Amplifying Your Privacy Program: Strategies for Success

Dan Costa
Carrie Gardner

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Today’s Discussion

State of the Practice for Privacy Programs
Privacy Program Alignment
Current and Future Work
State of the Practice for Privacy Programs

- Compliance-driven
- Rapidly changing and varied regulatory landscape
- Policy-practice gap
- Nascent technical controls
Risk Mindset

The Business Case for a Privacy Risk Mindset

- Data Breaches Happen
  - Financial Impact
  - Infrastructure Impact
  - Brand/Credibility Impact
  - Reporting Requirements
- Active Control of Risk
- Swift Recovery
- Compliance Management

**Goal:** Operational resilience through effective risk management

**Figure 2** Business impact of privacy

- Percentage of companies getting significant benefits in each area, N=2549

- 67% Reducing sales delays
- 71% Mitigating losses from data breaches
- 71% Enabling agility and innovation
- 72% Achieving operational efficiency from data controls
- 73% Making company more attractive to investors
- 74% Building loyalty and trust with customers

Source: Cisco 2020 Data Privacy Benchmark Study
Privacy Program Alignment

Enterprise Risk Management

- Financial
- Information Technology
- Compliance
- Strategic
- Insider Risk
- Privacy
- People
- Process
- Technology

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.
Current and Future Work

• Research
  • PII identification and categorization
  • Control design, verification, and validation
  • Operational performance

• Potential Artifacts
  • Privacy by design for build or buy decisions
  • Privacy by design system assessment
  • Privacy program evaluation

• Outreach
  • Privacy Special Interest Group (PSIG)
Questions & Answers