Breaking Down the Silos:

Integrating Privacy, AI, and Cyber into Core Corporate Governance.

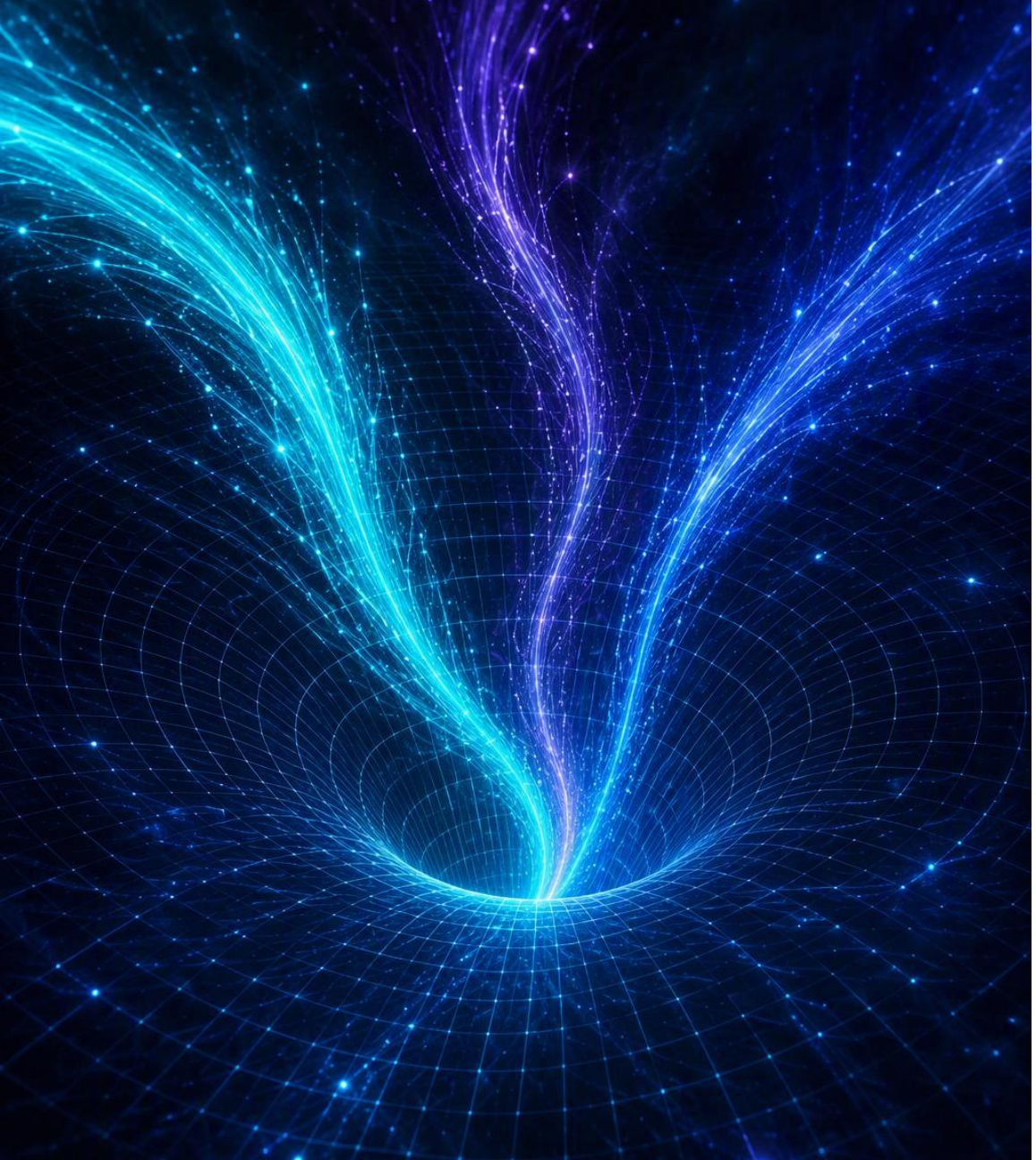
IAPP European Privacy KnowledgeNet 2026
Munich

Thoralf Knuth, Bosch

Pictures and Illustrations AI-generated

Public C-SC0

BOSCH



The new and shared “Gravity Well”

- **The Reality:**
  Security, Privacy, and AI have collapsed into a single risk domain.
- **The Scale Challenge:**
  One-size-fits-all governance does not exist.
- **The Mission Today:**
  Share cross-industry experiences, failures, and ideas.

BOSCH

The Cross-Silo Blindspot

- **The Scenario:** Deploying an external AI-driven service.
- **The “Silo Success” Illusion:**
  - **IT/Security:** Firewall and cloud access are locked down.
  - **Legal/Privacy:** Basic data-minimization rules are checked.
  - **Product/AI:** The model is optimized for maximum helpfulness.
- **The Blindspot:** An adversarial input bypasses the perimeter, tricking the model into leaking training data.





Cross-Industry Approaches

- **Continuous Compliance**
  Embedding and Automating privacy & security checks directly in the development pipeline.

- **Integrated Risk Translation**
  Linking technical vulnerability scores directly to corporate risk registers.

- **Financial Risk Quantification**
  Translating cyber and privacy threats into standard risk management terms.

BOSCH



Where do we all sit?

- **The Trade-Offs:** Balancing agility, budget, and regulatory risk.
- **Our Discussion Agenda:**
  - How does your company bridge the gap between technical teams and legal compliance?
  - Where have you seen cross-department communication break down?
  - What is one lightweight, practical “silo-buster” you’ve successfully used?

BOSCH

Examples & Exchange

Public C-SC0

BOSCH

Breaking the Silos
Examples

DPO Audits as the “Front Line” of Internal Controls

- Historically, Data Protection Officer (DPO) audits and Internal Audit (IA) functions operate in separate tracks. Bridging them creates a highly efficient, unified defensive line.
- How it could work:
  - Continuous Monitoring vs. Point-in-Time Auditing: Link typical checks (TIA, DPIA, LIA etc.) into a standardized a control approach
  - Combine DPO audits with internal controls, internal audits etc.
  - Make DPO audits not singular measures, but part of compliance or security audits

© Robert Bosch GmbH 2026. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Breaking the Silos
Examples

Cyber and InfoSec, AI and Privacy risks as part of the corporate risk management

- Cybersecurity often suffers from “technical translation loss.” CISOs present risks using technical terms (e.g., "unpatched vulnerabilities," "SQL injections"), DPOs present risks with legal terms (e.g., “insufficient legal basis”, “data subject rights”) while the Board of Directors speaks in financial terms (e.g., "value at risk," "return on investment").

- How it could work
  - Apply risk methodology: Rather than saying: *“Our database has a high risk of being breached.”*
    You translate it to: *“There is a 10% probability that we will experience a data breach in the next 12 months, resulting in a financial loss of **EUR xxm to EUR xxm** (incorporating DPO fines, forensic costs, and operational downtime).”*

© Robert Bosch GmbH 2026. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Breaking the Silos
Examples

- Merge Cyber and Privacy incident process and handling, also include AI; don’t forget Quality and Product, don’t forget compliance
- Use unified product lifecycle (security & privacy by design in the development)
- “Steal” ESG metrics
- Do not limit red teaming just to Cyber Security

© Robert Bosch GmbH 2026. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.