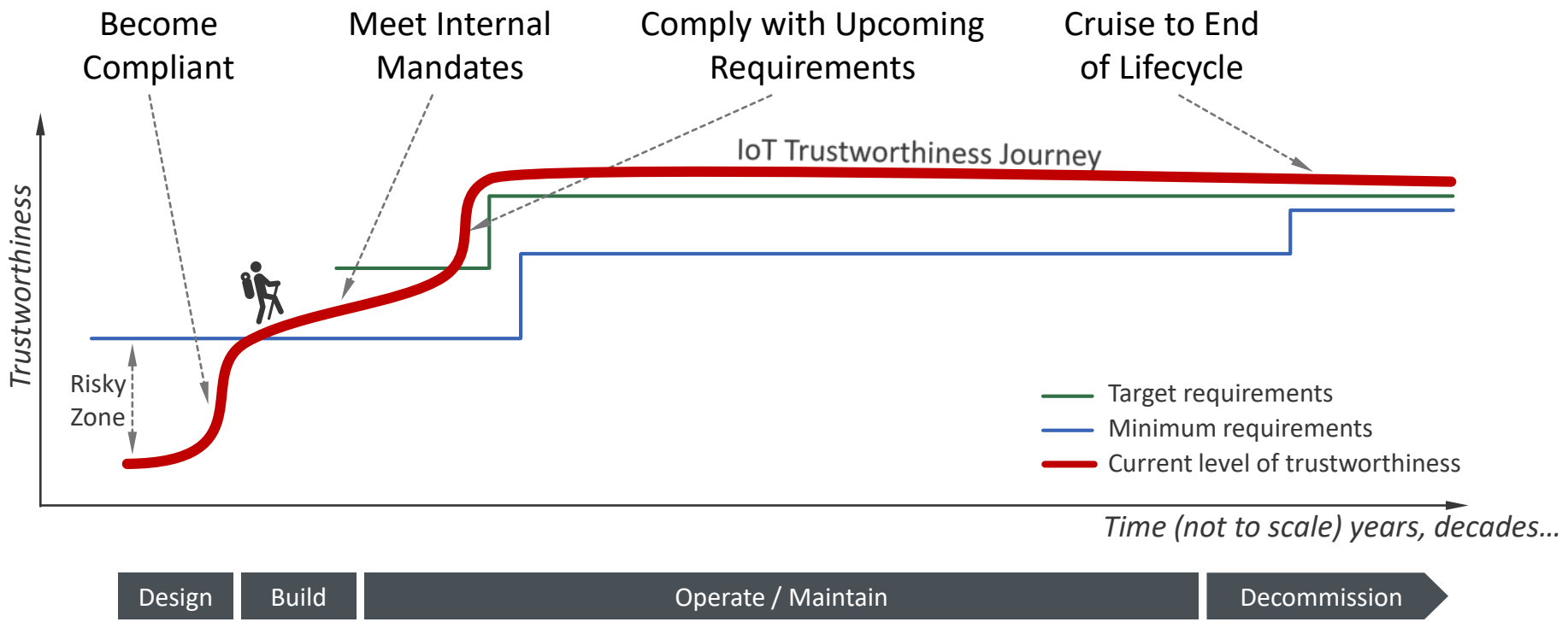
Target State (internal drivers)

- Objective level of Trustworthiness to achieve
- Alignment with corporate vision, ROI, risk, etc.
- Alignment with product strategy and roadmap



* Eg: OSHA 29 CFR 1910, IEC 61508, EU GDPR, EDRM.net, etc.

IoT Trustworthiness… is a Journey



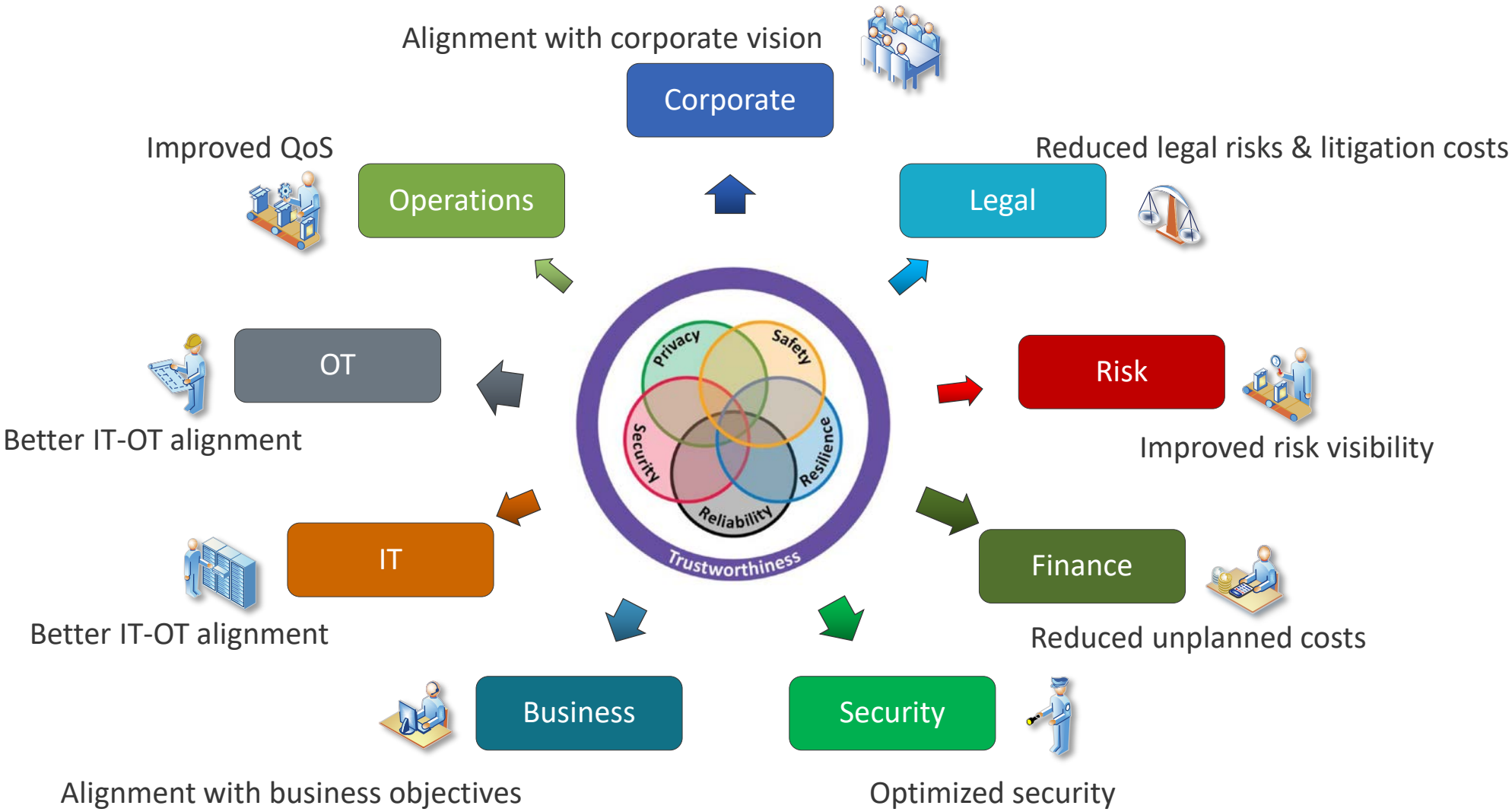
Trustworthiness requirements may change during lifecycle
System structure & architecture may change/evolve
IoT data produced/consumed have their own lifecycle

Intelligent Transportation Systems

IoT Trustworthiness Journey MUST be powered by a Program

Responsibilities? | Profile/Role? | Reporting? | Budget?

IoT Trustworthiness… MUST deliver real value to the organization

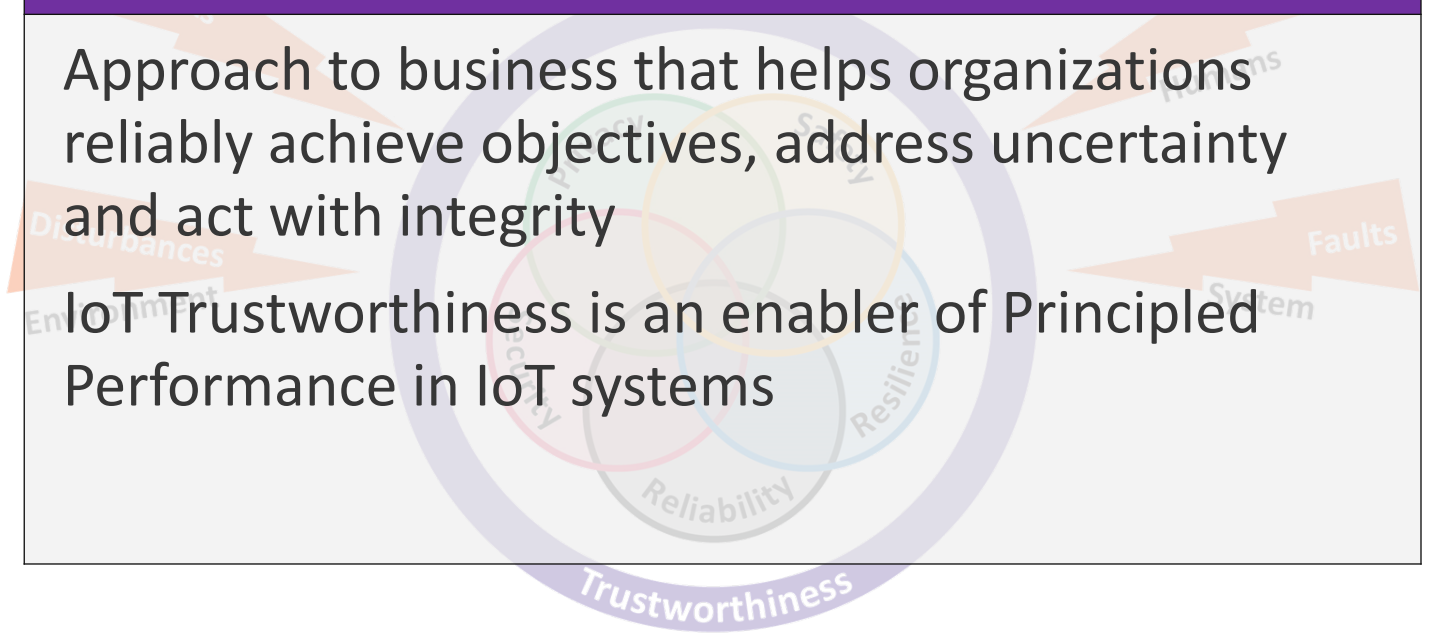


IoT Trustworthiness ⇔ Principled Performance in IoT systems

Principled Performance

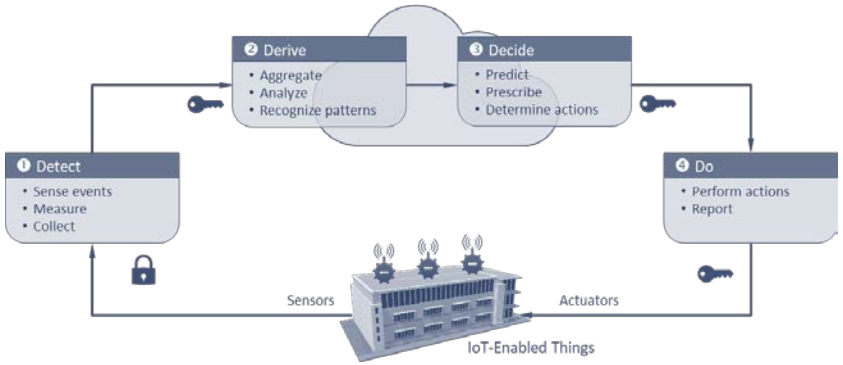
Approach to business that helps organizations reliably achieve objectives, address uncertainty and act with integrity

IoT Trustworthiness is an enabler of Principled Performance in IoT systems

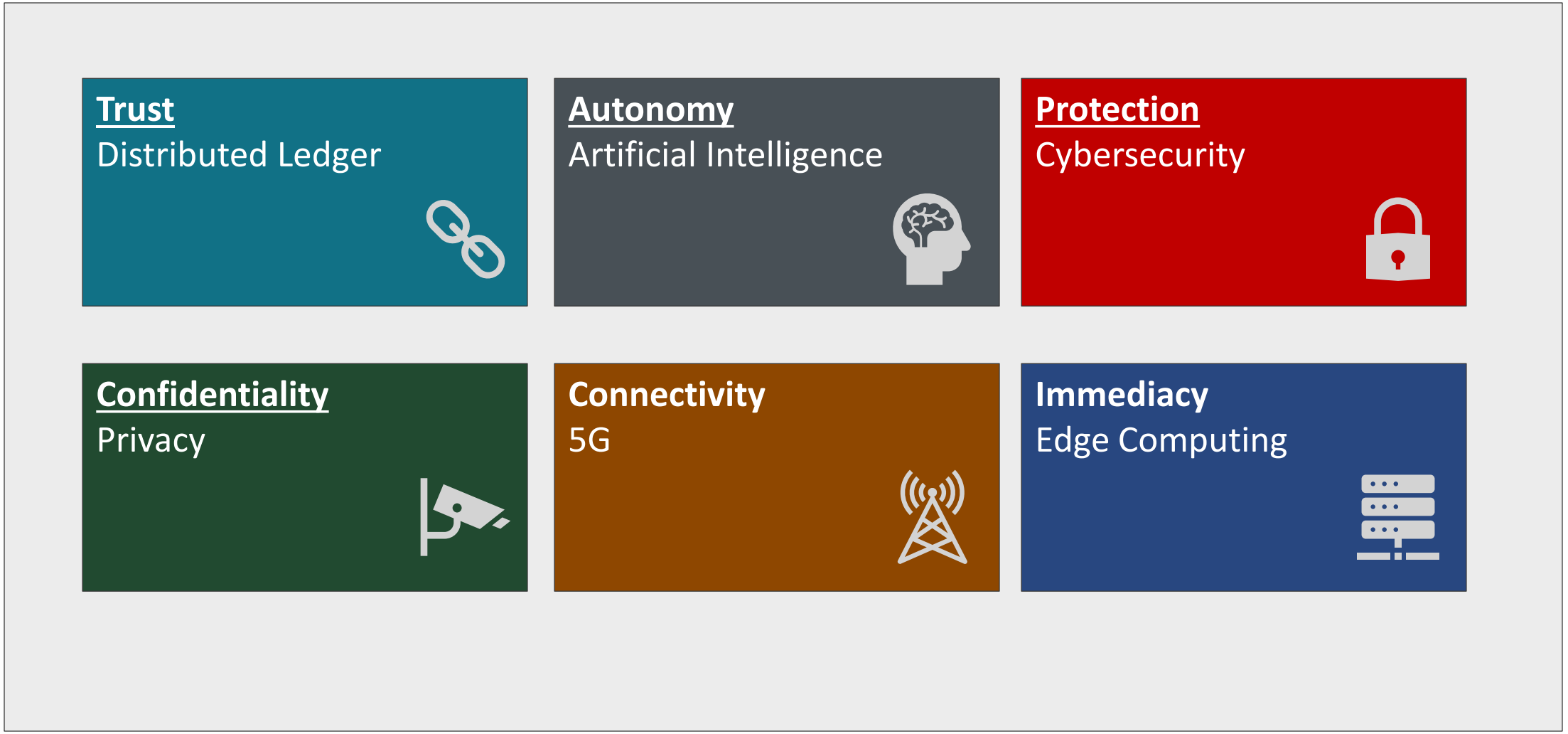


Contents

- Introduction
- IoT Trustworthiness
- Related Topics
- Governance of IoT Data
- Conclusion

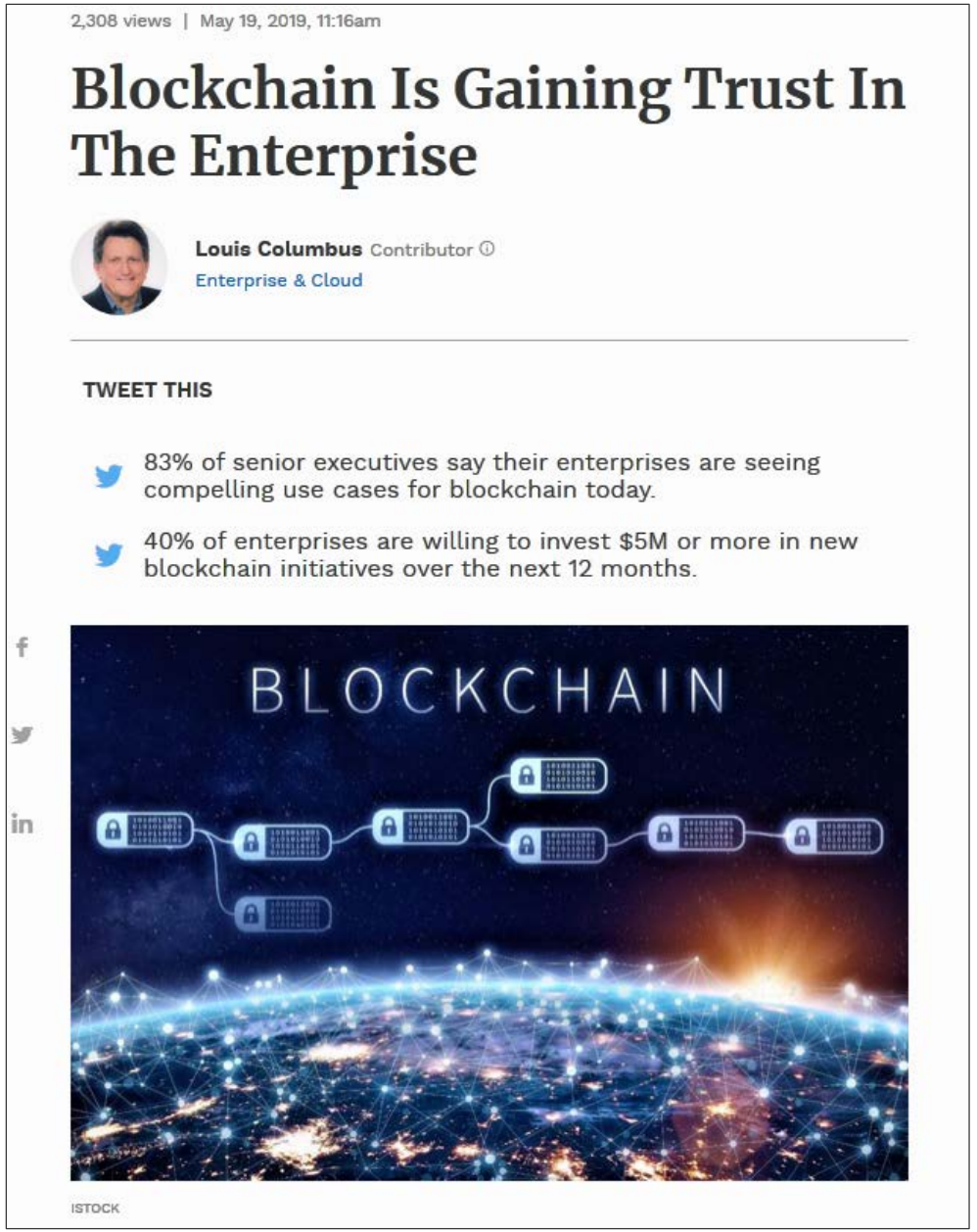


Topics related to IoT



Distributed Ledger (DL)

- Blockchain → type of Distributed Ledger
- Cloud-based database shared by every participant in a transaction
  - Essentially a peer-to-peer ledger
- Blockchain protects data integrity
  - Secure data integrity
  - Strengthen chain of custody of data
- Integrated approach
  - IoT, Ubiquitous Connectivity (5G), AI, etc.
  - Cloud is so 2010's… welcome to Fog & Edge



2,308 views | May 19, 2019, 11:16am

Blockchain Is Gaining Trust In The Enterprise

Louis Columbus Contributor ⓘ
Enterprise & Cloud

TWEET THIS

83% of senior executives say their enterprises are seeing compelling use cases for blockchain today.

40% of enterprises are willing to invest $5M or more in new blockchain initiatives over the next 12 months.

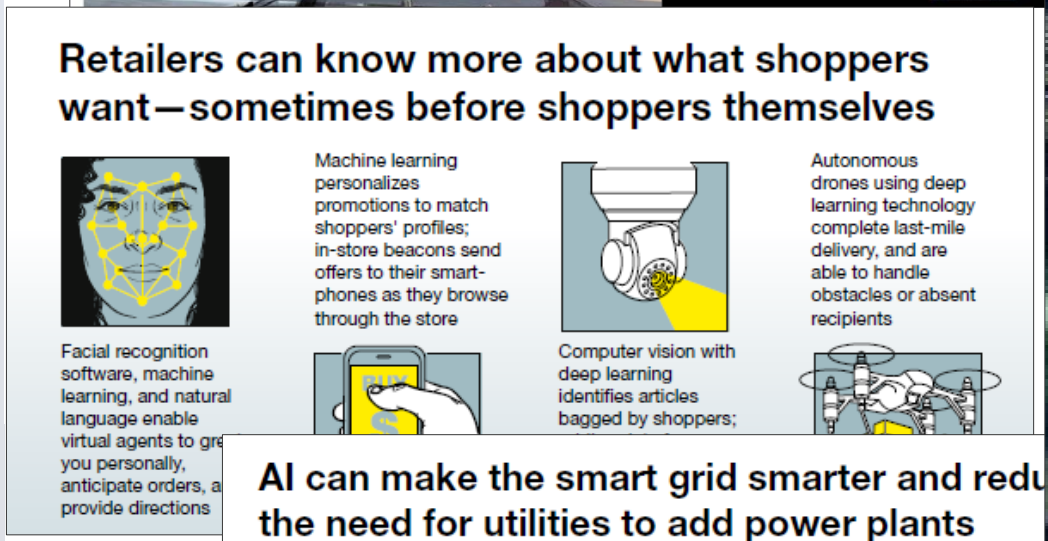
ISTOCK

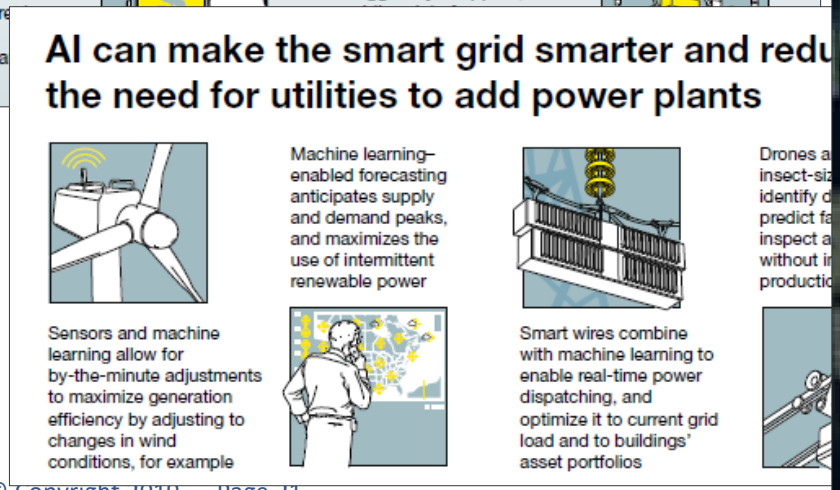
Source: Forbes

Distributed Ledger (DL)

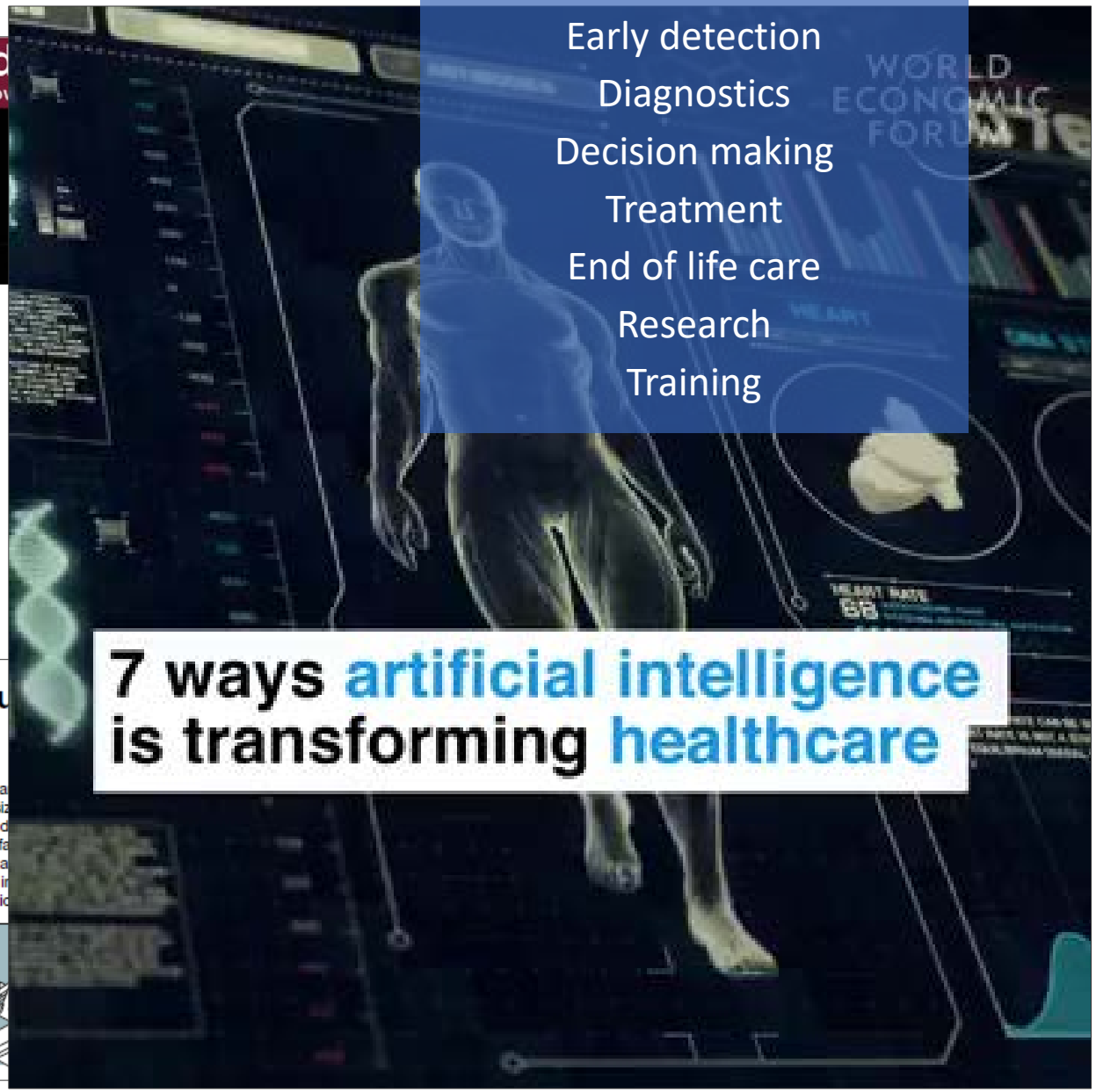
- Smart Cities
  - Improve operational efficiency, drive citizen engagement, identify new revenue sources, etc.
- Smart Contracts
  - Computer protocols that facilitate, verify, or enforce negotiation / performance of contract
  - Smart Contracts in State Government business
- Supply Chains
  - Time Is Right For Disruption (Forbes)
  - Government, Aerospace, Automotive, other

AI in various domains





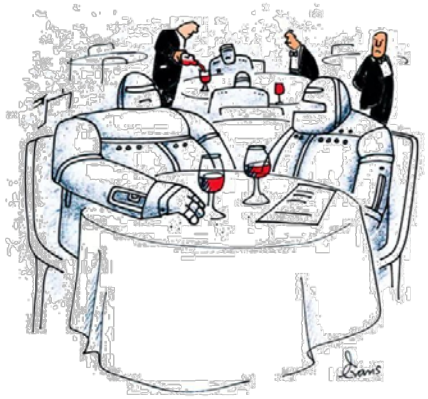
Keeping well
Early detection
Diagnostics
Decision making
Treatment
End of life care
Research
Training



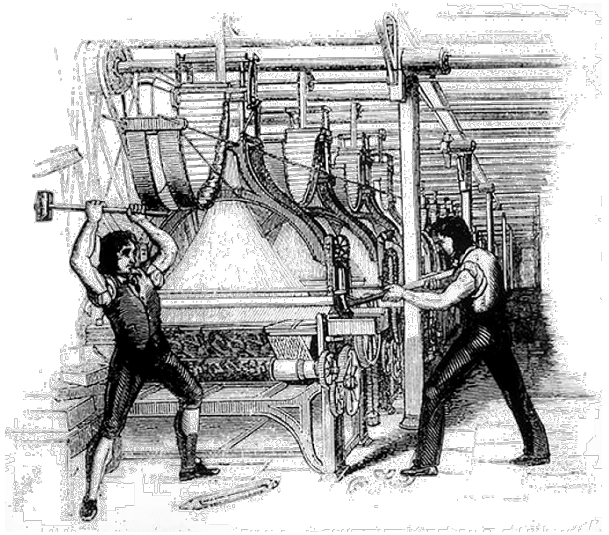
Various AI Topics: Jobs, Ethics

AI Impact on Jobs

- Fully automate simple and repetitive tasks? or
- Augment workers experience in complex tasks?



'I can't imagine why they ever thought we'd take their jobs away.'



The Luddites in 1812

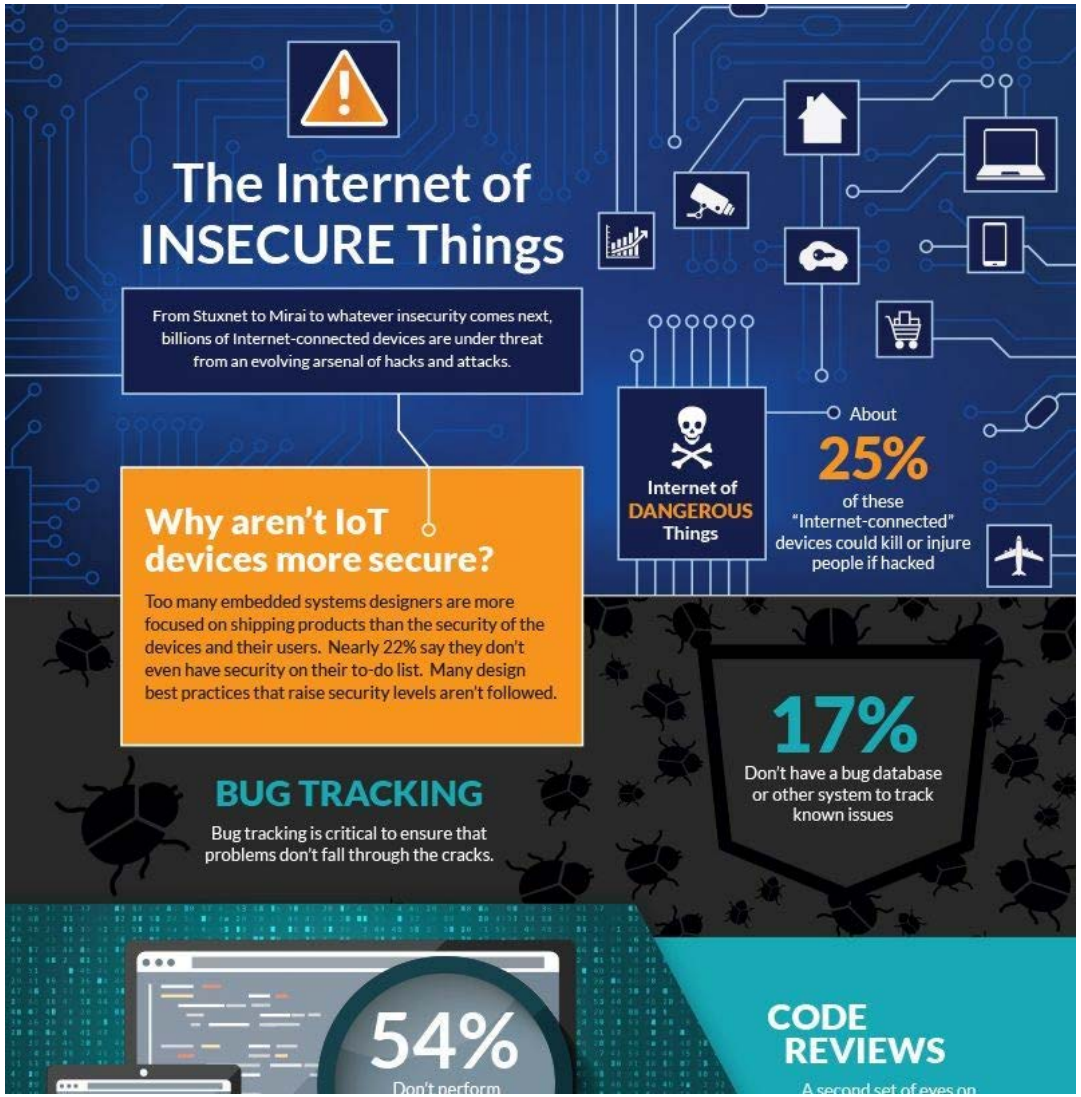
AI Ethics

1. Do no harm
2. Generate net benefits
3. Comply with laws and regulations
4. Protect privacy
5. Be fair
6. Be transparent and explainable
7. Be accountable

Gavin Newsom (California Governor) at HAI 2019 Stanford CA

- “I read [PricewaterhouseCoopers]: 38 percent of jobs will be automated in the next 15 years. Then I relax because Bain comes out and says just 25 percent of the jobs in the next 20 years. Then Oxford says, that’s an old study, that 47 percent is only in 702 job categories, not all job categories. Then I got James [Manikya], which says it’s just 60 percent of current jobs that will be just 30 percent augmented.”
- With that kind of conflicting information flying around, Newsom asked rhetorically, “what do you want me to do as a policymaker?”

Cybersecurity… a major concern



Source: Twitter

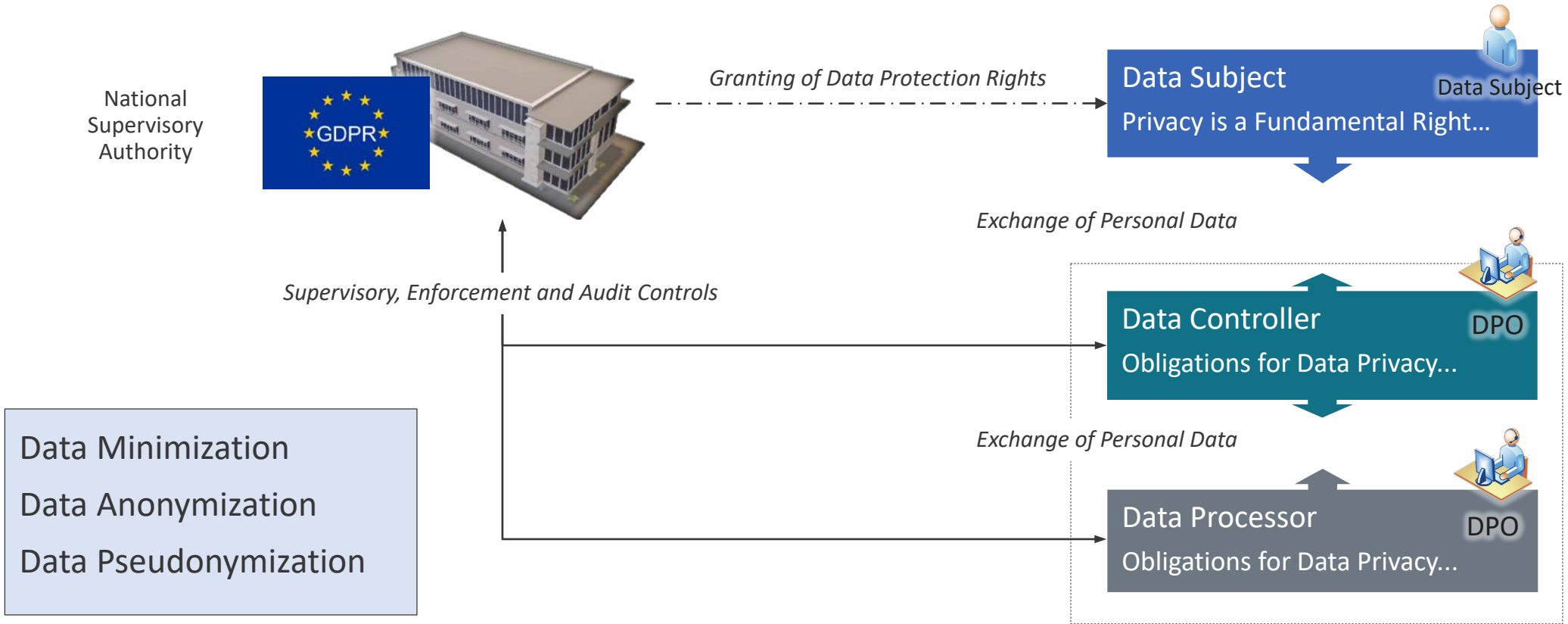
Data Protection and the important role of Data Security

Information and Data Protection & Privacy

- Aspect of Information Technology that deals with the ability of an Organization to determine what Personal Data (data about individuals) can be shared with 3rd parties
- Privacy Laws in the US
  - US Federal Privacy Act
  - State-level Privacy Acts, eg CCPA
  - HIPAA
  - PCI
  - Other

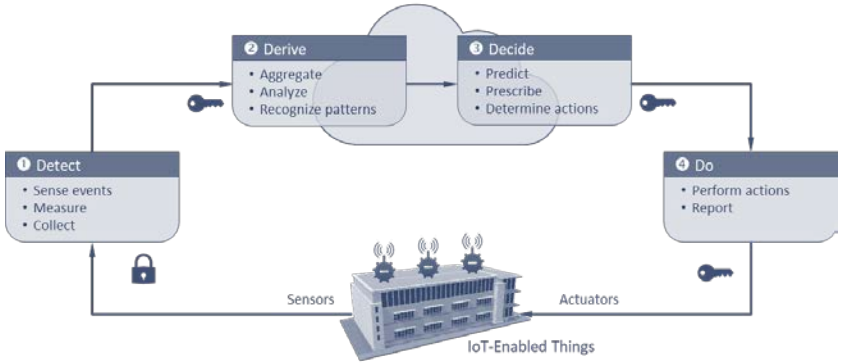
Information & Data Privacy

Information and Data Protection & Privacy



Data Security plays a central role in Data Privacy

Contents



Challenges facing Information Governance

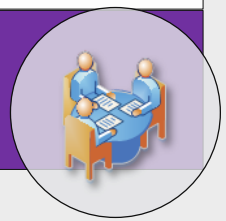
Despite its short history, Information Governance has had its fair share of challenges…

- Lack of maturity in discipline and organizations
- Technical complexity
- Organizational complexity
- Moving target… Privacy, IoT, Blockchain, etc.

IG practices are maturing

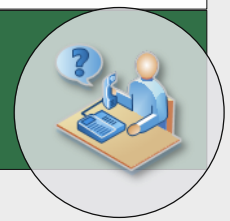
- Long on vision
- Short on execution
- Short on effective executive sponsorship

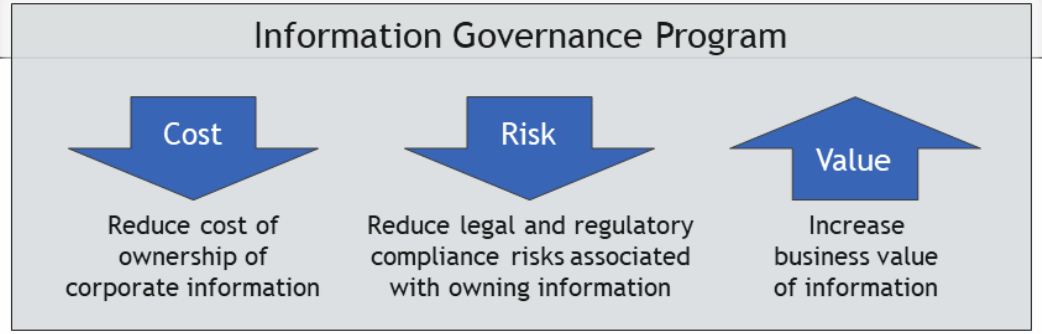
Most IG programs not well established



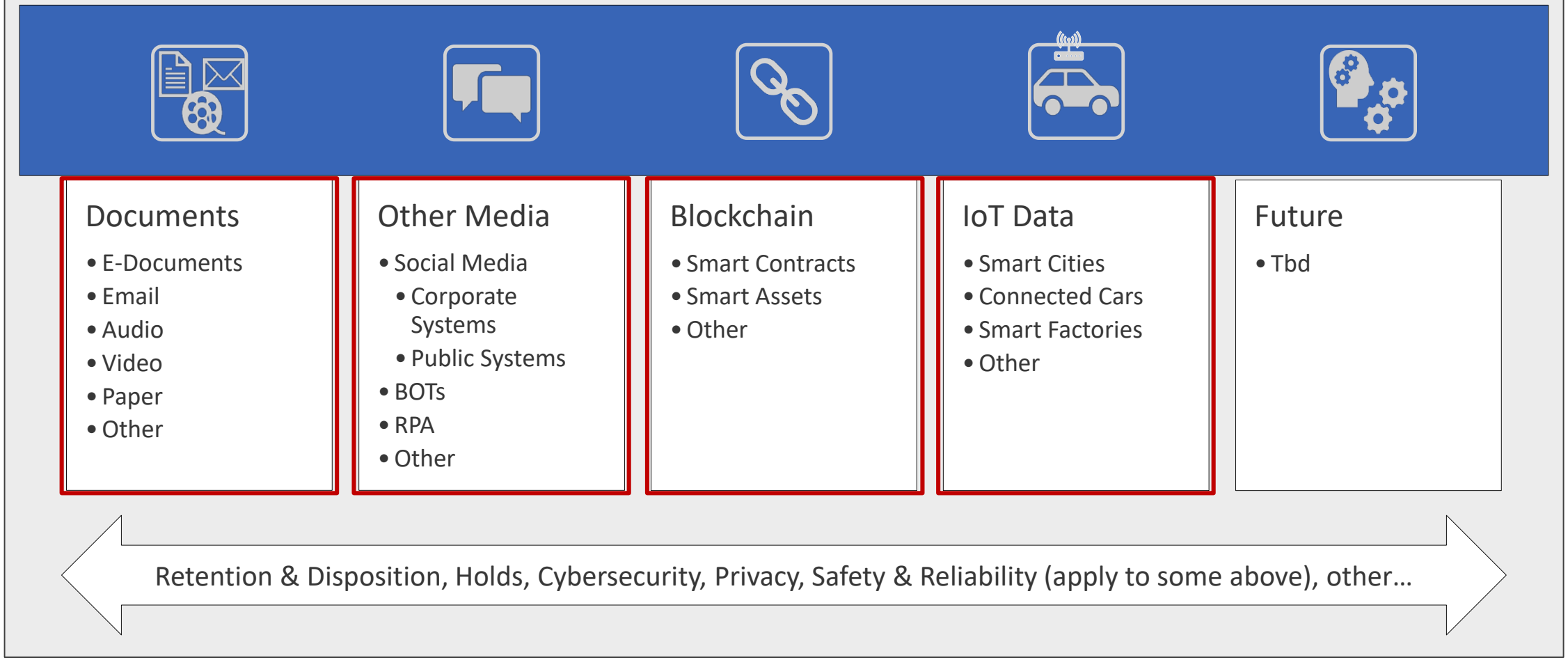
- Tighter IT budgets
- Most CIOs focused on infrastructure
- RM stuck in the past
- Business Leaders focused on business

Unclear who is in charge



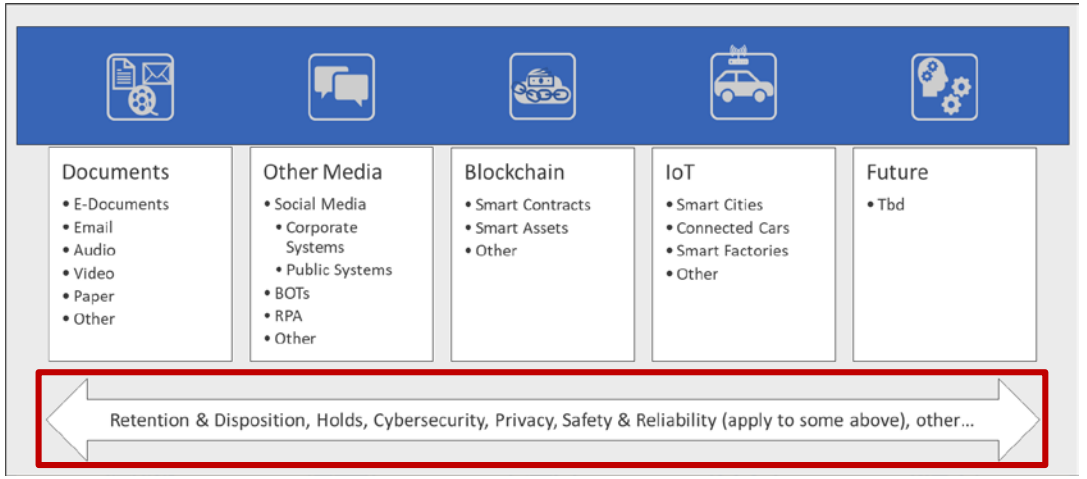


More to Information Assets than just Documents



Multiple Governance & Control concerns about Information Assets

- Retention, Disposition, and Holds
  - Applies to Information Assets
  - Records Management, Information Governance, eDiscovery
- Cybersecurity
  - Applies to Assets and Information Assets
- Privacy
  - Applies to Information Assets that reference Data Subjects
- Safety & Reliability
  - Applies to Assets
- Other



Notes

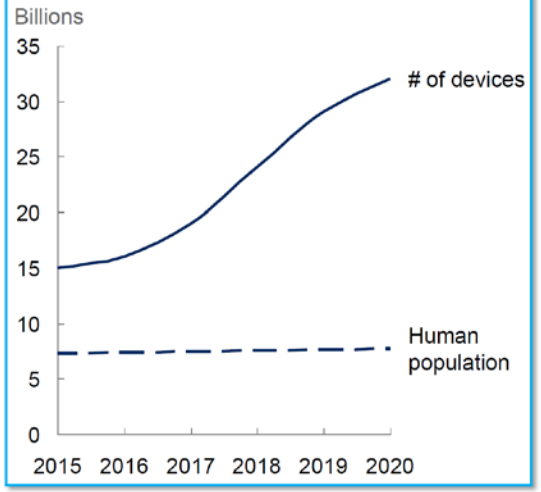
- Multidisciplinary effort
- IG and RM are part of it
- Security is part of it
- Privacy is part of it
- In some cases, Safety and Reliability are part of it

Sometimes these requirements conflict with each other

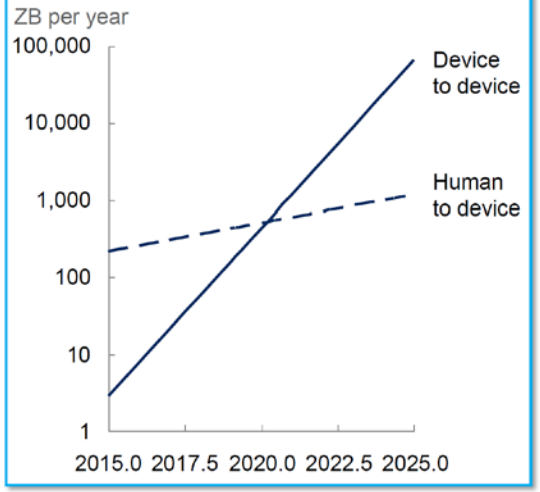
If you think there is lots of corporate information… think again

IoT is quickly becoming ubiquitous…

Projections for world population and number of IoT devices



Projections for human to device and device to device data consumptions[1]

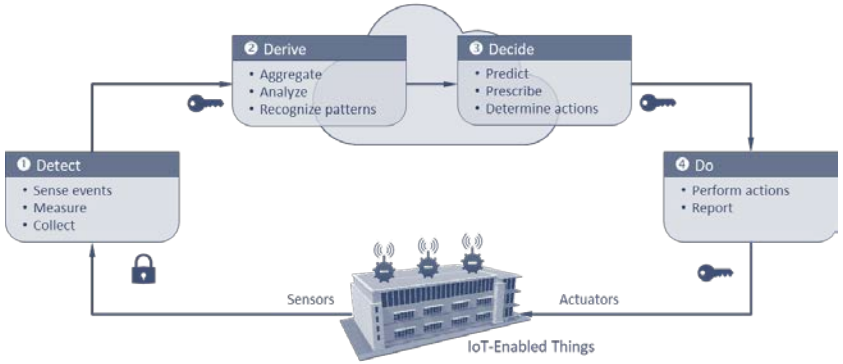


Explosive growth in device to device traffic will introduce new challenges in areas such as bandwidth, management and security

McKinsey&Company

Contents

- Introduction
- IoT Trustworthiness
- Related Topics
- Governance of IoT Data
- Conclusion



Conclusion and Takeaways

IoT Trustworthiness and Governance of IoT data

- Principled performance
- KEY to ensuring IoT systems can deliver on their intended objectives

There is no time to waste here

- IoT technologies and architectures evolving fast
- IoT data volumes are exploding

AI, DL, 5G, Edge Computing

- Play central roles within IoT systems
- AI ethics: why did the AI make that decision?
- Blockchain vs Privacy (Right-to-Forget)… conflict?

Safety-by-Design Security-by-Design Privacy-by-Design

- Also “by Default”
- NOT mere catchy buzzwords
- Critical for success of Digital Transformation
- Must be understood and principles behind them woven into fabric of IoT systems

Conclusion and Takeaways

Safe to say that the need to govern IoT data is real and looming

It is also inescapable!

Issues related the trustworthiness of IoT systems will dominate the conversation

IG professionals have an important role to play in all this

Thank You…


ignpower™
Bassam Zarkout
IGnPower Inc.
mobile: +1.613.7913033
email: bzarkout@ignpower.com
twitter: @bzarkout
skype: bzarkout
web: www.ignpower.com