RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PRV-W01

NIST Privacy Framework IRL: Use Cases from the Field

MODERATOR: **Naomi Lefkovitz**
Senior Privacy Policy Advisor
NIST
@NISTcyber

PANELISTS: **Nick Oldham**
Chief Privacy and Data Governance Officer
Equifax

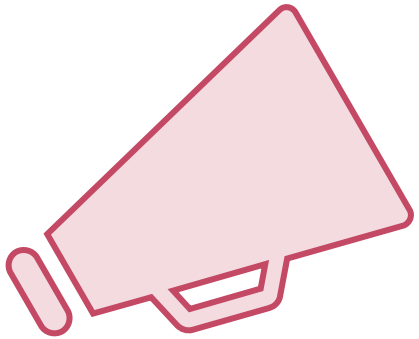
Timothy McIntyre
Associate General Counsel, Privacy and Product
Okta

Value Proposition

Privacy Framework supports:

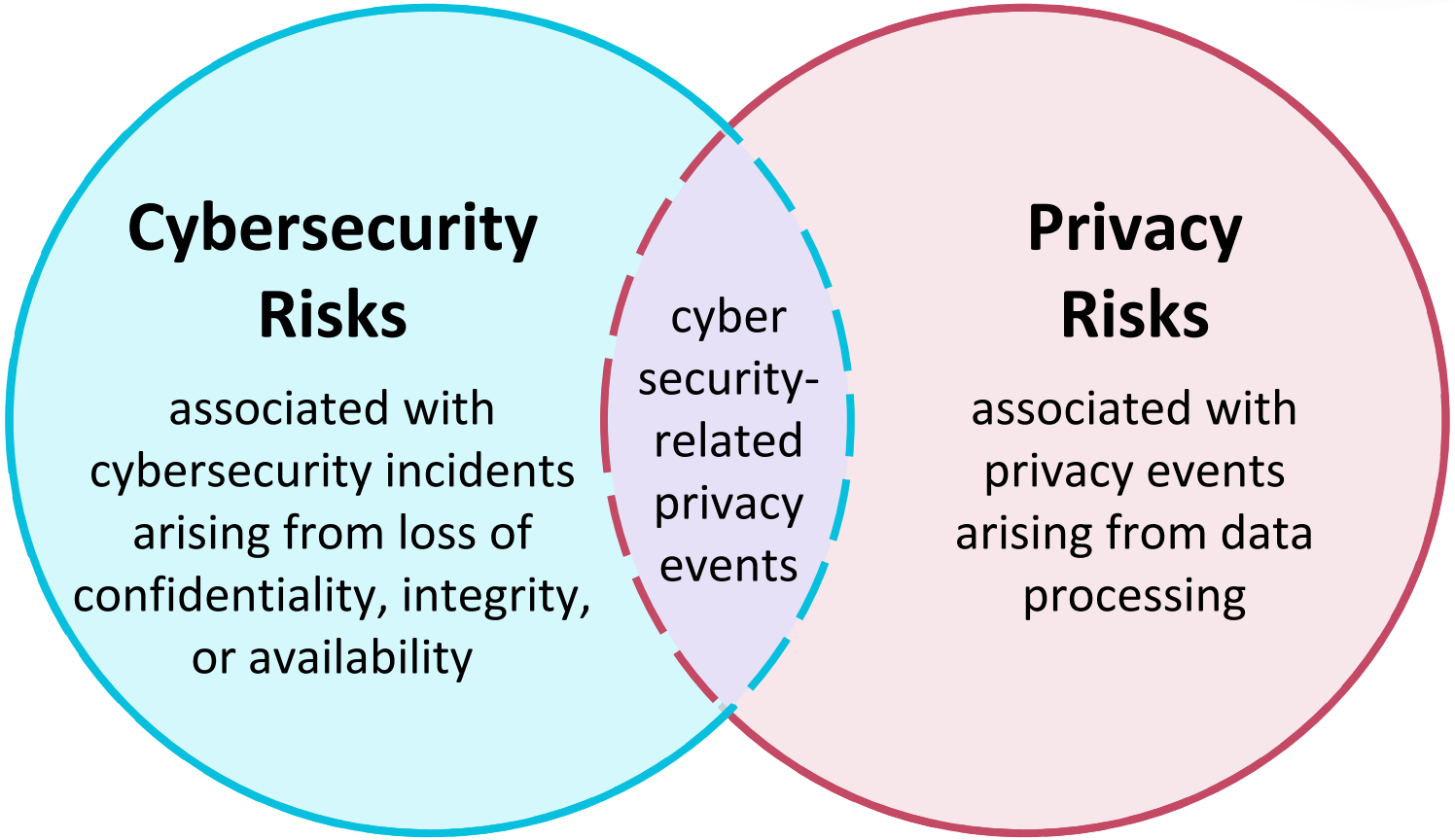
Building customer trust

Fulfilling current compliance obligations



Facilitating communication

Relationship Between Cybersecurity and Privacy Risk



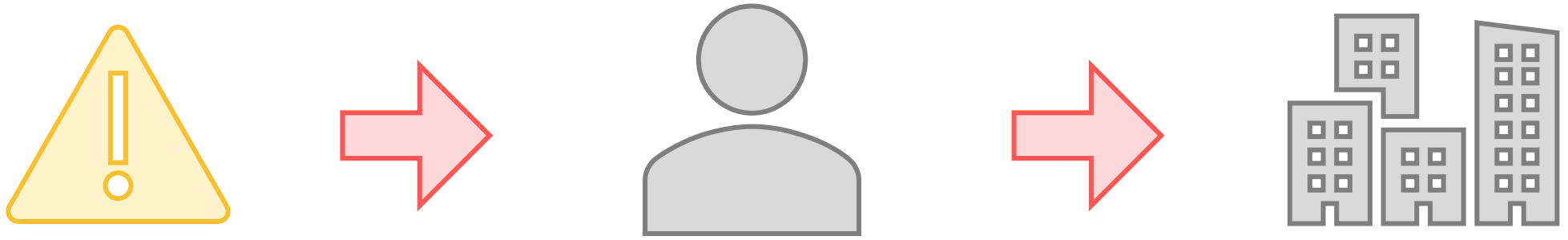
Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

Privacy Risk and Organizational Risk



Problem

arises from data processing

Individual

experiences direct impact
(e.g., embarrassment, discrimination, economic loss)

Organization

resulting impact
(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

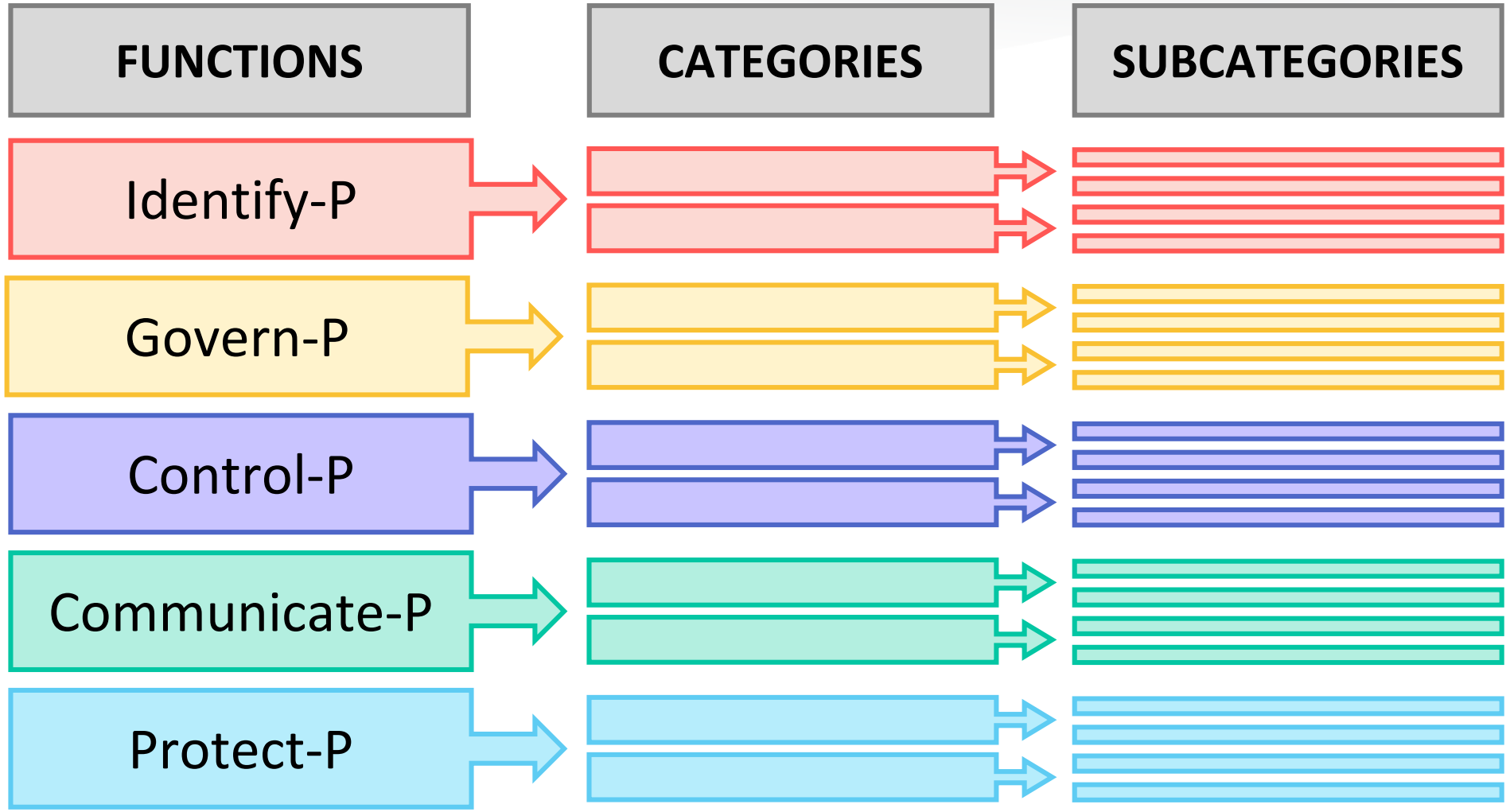
Privacy Framework Structure

The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

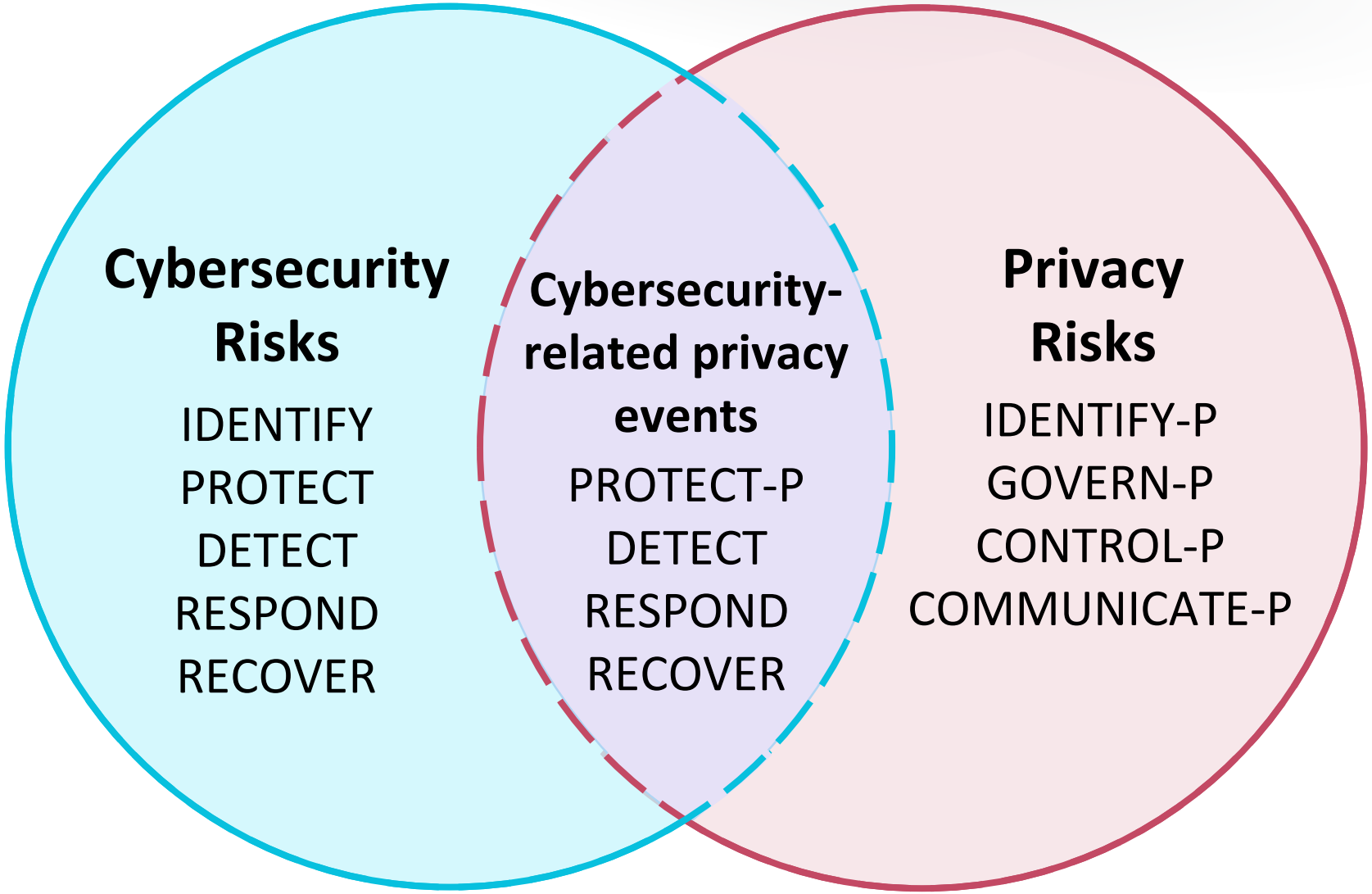
Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk

Implementation Tiers help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

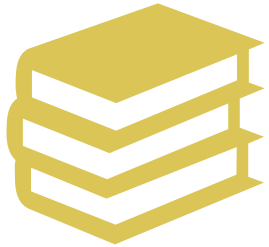
Privacy Framework Core



Cybersecurity Framework Alignment

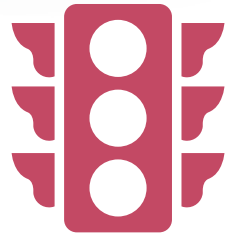


How to Use the Privacy Framework



Informative References

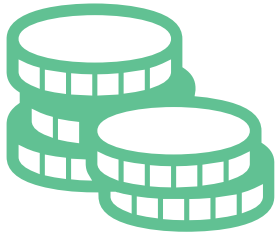
Strengthening Accountability



Establishing or Improving a Privacy Program

Applying to the System Development Life Cycle

Using within the Data Processing Ecosystem



Informing Buying Decisions

RSAConference2020

NIST Privacy Framework IRL at Okta

Tim McIntyre, Data Protection Officer & Associate General Counsel, Okta

RSAConference2020

Okta’s Privacy Commitments

Okta's Core Privacy Principles

- With Okta, Customers always own their Customer Data
- Okta is committed to only using Customer Data in order to provide the services that customers purchase under their contracts with us
- It's our most critical priority to ensure that Customer Data is kept safe and secure

Okta's Compliance

- Okta complies with the GDPR, CCPA, and applicable data protection laws in its provision of our services to our customers
- Service Organization Control 2 ("SOC 2")
- Comprehensive Information Security Management Program ("ISMP")
- ISO 27001, 27002, and 27018 Certifications
- FedRAMP (Moderate Impact Level)
- Okta's services help customers comply with NIST guidance

RSAConference2020

NIST Privacy Framework

Implementation of NIST Privacy Framework at Okta

- Participated in Multi-Stakeholder Discussions, Drafting
- Internal Buy-in from Stakeholders at Okta
- Benefits of the Framework
  - Flexible
  - Includes Identity Management and MFA
  - Outcome-Driven
  - Global: Can Encompass Different Privacy Frameworks

RSAConference2020

Equifax's NIST Privacy Journey

Nick Oldham, Chief Privacy and Data Governance Officer, Equifax

Contents

- Key Elements of Our Privacy Transformation
- The Equifax Approach to Privacy
- Privacy Framework Alignment
- Privacy Framework Implementation

Equifax understands people want more control over how their personal information is collected, used, shared and protected.

As a result, Equifax has committed to responsibly and appropriately using personal information and to properly balance privacy with the important role data plays in today's modern economy.

Key Elements of Our Privacy Transformation

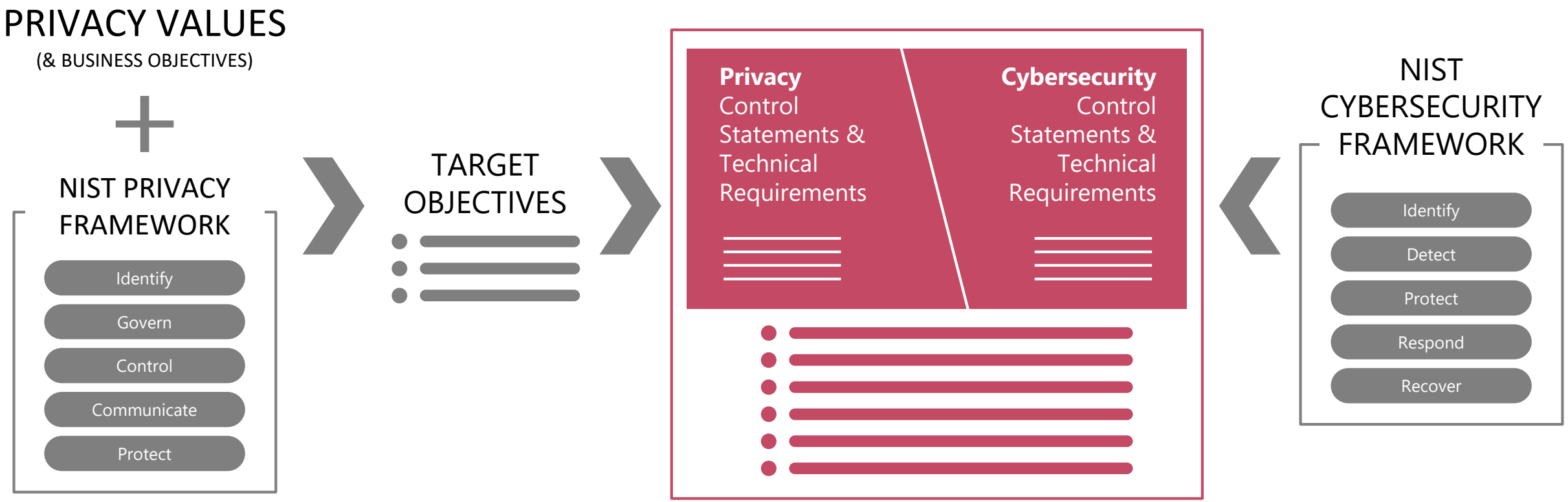
Early adopter of the NIST Privacy Framework

Security Framework aligned to NIST Cybersecurity Framework

Committed to responsible use of personal information

Driving toward a single enterprise framework for privacy and security based on the NIST models

Equifax's Approach to Privacy Controls



NIST Privacy Framework Alignment

KEY CONSIDERATIONS

1. Current security program framework
2. Privacy program maturity
3. Enterprise Privacy Values

HELPFUL FACTORS

1. NIST CSF alignment
   - Common framework structure
   - Mapping between security and privacy controls

SCENARIOS

In general, we have seen three scenarios as we have folded the NIST PF into our overall control framework:

1. **Revisions** to existing controls (through additional Technical Requirements or modifications to existing language)
2. **Net new** controls (beyond the scope of the NIST CSF)
3. Existing controls without need for modification

RSAConference2020

Closing

Apply What You Have Learned Today

- Lead on privacy and adopt the NIST Privacy Framework
- Provide NIST with implementation feedback
- Help the community and contribute to the Resource Repository

NIST Privacy Framework Resources

Website

https://www.nist.gov/privacyframework

Mailing List

List.nist.gov/privacyframework

Contact Us

PrivacyFramework@nist.gov

@NISTcyber #PrivacyFramework