Amplifying Your Privacy Program: Strategies for Success

Dan Costa

Carrie Gardner

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM21-0303

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

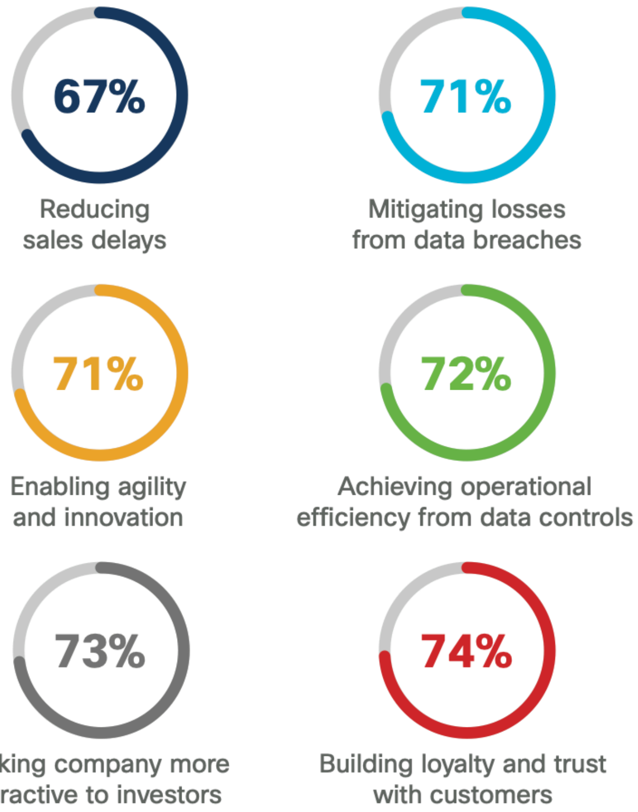
Risk Mindset

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

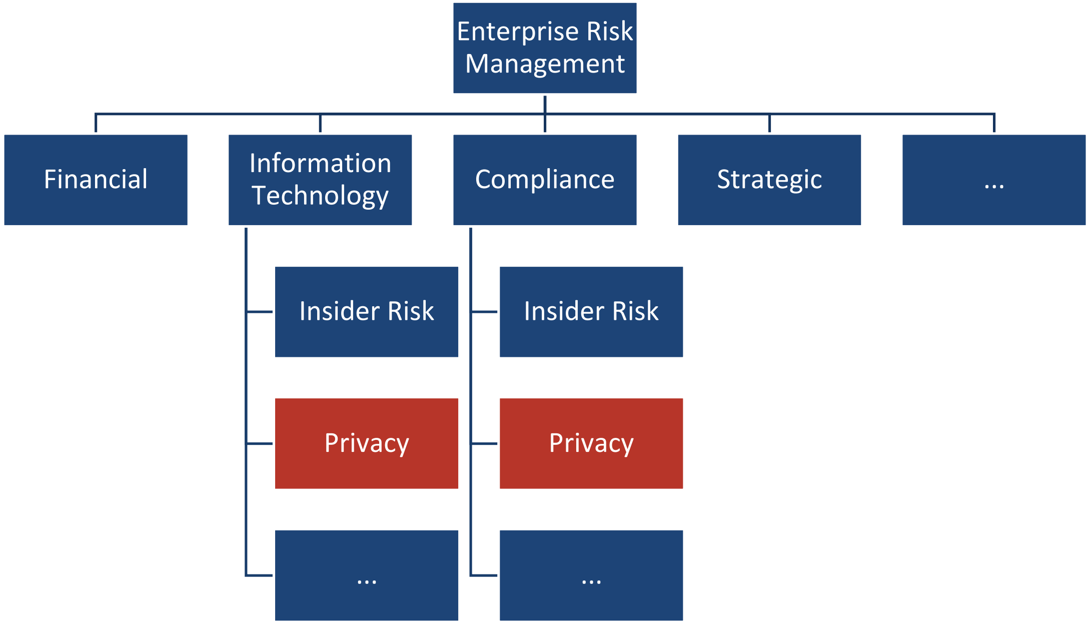
Goal: Operational resilience through effective risk management

Figure 2 Business impact of privacy
Percentage of companies getting significant benefits in each area, N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

Privacy Program Alignment



Enterprise Risk Management

Financial

Information Technology

- Insider Risk
- Privacy
- …

Compliance

- Insider Risk
- Privacy
- …

Strategic

…

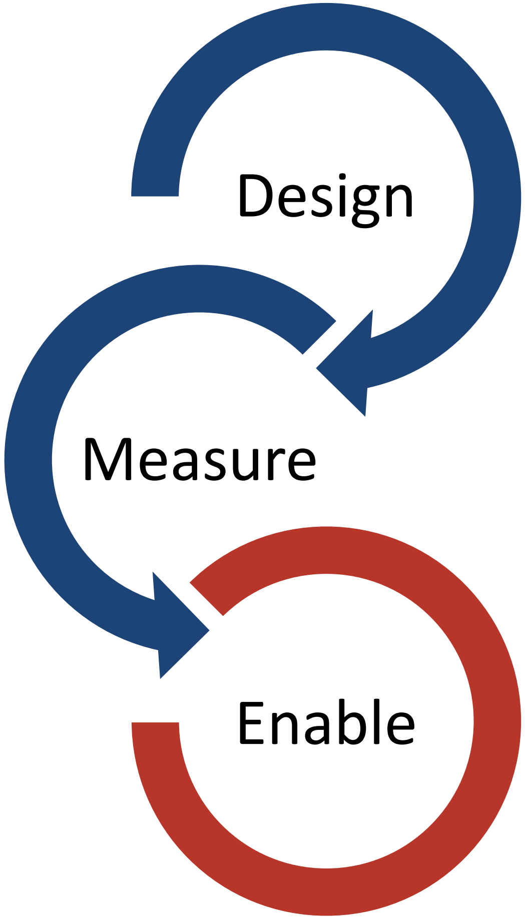
People

Process

Technology

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

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