

# Holistic cybersecurity for the AIoT ecosystem

Panel discussion – session 5

**Dr. Jesus Luna Garcia**

# Panel Discussion

## Setting the context – AIoT and Cloud

- AI-enabled IoT systems (**AIoT**) are intrinsically related to **digital transformation**, even in our daily life.
- This is an ever-growing global market, which has a **huge dependency on (complex) cloud systems and architectures**.
  - Hybrid-cloud
  - Multi-cloud
  - Cloud plugins, cloud APIs, cloud marketplaces
- Given the pervasive nature of AIoT, consumers need to have **confidence in the cybersecurity** of connected products and solutions.

How CIOs and CEOs accelerate digital transformations through cloud platforms

September 15, 2020 | Article

By Jayne Giermo, Mark Gu, James Kaplan, and Lars Vinter

To capture the real value from cloud, companies need to focus their investments and build a cloud-ready operating model.

It has been more than a decade since the first corporate experiments with external cloud platforms, and the verdict is long in on their business value. Companies that adopt the cloud well bring new capabilities to market more quickly, innovate more easily, and scale more efficiently—while also reducing technology risk.

DOWNLOADS

Article (10 pages)

Source: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms>

# Panel Discussion

## Challenges

- Parallel to its growth, **consumer trust in AIoT** has shaken since several years.
- Where are (some of) the challenges?
  - Misconfigurations (*cloud / AIoT*)
  - Shared responsibility (*cloud*)
  - Alignment with enterprise cybersecurity framework (*cloud*)
  - Externalization of cloud cybersecurity (*MSSP*)
  - Security culture (*cloud / AIoT*)
- Is it about AIoT or cloud?
  - Both 😊 we the need **holistic approaches!**



### “Hopeless”

Ron Rivest (2012), Co-Inventor of RSA-Crypto Systems, Turing Award (2002)



### “Lousy IoT Security”


Bruce Schneier (2019) Writer, fellow and lecturer at Harvard's Kennedy School, board member of Electronic Frontier Foundation

## SECURITY BOULEVARD

Home ▾ Security Bloggers Network ▾ Webinars ▾ Chat ▾ Library Related Sites ▾ Media Kit

ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES

Home » Security Bloggers Network » Most Cloud Breaches are Due to Misconfigurations

 Most Cloud Breaches are Due to Misconfigurations  
by David Mundy on April 29, 2019

TechRepublic.

SEARCH

QGift Guides Black Friday Deals Windows 10 20H2 Update COVID-19 IT Policy Downloads More ▾ Newsletters Forums Resources

Cloud misconfigurations cost companies nearly \$5 trillion

# Panel Discussion

## Holistic cybersecurity

- Notwithstanding its criticality, **cloud systems are not deployed in isolation.**
  - Cloud is essential part of service/supply-chains for AIoT and other connected products.
- Therefore, cybersecurity must be seen as a whole/**end-to-end** solution.
- In such complex scenarios, additional challenges (e.g., interoperability of SIEM solutions) become more evident.



Source (2007): <https://youtu.be/1N9zKS9s4oY>

# Panel Discussion

## Strengths and Opportunities – EU focus

### ■ Where are the strengths?

- Strong regulatory framework
- Many relevant R&D+I initiatives
- Conspicuous increase of cloud security solutions in the market
- Cloud provides huge automation capabilities (cybersecurity included)

### ■ Where are the opportunities?

- Interoperability and standardization ([we're still cutting through the jungle](#))
- Concrete guidance/good-practices for shared responsibility
- *Productization* of R&D+I activities
- Trainings and skillset (special focus on SaaS)



### ■ Food for thought:

- Cybersecurity vs. Trustworthiness
- How secure is a cloud-security solution? (see next panel on certification)



# Thanks!

[jesus.lunagarcia@de.bosch.com](mailto:jesus.lunagarcia@de.bosch.com)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952633

