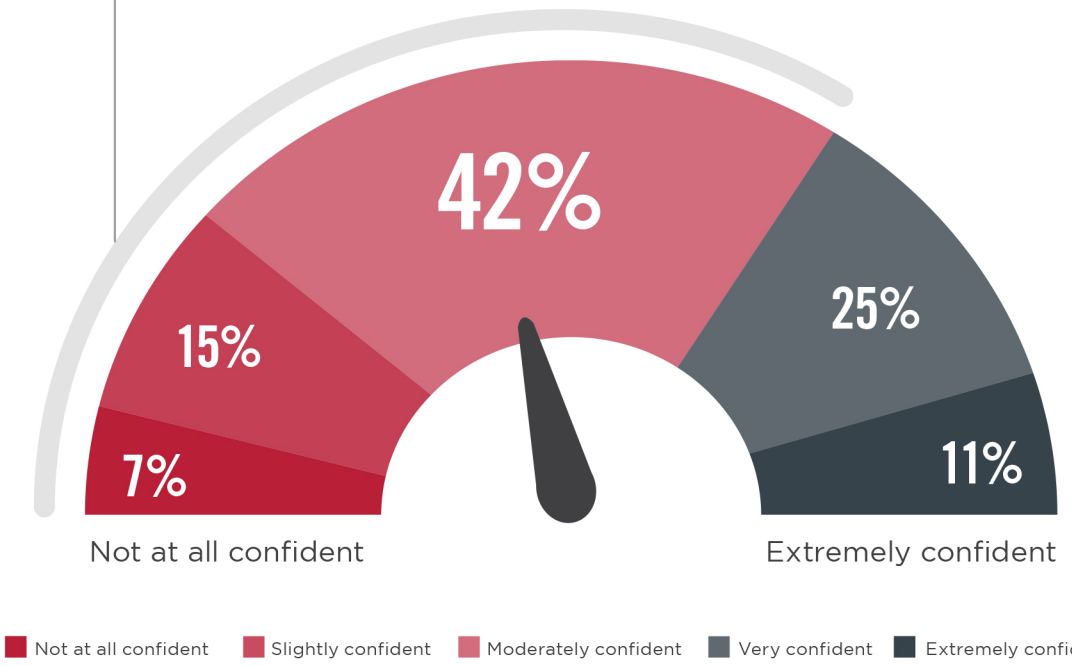
VIRTUAL 2021
ProcessUnity
CUSTOMER SUMMIT

Cybersecurity Program Management

May 18, 2021

How confident are you in your organization's ability to respond to a cyberattack?

64% Are at best moderately confident in their ability to respond to a cyberattack.



The Challenges

ACCOUNTABILITY MATTERS

Goal: Demonstrate good cybersecurity practices

Changes in the Industry

- CPRA (inf. “CCPA v2.0”) – augmented enforcement

Crackdown on Regulations – guilty offenders getting fined

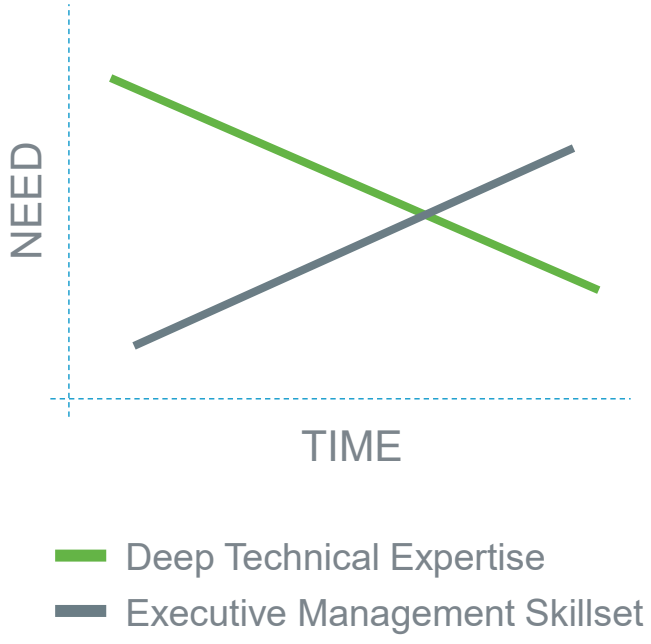
- GDPR
  - Google $56.6M
  - H&M $41M
  - TIM (Telecom Italia) $31.5M
  - British Airways $26M
  - Marriott $23.8M

Fragility of Third-Party Network

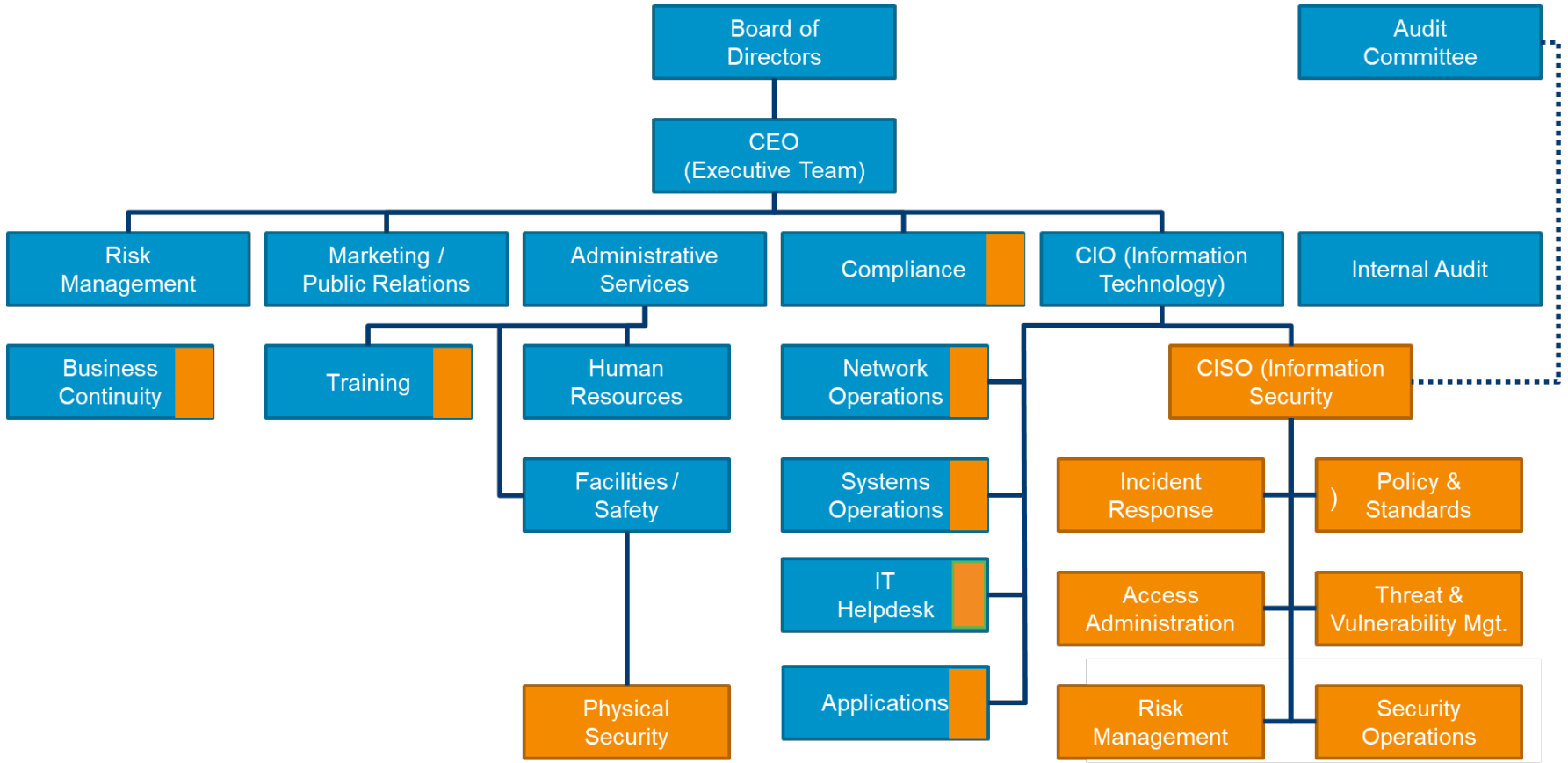
- SolarWinds

THE ROLE OF THE CISO

- There is a change happening.
- The CISO role will grow and gain respect.
- The CISO will become an enabler rather than a disabler.
- Enterprises will embrace the CISO's teaching function.

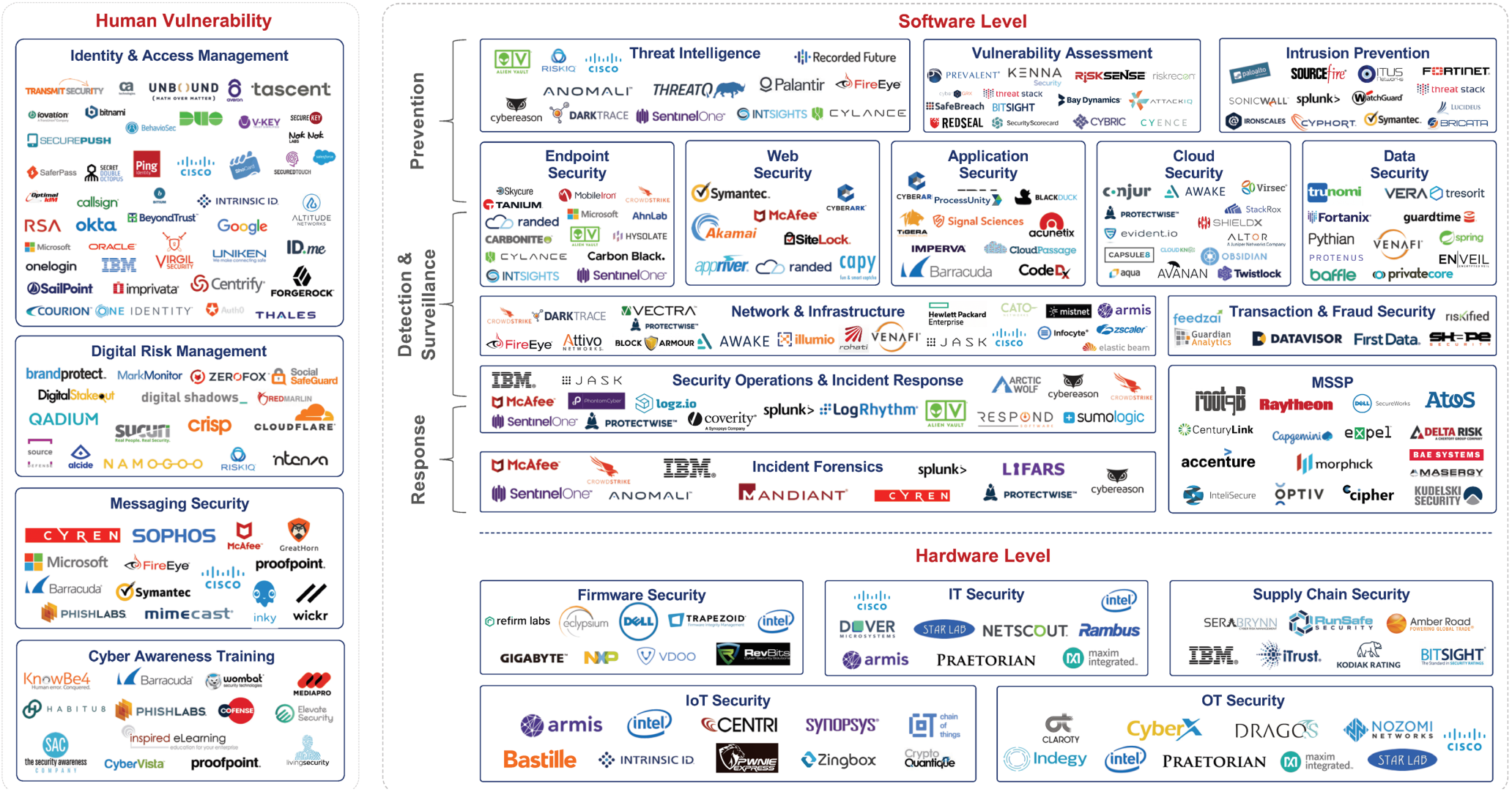


Cyber Risk is Pervasive



- Cross Functional
- Technical Depth & Guidance
- Business Recommendation & Policy
- Corporate-Wide Enablement & Testing
- Risk & Compliance Focal Point
- Incident Management Analytics

Cybersecurity Tools Alone Only Go So Far



Q: How are we doing overall for cyber?
A: ?

Q: Have we improved over time?
A: ?

Q: Where do we need to focus our attention
A: ?

Q: Where are our weaknesses?
A: ?

Source: https://foundationcapital.com/cybersecurity-the-next-trillion-dollar-market/

THE STATE OF THE STATE

- Last Fall, IBM Security and the Ponemon Institute published the *"5th annual Cyber Resilient Organization Report."* The report is based on their research from surveying more than 3,400 IT and security professionals around the world in April 2020, to determine their organizations' ability to detect, prevent, contain and respond to cybersecurity incidents.
- Here is a sample of their findings:

https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/

IBM/Ponemon Institute "Cyber Resilient Organization Report 2020"

ACCOUNTABILITY MATTERS

Prove to the C-suite, BoDs and regulators that the organization has:

A Plan

Compliant Controls and Processes

PRESENTING TO THE BOARD

Answering the 3 key questions

- Where is the risk?
- How are you going to fix it?
- How much does it cost?

Limited Visibility & Governance

★ Key Problem

CORP

Executive Leadership

CISO

Cybersecurity

Owners

METRICS

TOOLS

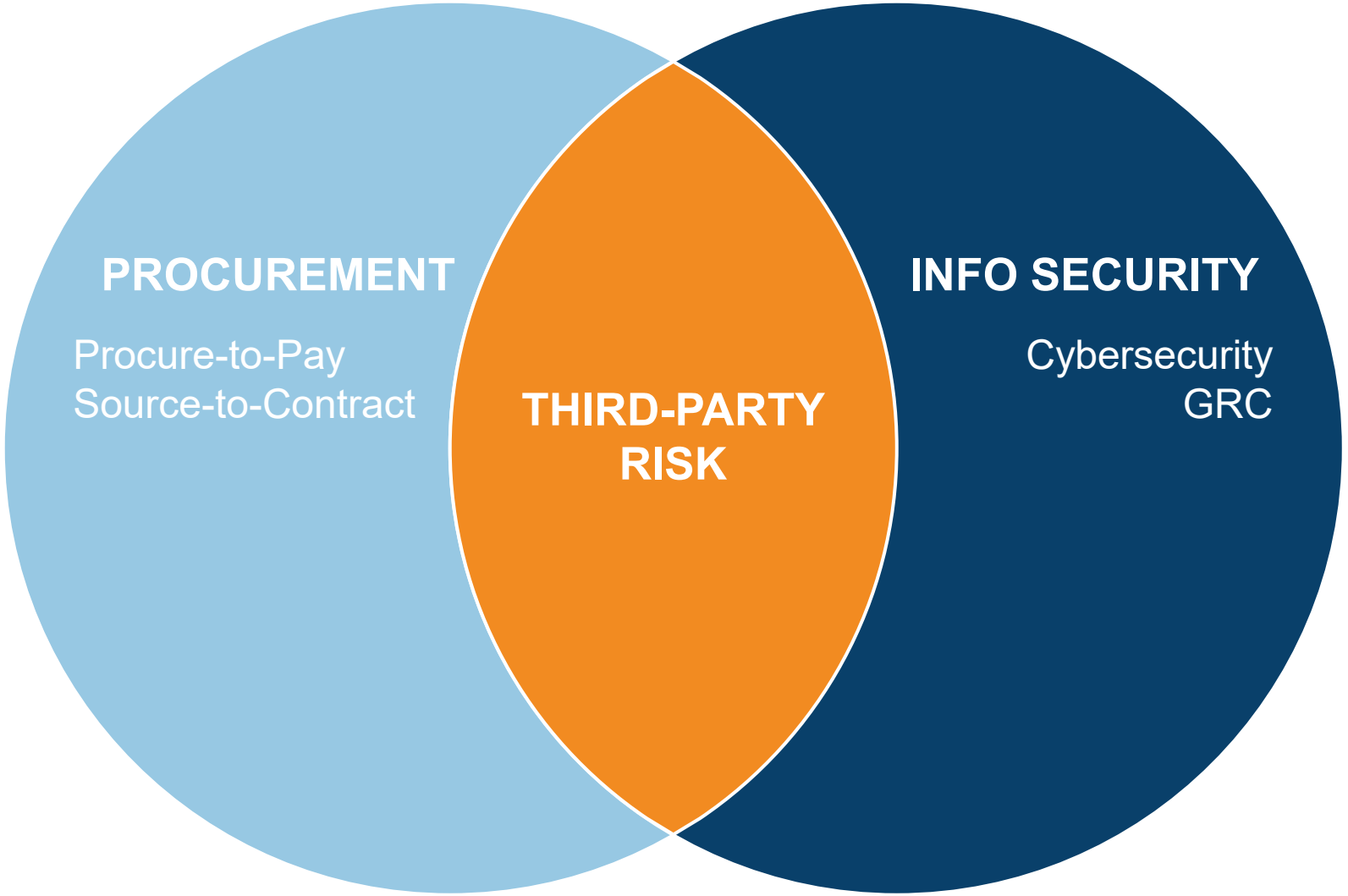
- SIEM
- Threat Intelligence
- Endpoint Security
- Application Security
- Cloud Security
- …

ORGANIZATION

- Networks
- Applications
- Organization
- Third Parties
- People
- Policies
- Systems

TPRM: Two Sides of the Same Coin

Flexible Configuration Covers Procurement and Information Security Use Cases



Establishing a Program

DEFINING YOUR CYBERSECURITY PROGRAM

Your Company Data

Organization

Policies

Processes

High Value Assets

Due Diligence

Training Programs

Third Parties

Risk & Control Methodology

Threats

Risks

Control Standards

Regulations

Assess, Review & Monitor Tools

Threat Reviews

Control Reviews

Risk Evaluations

Baseline Questionnaires

HVA Questionnaires

TPR Questionnaire

Assessments

"State of the State" for Cybersecurity Risk

Risk-Prioritized Projects

Schedule of Coverage

COMMITTING TO A CONTROL FRAMEWORK

- NIST 800-53
- NIST CSF
- SCF
- ISO 27001/27002
- IASME
- FAIR
- SOC 2
- CIS
- COBIT
- HITRUST
- …

GDPR

CCPA

NYDFS

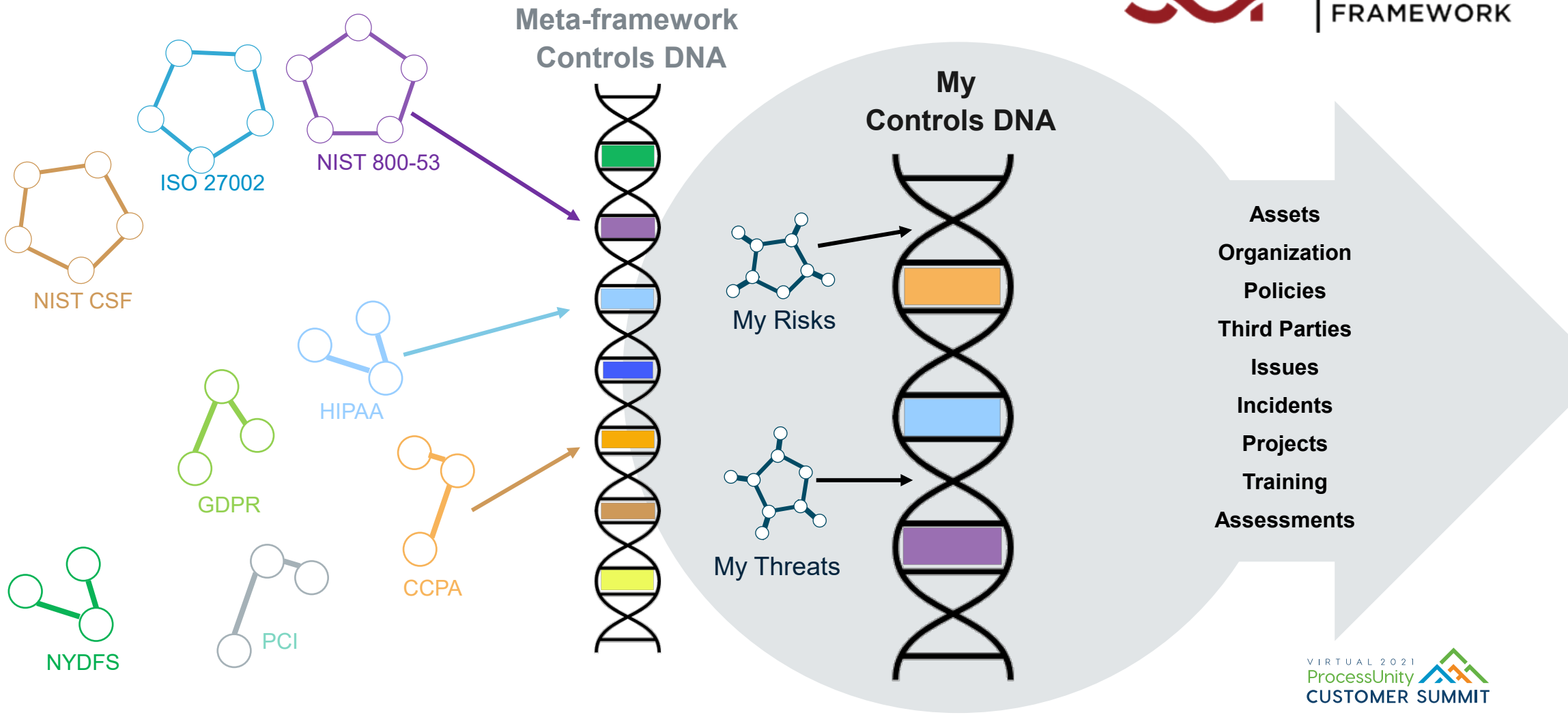
HIPAA

Many others…

COMMITTING TO A CONTROL FRAMEWORK

CONTROLS MAPPED TO YOUR PROGRAM COMPONENTS

SECURE CONTROLS FRAMEWORK



VIRTUAL 2021 ProcessUnity CUSTOMER SUMMIT

DATA MAPPING EXAMPLE

Framework	Name
HIPAA (Health Insurance Portability and Accountability Act	164.306: Security Standard: General Rules
HIPAA (Health Insurance Portability and Accountability Act	164.308: Administrative Safeguards
HIPAA (Health Insurance Portability and Accountability Act	164.316: Policies & Procedures / Documentation Requirements
HIPAA (Health Insurance Portability and Accountability Act	164.530:Administrative Requirements
CCPA (California Consumer Privacy Act)	1798.81.5
GDPR (General Data Protection Regulation) 1.0	32. Security of Processing
ISO 27002 Standard	A.5.1.1: Policies for Information Security
PCI DSS (Payment Card Industry Data Security Standard)	PCI DSS Requirements 12.1
PCI DSS (Payment Card Industry Data Security Standard)	PCI DSS Requirements 12.1.1
NIST (800-53 Standard) Rev. 4	PM-1: Information Security Program Plan
NYDFS (New York State Department of Financial Services)	Section 500.02: Cybersecurity Program

DEMO

VIRTUAL 2021
ProcessUnity
CUSTOMER SUMMIT

Thank You!