Is the IoT a threat to people, or on the contrary?

Piotr Pietrzak

Chief Technology Officer,
IBM Poland and Baltics

Grzegorz Śniadała

Senior IT Manager
P&G Global Business Services Senior IT Manager

Sławomir Lubak

Managing Director,
Communication Media & Technology
Accenture Poland

Michał Grabarz
Sales Director at Communications, Media and Technology, Accenture

accenture Strategy | Consulting | Digital | Technology | Operations

Let’s share our view

www.absl-conference.com/app

Surveys & Questions

Connected Operations

- CONNECTED PRODUCTION OPERATIONS
- CONNECTED MINE
- CONNECTED INDUSTRIAL WORKER
- CONNECTED INDUSTRIAL EQUIPMENT
- GETTING STARTED WITH SMART MANUFACTURING
- RFID TECHNOLOGY AS A KEY ENABLER FOR IIOT DEPLOYMENTS

Connected Transportation

- CONNECTED VEHICLE DASHBOARD ANALYTICS
- DRIVECONNECT
- CONNECTED VEHICLE LIVE

Connected Commerce

- PRODUCT AND SERVICES MARKETPLACE FOR IOT DEVICES

Connected Health

- CONNECTED WELLNESS AND PREVENTION
- CONNECTED CLINICAL TRIALS

Connected Spaces

- CONNECTED HOME
- CONNECTED OFFICE

High performance. Delivered.

Which of the below activities and directions do you find as the most important to counteract the IoT related threats:

1. **DESIGN** - Apply secure-by-design principles to components and products.
2. **MODEL** - Incorporate key business goals, the underlying technical infrastructure into the (security) models.
3. **LEARN** - Apply mobile and cyber-physical system (CPS) security lessons from early adopters (industries like telecoms?)
4. **MONITOR** - Continuously monitor the IoT's operational and security health
5. **GUARD** - Maintain access and authorization rights to data sets
6. **RACE** - Track and use emerging standards
7. **EDUCATE** - Continue to educate systems users

By 2030, the optimized production processes that the IIoT heralds could add trillions of dollars to the global economy and significantly improve long-term job growth—in part by bringing manufacturing back onshore

84%

asserted they could create new income streams from Indutrial IoT

VS

7%

have developed a comprehensive strategy

Accenture surveyed more than 1,400 global business leaders,

https://www.accenture.com/pl-en/insight-industrial-smart-production

accenture Strategy | Consulting | Digital | Technology | Operations

High performance. Delivered.

Which is the main area stopping us or slowing us down from secure IoT adoption?

1. **DESIGN** - Apply secure-by-design principles to components and products.
2. **MODEL** - Incorporate key business goals, the underlying technical infrastructure into the (security) models.
3. **LEARN** - Apply mobile and cyber-physical system (CPS) security lessons from early adopters (industries like telecoms?)
4. **MONITOR** - Continuously monitor the IoT's operational and security health
5. **GUARD** - Maintain access and authorization rights to data sets
6. **RACE** - Track and use emerging standards
7. **EDUCATE** - Continue to educate systems users

Five Cybersecurity Gaps Undermining Digital Trust

TALENT GAP

54% indicated their employees are underprepared to prevent security breaches.

TECHNOLOGY GAP (cyber threats growth vs ability to deploy & leverage new technologies to secure business initiatives)

The largest threat growth was anticipated in emerging technologies to mitigate advanced threats:

- cognitive computing/AI (33% increase)
- data anonymization (31% increase)
- behavioral tracking (25% increase)
- automation (21% increase).

PARITY GAP

BUDGET GAP

MANAGEMENT GAP

35% believed management is unconcerned with security, and 36% believed management considers security an unnecessary cost.

Accenture and HfS Research surveyed more than 200 enterprise security professionals
https://www.accenture.com/pl-en/insight-cybersecurity-digital-trust-2016

Todays survey results

High performance. Delivered.