Practical advantages of applying Privacy by Design in IoE

Thursday 6th of October 2016

Marc Vael

CISA, CISM, CISSP, CGEIT, CRISC, Guberna Certified Director

President of ISACA Belgium vzw

Chief Audit Executive of Smals vzw


Exposed record
Data breach
Protection
DATA
PRIVACY
law
anonimous
Metadata
Regulations
Search
classification
digital
Patient privacy
Privacy
Risk
Sensitive Information
Authentication
compliance

https://www.safeonweb.be/nl

JUST LAUNCHED TODAY!!!

https://www.safeonweb.be/nl

JUST LAUNCHED TODAY!!!

Privacy

> **Personal data is the new oil of the internet & the new currency of the digital world.**
>
> **MEGLENA KUNEVA**, European Consumer Commissioner

Privacy by Design

7 core PbD principles

1. **Proactive** not Reactive : **Preventative** not Remedial.
2. Privacy as the **Default** Setting.
3. Privacy **Embedded** into Design.
4. **Full** Functionality : Positive-Sum, not Zero-Sum.
5. End-to-End **Security** : Full Life Cycle Protection.
6. Visibility **and** Transparency : Keep it **open**.
7. Respect for User Privacy : Keep it individual and **user-centric**.

Ann Cavoukian, Ph.D., Information & Privacy Commissioner Ontario, Canada
https://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf

Main benefits of PbD

1. Increased **awareness** of privacy and data protection across an organisation.
2. Actions take privacy into account and generate a **positive impact** on individuals.
3. Potential privacy problems are identified at an **early** stage; addressing them early will often be simpler and less costly.
4. Organisations are more likely to meet their **legal obligations** and thus less likely to breach privacy laws and regulations.

AN ISACA SURVEY

Keeping a Lock on Privacy

HOW ENTERPRISES ARE MANAGING THEIR PRIVACY FUNCTION

Abstract

Announcements of major privacy breaches involving thousands, even millions, of data records are becoming common print and Internet headlines. We live in an information economy where no enterprise is exempt from security threats, vulnerabilities and privacy exposures. Because a privacy breach can generate a shocking degree of damage, enterprises cannot afford to overlook or mismanage their data security efforts.

ISACA, the world's leading independent, nonprofit association in governing, managing and assuring trust in an evolving digital world, conducted a survey among more than 15,000 members and others with privacy-related job titles to learn more about current privacy governance practices, structures and attitudes. This report presents the *ISACA Privacy Survey* results. ISACA takes seriously its responsibility to understand privacy issues and provide its stakeholders with tools to establish and manage an effective privacy program.

ISACA

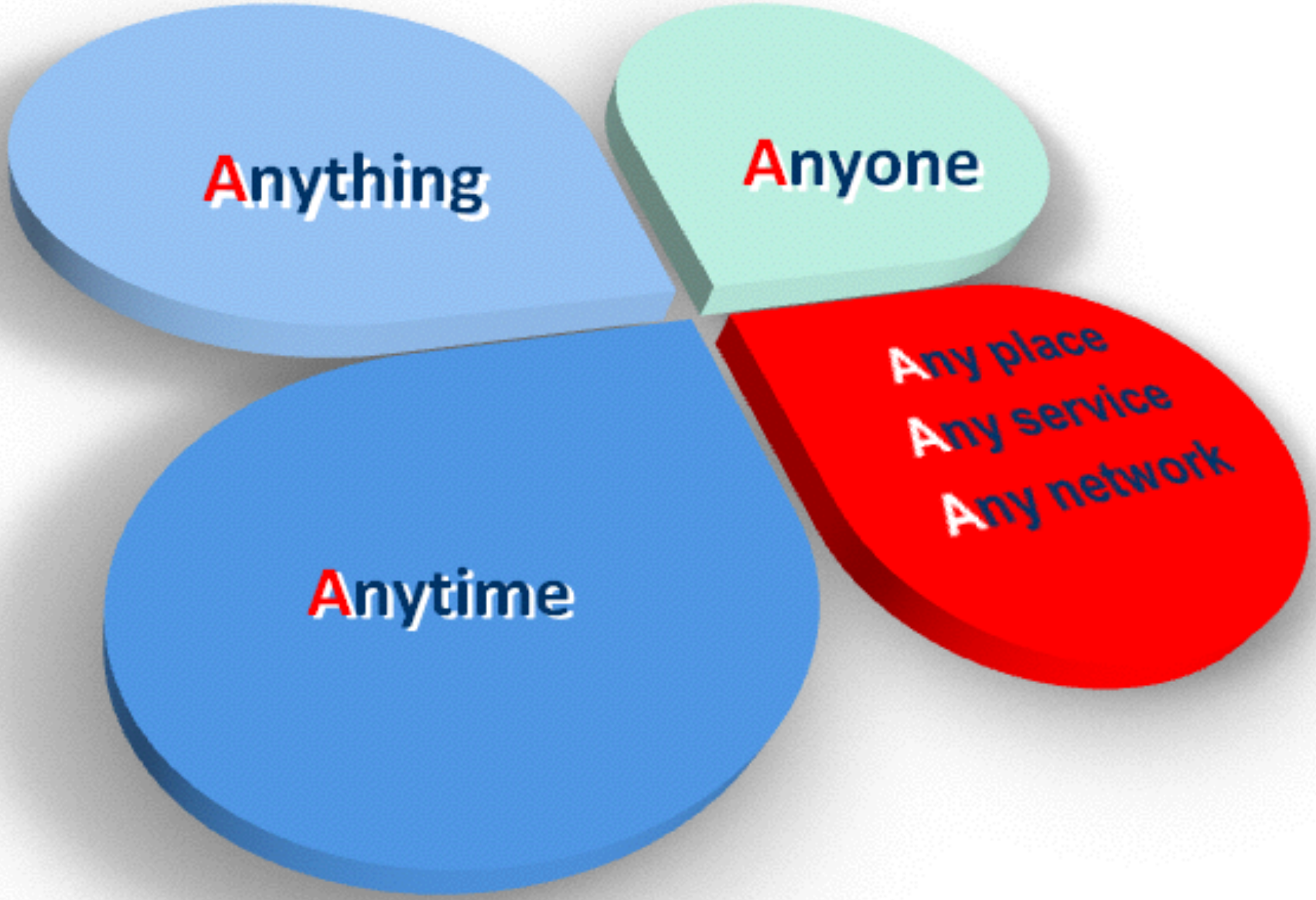
Definition of IoE

"The Internet of Everything (IoE)

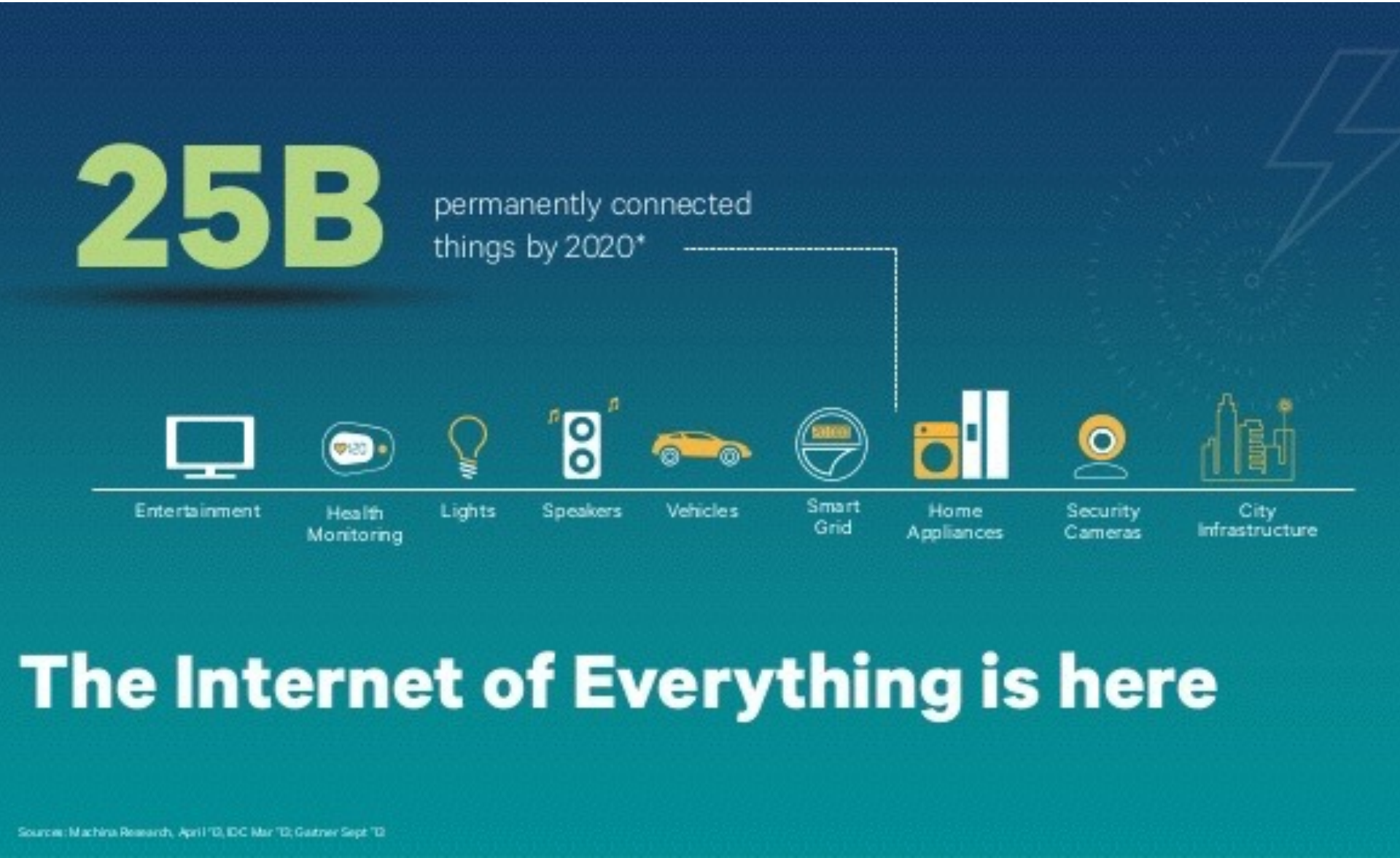
is a scenario in which objects, animals or people are provided with unique smart identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."

TechTarget

Connecting:



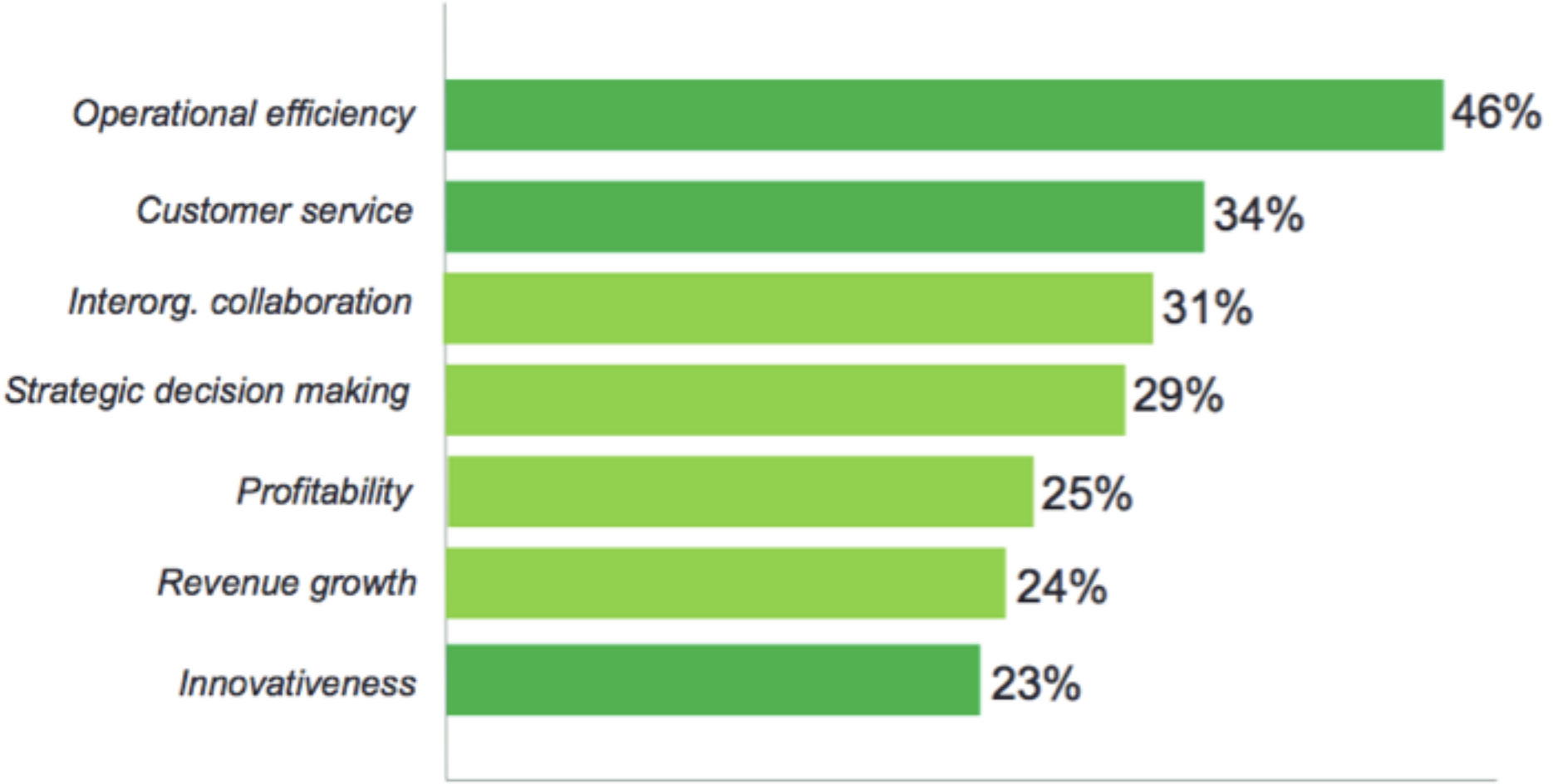
How will IoE change the world?



Most IoE devices will be B2B

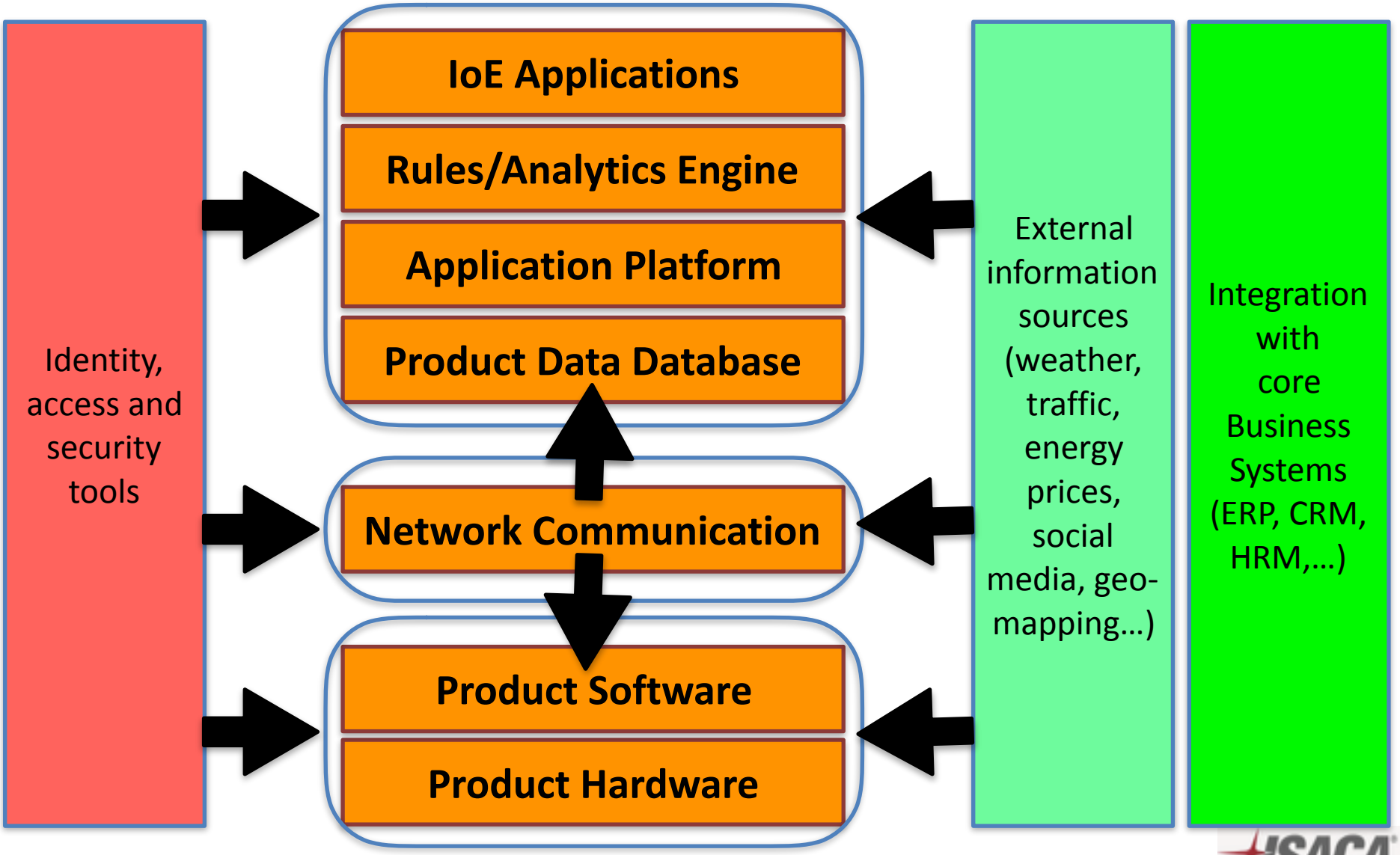
Source: McKinsey Global Institute, Intel infographic

Potential benefits of IoE

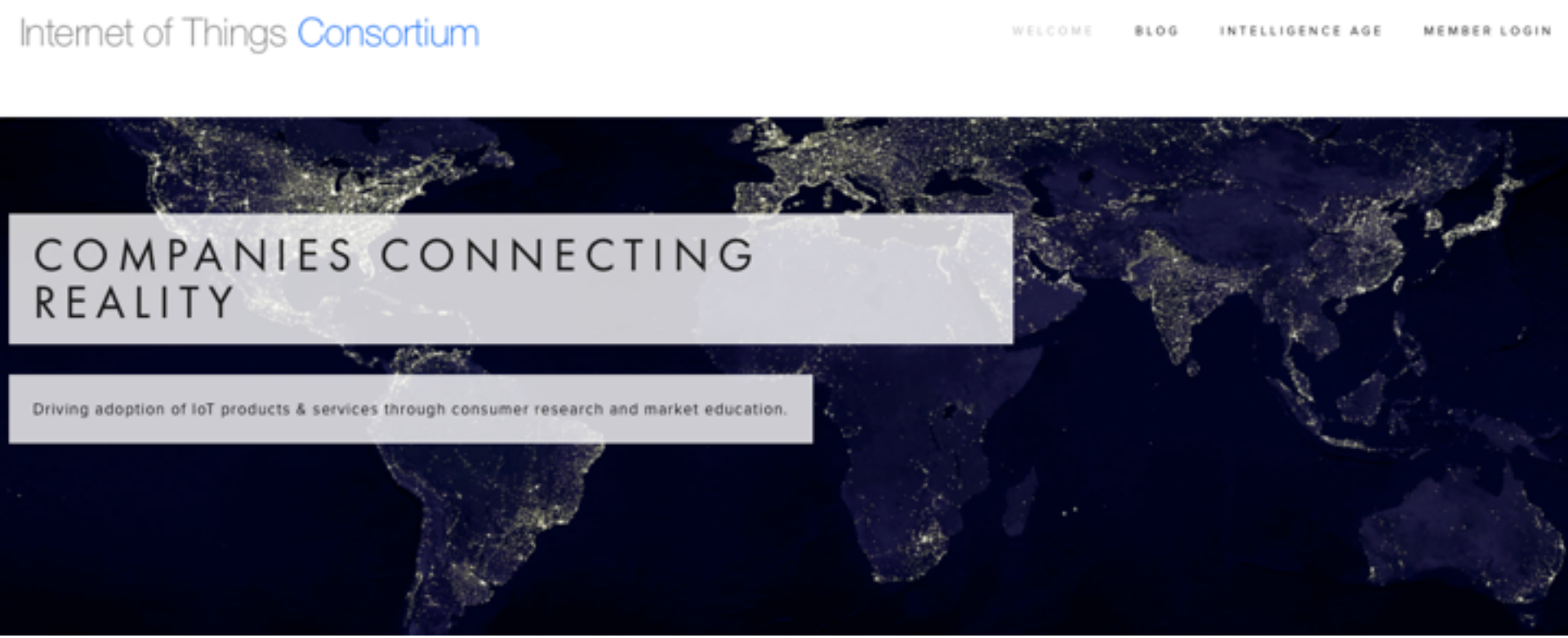


Source: BI Intelligence, Cisco 7000+ global executives

IoE blueprint architecture

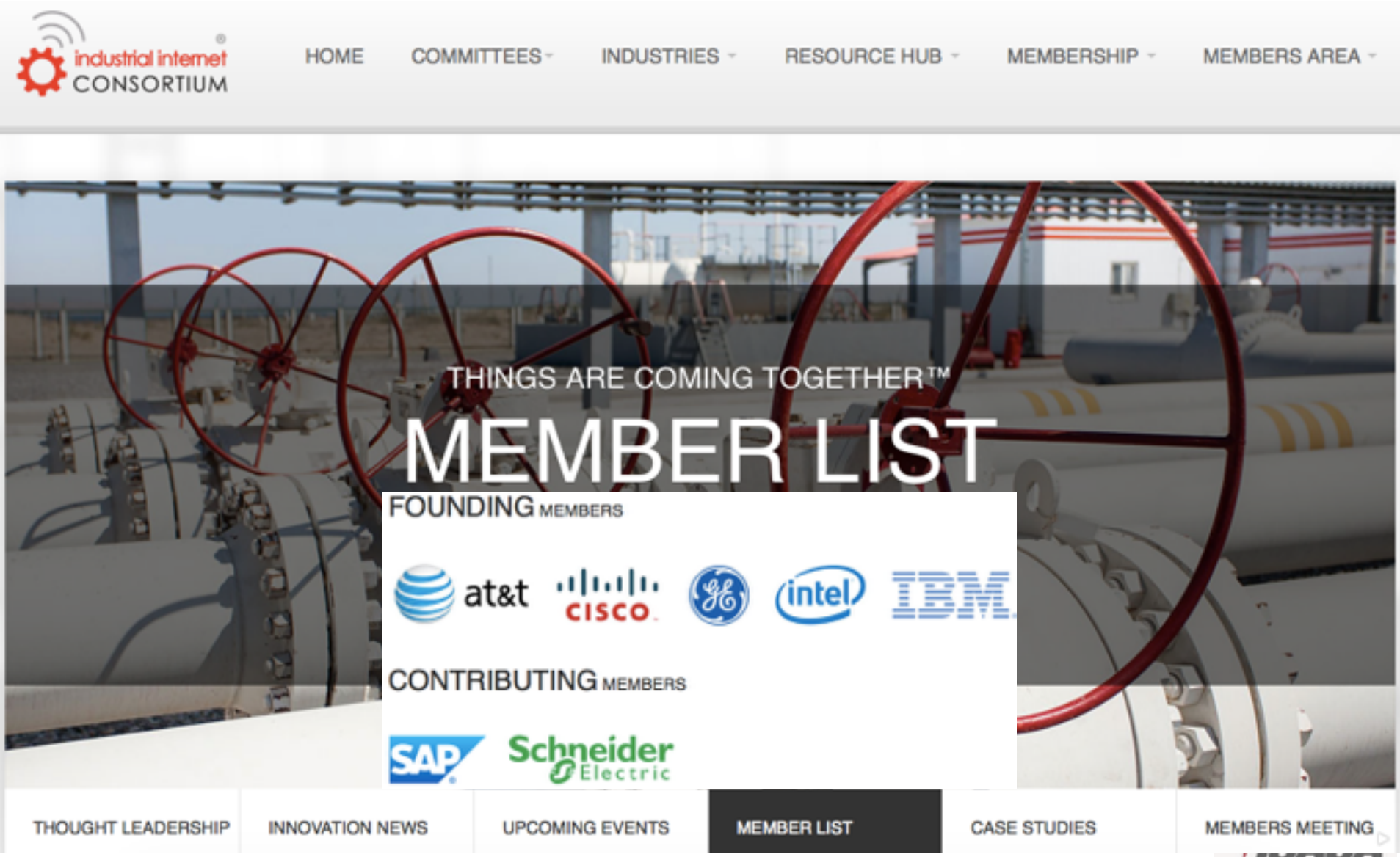


IoE Standards?



The Internet of Things Consortium (IoTC) is comprised of more than 60 leading hardware, software and analytics companies – in areas including home automation, wearables, connected cars, smart cities, 3D printing, and virtual/augmented reality. On behalf of its members, the IoTC is dedicated to the growth of the internet of things marketplace and the development of sustainable business models. The IoTC educates technology firms, retailers, insurance companies, marketers, media companies and the wider business community about the value of IoT. Founded in 2012, the IoTC is headquartered in San Francisco with a business development hub in New York.

IoE Standards?



IoE Standards?

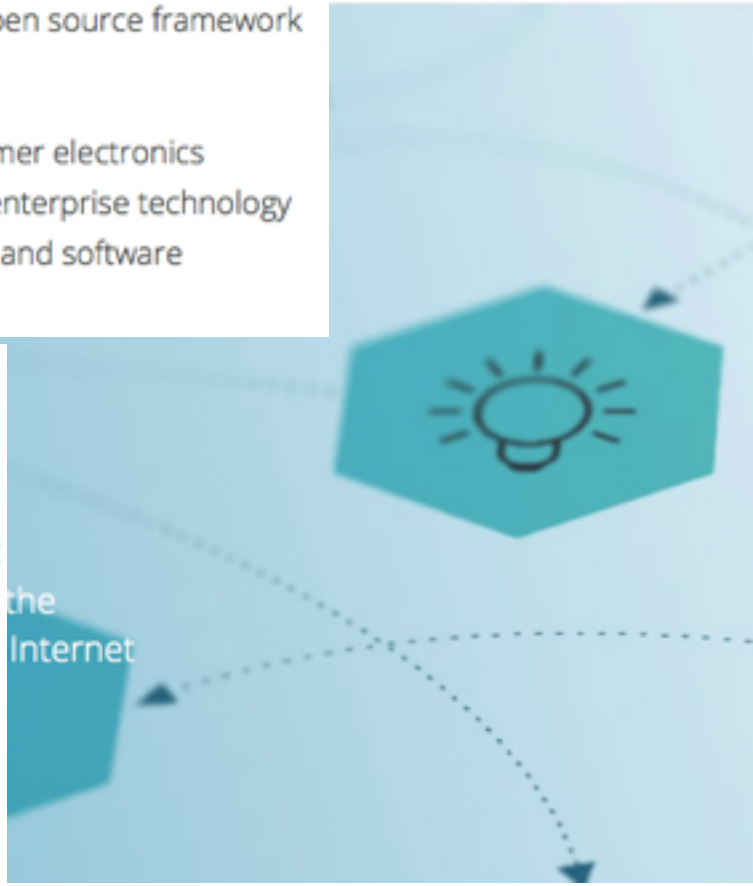
ALLSEEN ALLIANCE

Opportunities Framework Certification Alliance

Announcements News Events Blog Members' Area

Enable industry standard interoperability between products and brands with an open source framework that drives intelligent experiences for the Internet of Things.

The initiative includes more than 185 member companies including leading consumer electronics manufacturers, home appliance makers, automotive companies, cloud providers, enterprise technology companies, innovative startups, chipset manufacturers, service providers, retailers and software developers.



Arçelik A.Ş.

Canon

Electrolux

Haier

LG
Life's Good

Microsoft

Panasonic

PHILIPS

Qeo
a technicolor company

QUALCOMM
QUALCOMM CONNECTED EXPERIENCES, INC.

SHARP

Silicon Image
A Lattice Semiconductor Company

SONY

ISACA

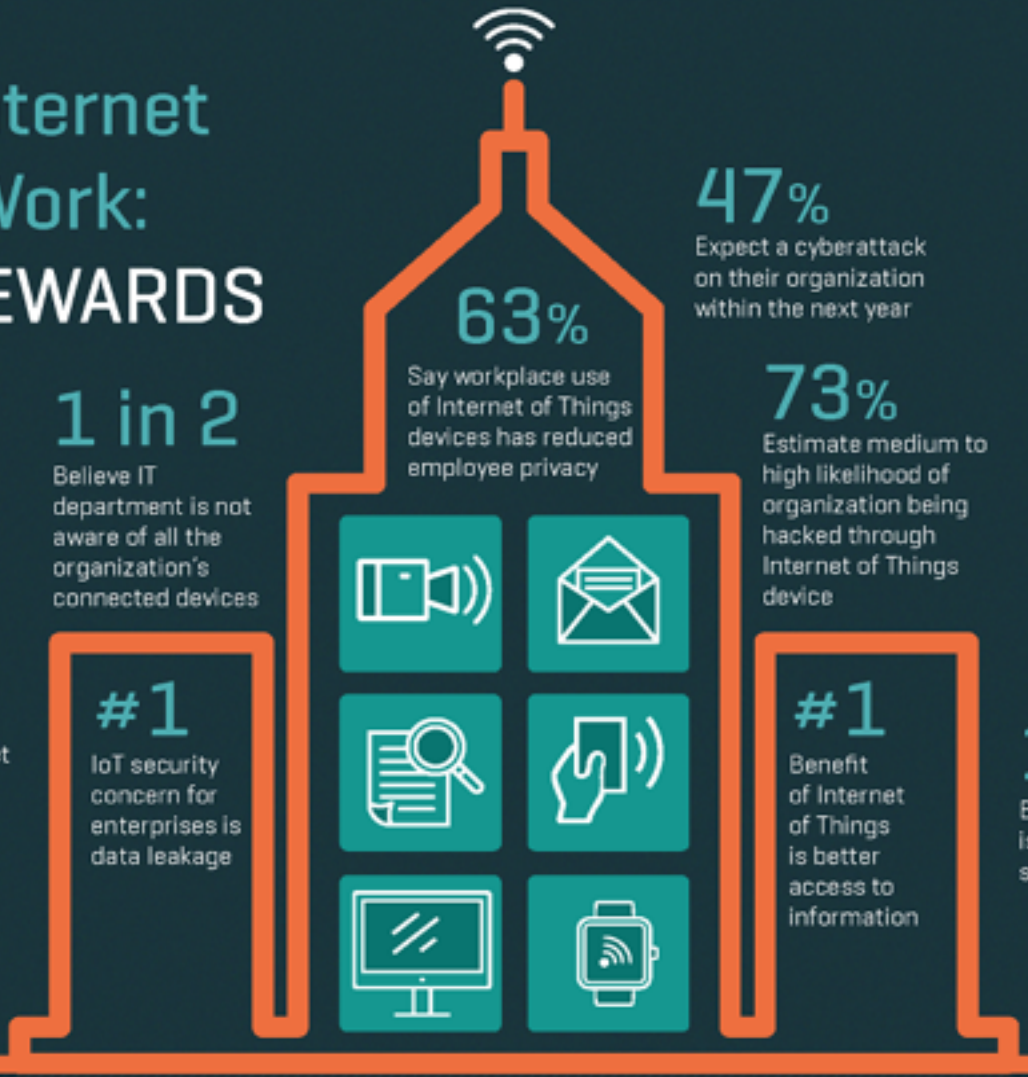
INTERNET OF THINGS:
RISK AND VALUE CONSIDERATIONS

An ISACA Internet of Things Series White Paper

ISACA
Trust in, and value from, information systems

ISACA
trust in, and value from, information systems

The Hidden Internet of Things at Work: RISKS AND REWARDS



63%
Say workplace use of Internet of Things devices has reduced employee privacy

47%
Expect a cyberattack on their organization within the next year

1 in 2
Believe IT department is not aware of all the organization's connected devices

73%
Estimate medium to high likelihood of organization being hacked through Internet of Things device

72%
Believe that Internet of Things device manufacturers do not implement sufficient security

#1
IoT security concern for enterprises is data leakage

#1
Benefit of Internet of Things is better access to information

1 in 3
Believe their organization is unprepared for a sophisticated cyberattack

The Internet of Things will continue to surround and connect people at home, at work and on the road.
The number of B2B Internet of Things devices is expected to expand from 1.2 billion devices in 2015 to 5.4 billion connected devices by 2020 (Verizon/ABI Research). To view IT and cybersecurity professionals' recommendations for maintaining a cyber-secure workplace and learn the steps that consumers can take to protect their data, visit: **www.isaca.org/risk-reward-barometer**.

CSX
CYBERSECURITY NEXUS

Source: ISACA 2015 IT Risk/Reward Barometer, global member survey

IoE risks

Business risk:

- Health and safety
- Regulatory compliance
- User privacy
- Unexpected costs

Operational risk:

- Inappropriate access to functionality
- Shadow usage
- Performance

Technical risk:

- Device vulnerabilities
- Device updates
- Device management

So what does IoE means for privacy?

So what does IoE means for privacy?

The main IoE risk is underestimating security & privacy risks!

“In essence, you've got a computer inside some device, whether it be a printer, a TV, a toaster, the Coke machine, etc., and that computer is just as vulnerable to attacks as a normal computer would be.”

Dan Frye, general manager MAD security

Privacy concerns on IoE

Consumer perspective of disclosing personal info to IoE

POTENTIAL BENEFITS	POTENTIAL COSTS
Convenience Service (information, transaction, entertainment) Customization / Personalization Lower search costs Attention Relationship management Psychological well being	Increasing complexity Referral permission Higher prices Time consuming Spam Attention Reputation management Psychological distress

Privacy concerns on IoE

Organization perspective of using IoE consumer info

POTENTIAL BENEFITS	POTENTIAL COSTS
Efficient and effective strategy development Effective resource allocation and operational practices Increased number of target touch points Customer loyalty management Additional revenue streams	Upfront investment in top IT and top security (24/7) Marketing research costs Business Intelligence and datawarehouse costs Personalisation costs Reputation management Legal compliance costs

Privacy concerns on IoE

- IoE introduces new ways of collecting and processing massive amounts of information from "everything"
  - correlation & association => **abuse potential**
- IoE devices can reveal sensitive information about the individual (like purchasing patterns, driving habits, access codes, locations, …)
  - **Who** can access this IoE data?
  - How should this IoE **data** be **protected**?

Do you have the right to know what companies are collecting your info and how they are using your info?

The Global Information Technology Report 2008–2009

Mobility in a Networked World

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

CHAPTER 1.6

Reality Mining of Mobile Communications: Toward a New Deal on Data

ALEX PENTLAND, Massachusetts Institute of Technology (MIT)

Within just a few years "people data" will be 90% of the world's collective data.

—Jeff Nick, CTO of EMC, personal communication

We have enough water, enough food, enough money; we have enough of everything except the ability to agree and move forward.

—Abdul Kalam, former President of India, personal communication

http://hd.media.mit.edu/wef_globalit.pdf

ISACA

The New Deal on Data

The first step is to give people ownership of their data.

"own your own data"

Old English Common Law has 3 basic tenets of ownership.

http://hd.media.mit.edu/wef_globalit.pdf

The New Deal on Data

"own your own data"

1. The right of possession:

You have a right to possess your data. Companies should adopt the role of a Swiss bank account for your data. You open an account (anonymously, if possible), and you can remove your data whenever you'd like.

http://hd.media.mit.edu/wef_globalit.pdf

The New Deal on Data

"own your own data"

2. The right of use: You, the data owner, must have full control over the use of your data. If you're not happy with the way a company uses your data, you can remove it. All of it. Everything must be opt-in, and not only clearly explained in plain language, but with regular reminders that you have the option to opt out.

http://hd.media.mit.edu/wef_globalit.pdf

The New Deal on Data

"own your own data"

3. The right of disposal: You have a right to dispose or distribute your data. If you want to destroy it or remove it and redeploy it elsewhere, it is your call.

http://hd.media.mit.edu/wef_globalit.pdf

The New Deal on Data

+ ONE EXTRA PRINCIPLE

4. The right of anonymously sharing:

You have the right to share massive amounts of your data anonymously to promote the common good, since aggregate and anonymous data can dramatically improve society. Patterns of how people move around can be used for early identification of infectious disease outbreaks, protection of the environment and public safety. It can also help measure the effectiveness of various government programs and improve the transparency and accountability of government and non-profit organizations.

http://hd.media.mit.edu/wef_globalit.pdf

The New Deal on Data

"own your own data"

4 basic tenets of ownership:

1. **The right of possession**
2. **The right of use**
3. **The right of disposal**
4. **The right of anonymously sharing**

http://hd.media.mit.edu/wef_globalit.pdf

Applying Privacy by Design in IoE

1) Integrate IoE data quality as a design discipline in all processes

- Ask what data really need to be captured, and what data really need to be stored vs. what can be processed in real time without storing.
- Aim to store data showing a consumer action separately from data showing what triggered that action or the actual consumer behaviour.
- Preemptively outline data risks and intended course of action in the event of crisis.

Applying Privacy by Design in IoE

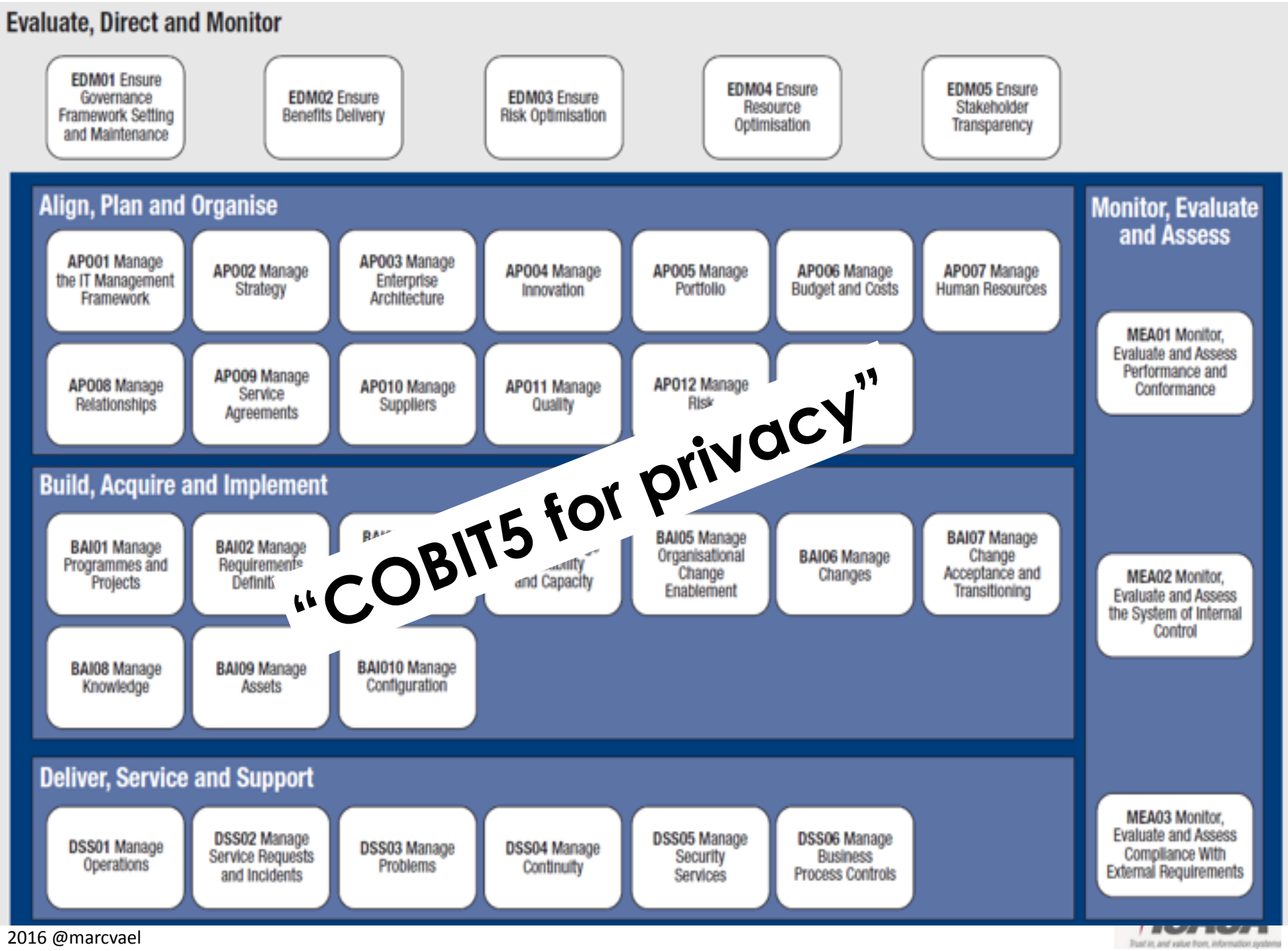
2) Evolve from complex legal fine print to transparent IoE disclosures

- Disclose all intended and potential future uses of consumer data in simple language at the point of data collection.
- Incorporate store/do not store and use/do not use checkbox options on forms next to sensitive data fields.
- Offer and train live chat experts to answer privacy questions (not just product/service questions) directly.

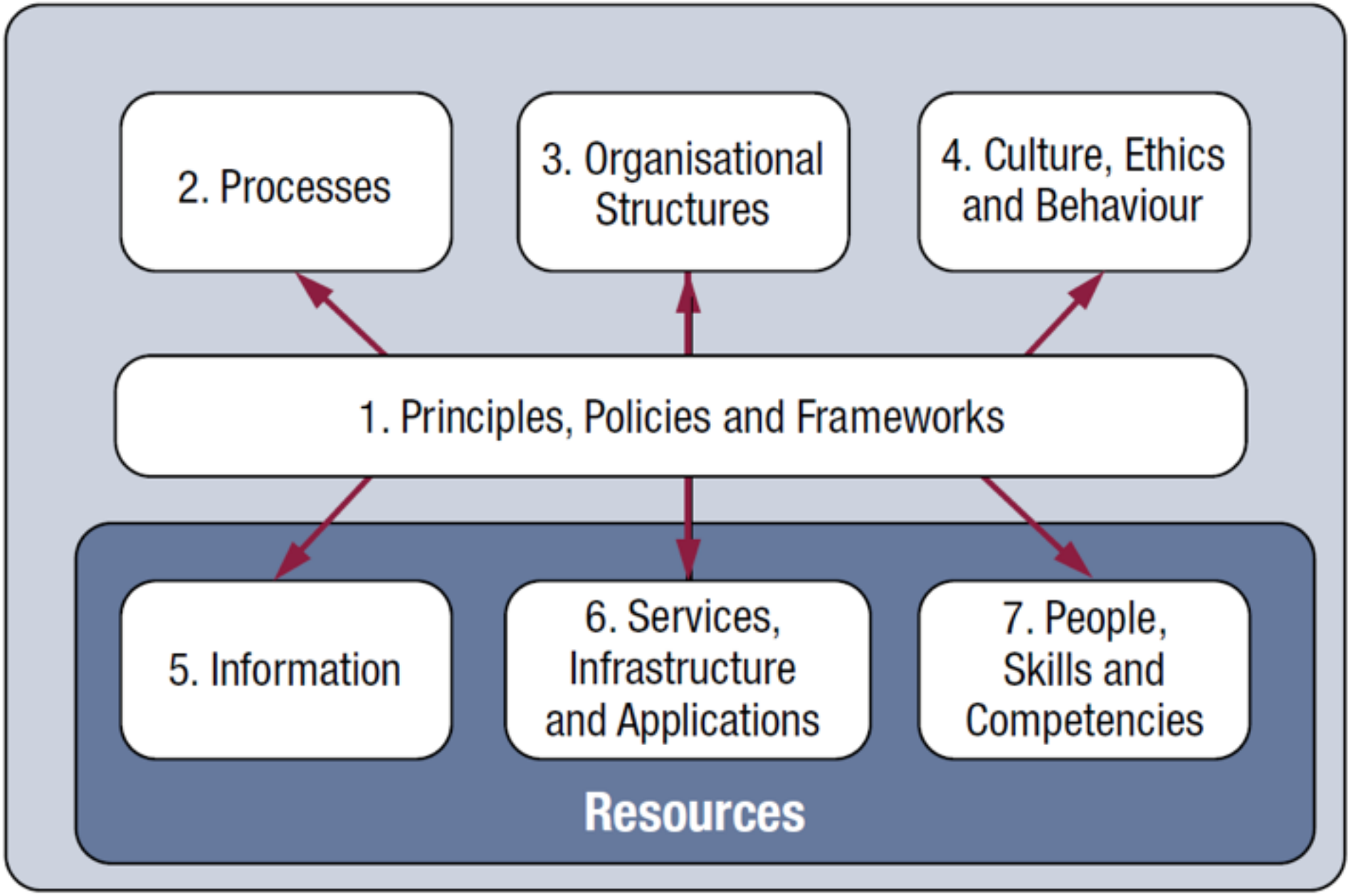
Applying Privacy by Design in IoE

3) Make privacy a positive part of the IoE brand experience

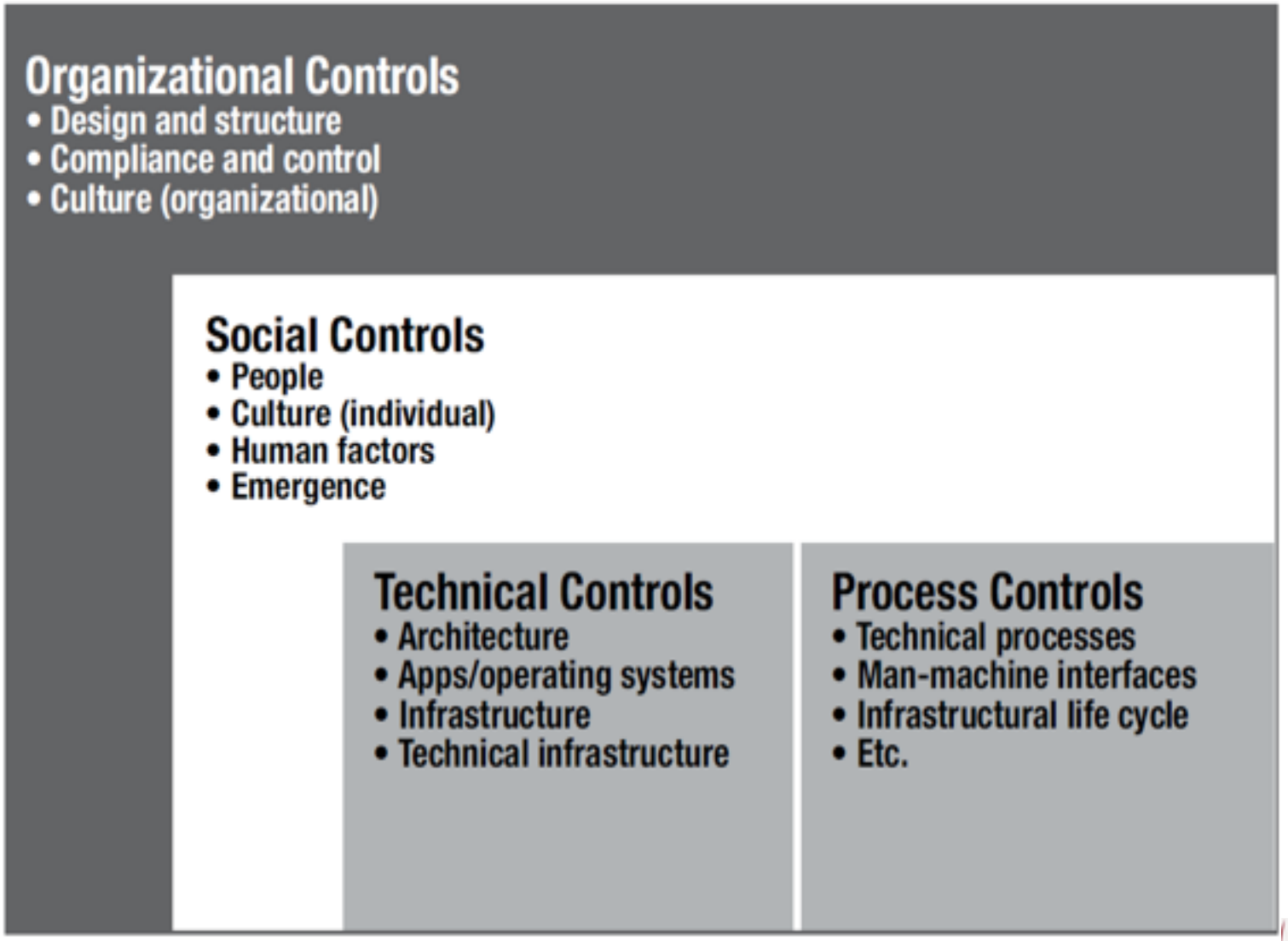
- Formalize robust preference centers as a new user experience best practice, including options to receive (or not receive) content customized to location, interests and purchase history.
- Make privacy decision points more bite-size and contextual.
- Have the system reviewed by specialist data auditors



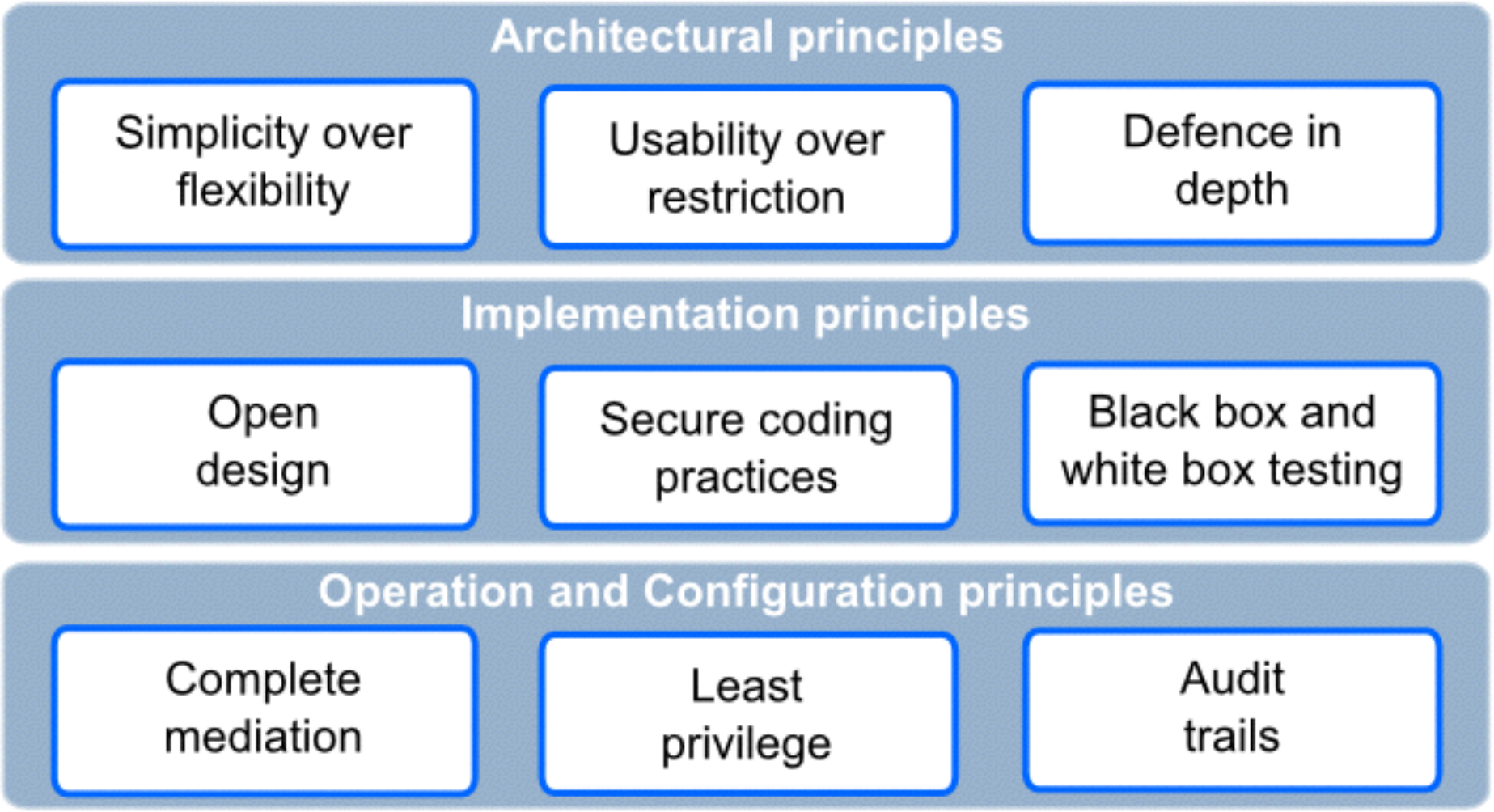
2016 @marcvael



Applying Privacy by Design in IoE



Applying Privacy by Design in IoE



Source: www.opensecurityarchitecture.org

Practical advantages of applying Privacy by Design in IoE

In short, **EVERYBODY WINS**

Protecting consumers and brand integrity and building consumer confidence whilst delivering on efficiency, effectiveness, bottom line and increasing customer experience and loyalty.

Practical advantages of applying Privacy by Design in IoE

In short, **EVERYBODY WINS**

The new data economy will be healthier if the relationship between companies and consumers is more respectful and balanced. That is much more sustainable and will prevent real life disasters.

Practical advantages of applying Privacy by Design in IoE

In short, **EVERYBODY WINS**

The new data economy will bring first greater stability and then eventually greater profitability as people become more comfortable sharing their own data.

Practical advantages of applying Privacy by Design in IoE

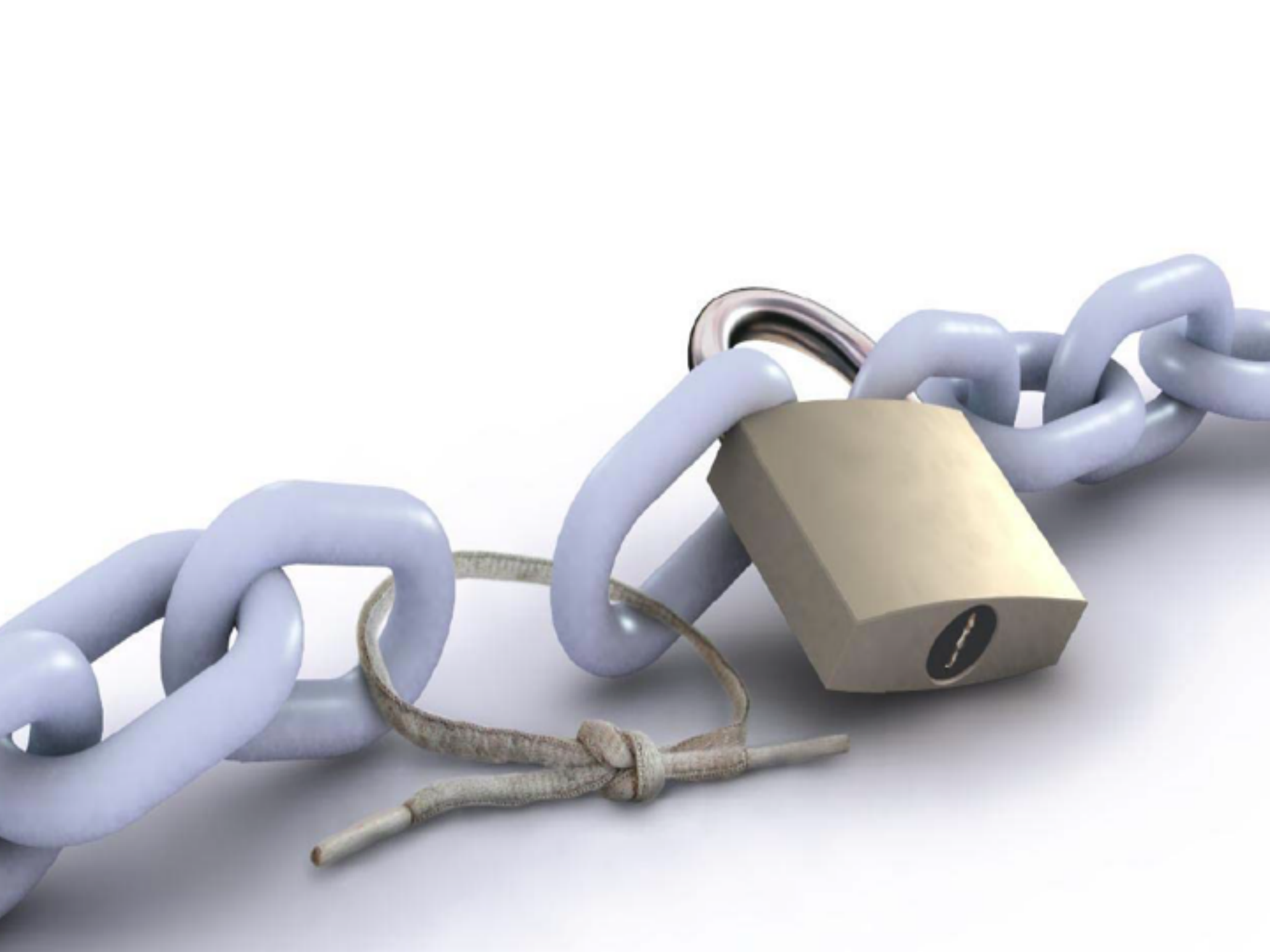
By adopting a sound transparent privacy-by-design approach from the start, IoE solution providers can transform their innovative ideas into good practices that provide long-term trust and value for both IoE users and themselves.

Practical advantages of applying Privacy by Design in IoE

Trust in, and value from, IoE solutions

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier,
Security Technologist (www.schneier.com)



Contact details

Mr. Marc Vael

President

ISACA BELGIUM vzw

Koningsstraat 109 box 5

1000 Brussel

Belgium

www.isaca.be

www.isaca.org

president@isaca.be

marc@vael.net

http://www.linkedin.com/in/marcvael

@marcvael